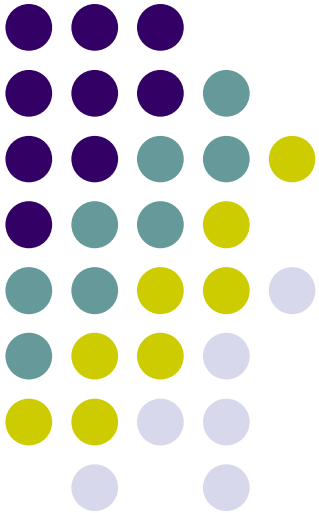
信息隐藏技术

第10讲：图像隐密术(变换域图)

（Image Steganography）

周琳娜

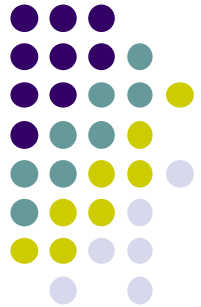
2023.05.10



图像隐密术

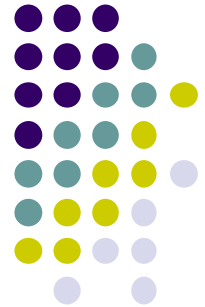
- 1、图像基本知识
- 2、位图隐密术
- 3、索引图隐密术
- 4、变换域图隐密术
  - ✓ 变换域图像压缩
  - ✓ 变换域隐密术
- 5、图像隐密编程实践（互动）

变换域图像压缩



- **图像变换**
  - ✓ **空域→正交矢量空间**
- **变换类型**
  - ✓ **离散傅立叶**
  - ✓ **希尔伯特**
  - ✓ **小波**
  - ✓ **离散余弦(DCT)**
  - ✓ **…**

变换域图像



- JPEG图像
  - DCT变换
  - 来源广泛
    - 手机、数码相机、网络…

图像压缩

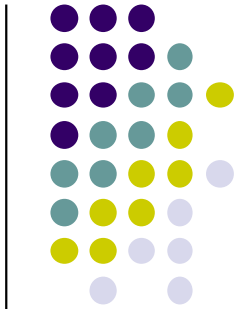
- 压缩目的
  - 减少数据量，便于存储、传输、处理
- 压缩必要性
  - 数据量大，导致存储和传输带宽瓶颈
- 压缩可能性
  - 信源数据存在极强的相关性
    - 编码熵冗余
    - 空域冗余
    - 时域冗余
    - 视觉冗余

JPEG背景

- JPEG(Joint Photographic Experts Group)
  - 由 ISO和IEC两个机构联合组成的一个图像专家小组
  - 负责制定静态的数字图像数据 压缩编码标准
- JPEG 标准
  - 该专家组开发的算法称为JPEG算法
  - JPEG 已经成为国际上通用图像的标准
- JPEG 标准适用范围
  - 灰度图像，彩色图像
  - 静止图像的压缩，视频序列帧内图像压缩
  - JPEG可以大范围地调节图像码率和质量

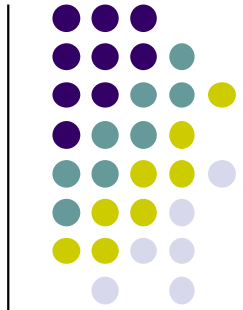
JPEG背景

- JPEG算法与颜色空间无关
  - 对于单色图像，只有一个亮度分量
  - 对于彩色图像，JPEG对每个分量进行单独编码
- 颜色空间转换不包含在JPEG算法中
  - 对于YUV图像: 对于Ｙ Ｕ Ｖ采用不同的分辨率，对每个不同分量的可以采用不同的量化参数和熵编码表。
  - 可压缩来自不同颜色空间的图像:RGB,CMKY等



JPEG背景

- JPEG核心算法
  - **DCT（Discrete Cosine Transform）**离散余弦变换
  - **DPCM（Differential Pulse Code Modulation）**差分脉冲编码调制，简称差值编码



JPEG背景

- 对于一个图像分量，JPEG规定了4 种操作方式
  - 基于DCT的顺序编码模式 （**baseline CODEC**）
    - 单遍扫描完成一个图像分量的编码，扫描次序从左到右，从上到下。
  - 基于DPCM(差分脉冲编码调制)无损编码模式
    - 无损编码
    - 压缩比可以达到2:1
  - 基于DCT的渐进编码模式
    - 通过多次扫描一幅图像分量的编码，提供了一个由粗到精的渐进码流结构。
  - 基于DCT的分层编码模式
    - 提供多分辨率的码流结构。

基于DCT的顺序编码模式

- 算法基本步骤
  - 将原图转换为亮度（Y）、色差（Cb、Cr）表示，并进行下采样
  - 分成8×8数据块，数据[0~255]转换为[-128~127]
  - 进行正向离散余弦变换(FDCT)
  - 量化(quantization)
  - Zig-Zag排列量化结果(zigzag scan)
  - 使用DPCM对直流系数(DC)进行编码
  - 使用行程编码对交流系数(AC)进行编码
  - 熵编码(entropy coding)：哈夫曼或算术编码

基于DCT的顺序编码模式

- 系统框架

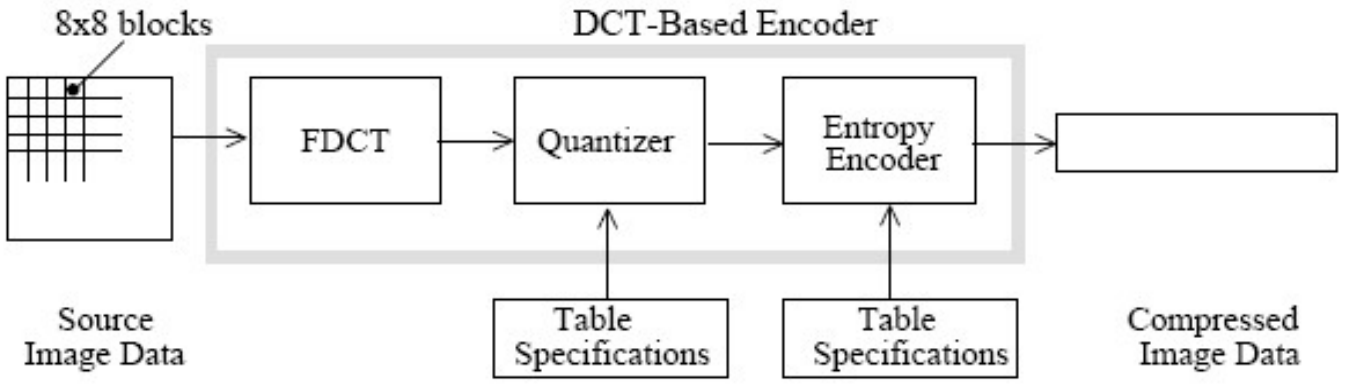


Figure 1. DCT-Based Encoder Processing Steps

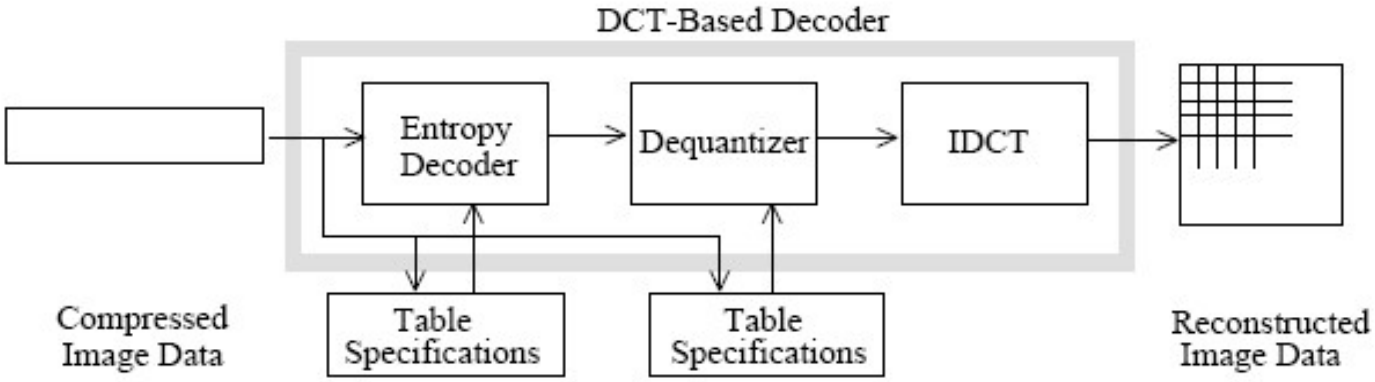


Figure 2. DCT-Based Decoder Processing Steps

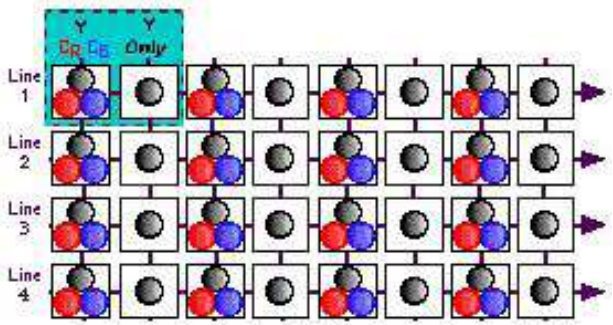
基于DCT的顺序编码模式

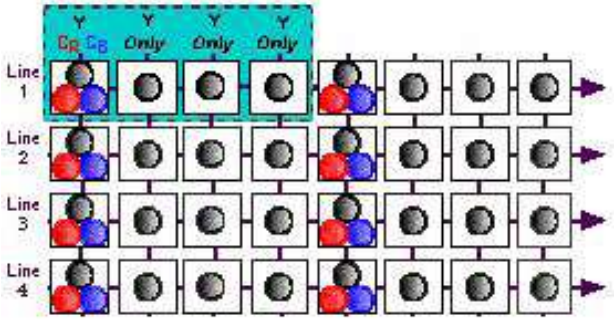
- RGB与Y、Cb、Cr之间关系
  - RGB、YCbCr为8bit unsigned类型

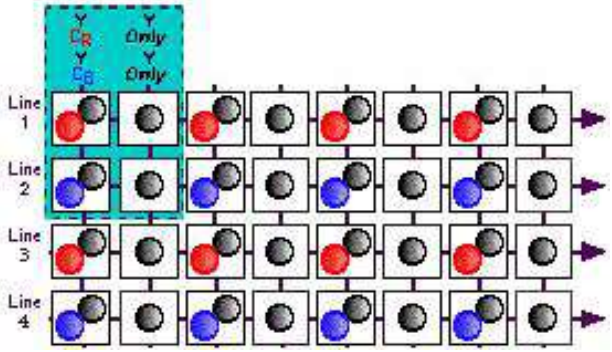
$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.5870 & 0.1140 \\ -0.1687 & -0.3313 & 0.5000 \\ 0.5000 & -0.4187 & -0.0813 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix}$$

基于DCT的顺序编码模式

- 采样格式

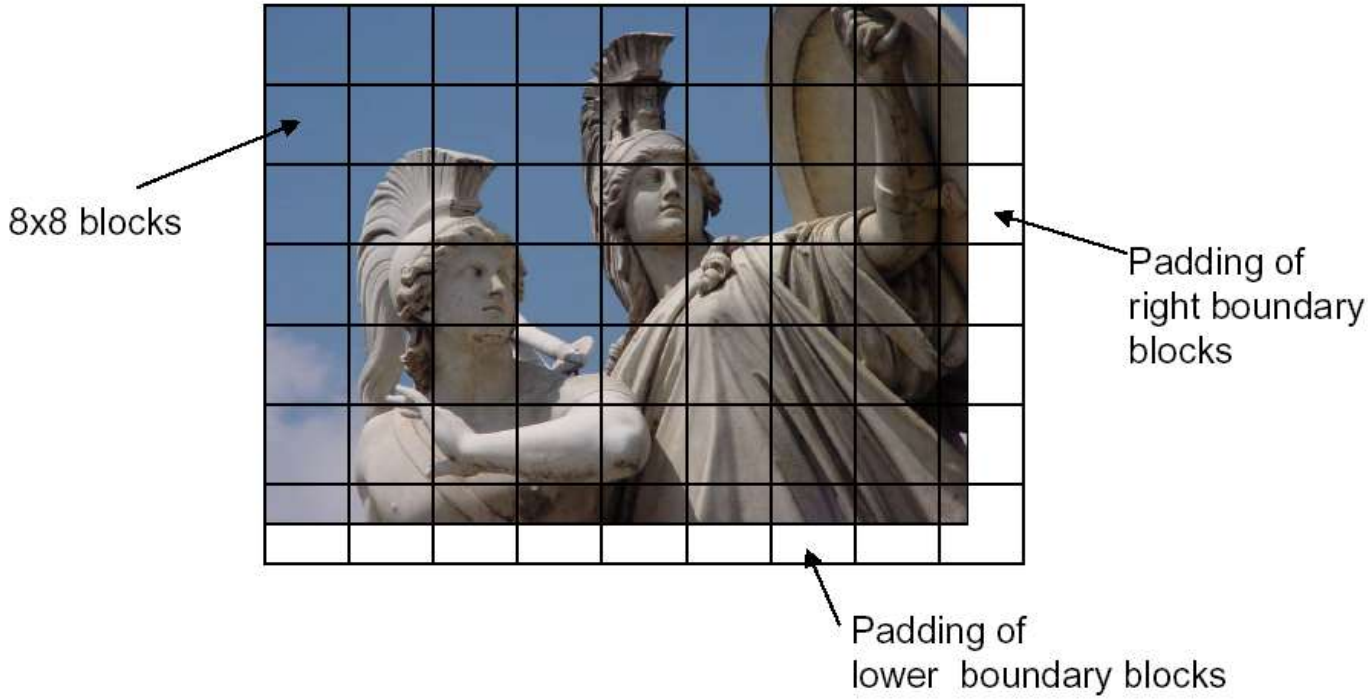






基于DCT的顺序编码模式

- 图像块的划分



基于DCT的顺序编码模式

- 离散余弦变换(DCT)
  - 设X的离散余弦变换为Y, X ,Y是N × N 块
  - 正变换FDCT $Y = CXC^T$
  - 逆变换IDCT $X = C^T YC$
  - C为离散余弦变换矩阵，C^T 为C的转置矩阵

基于DCT的顺序编码模式

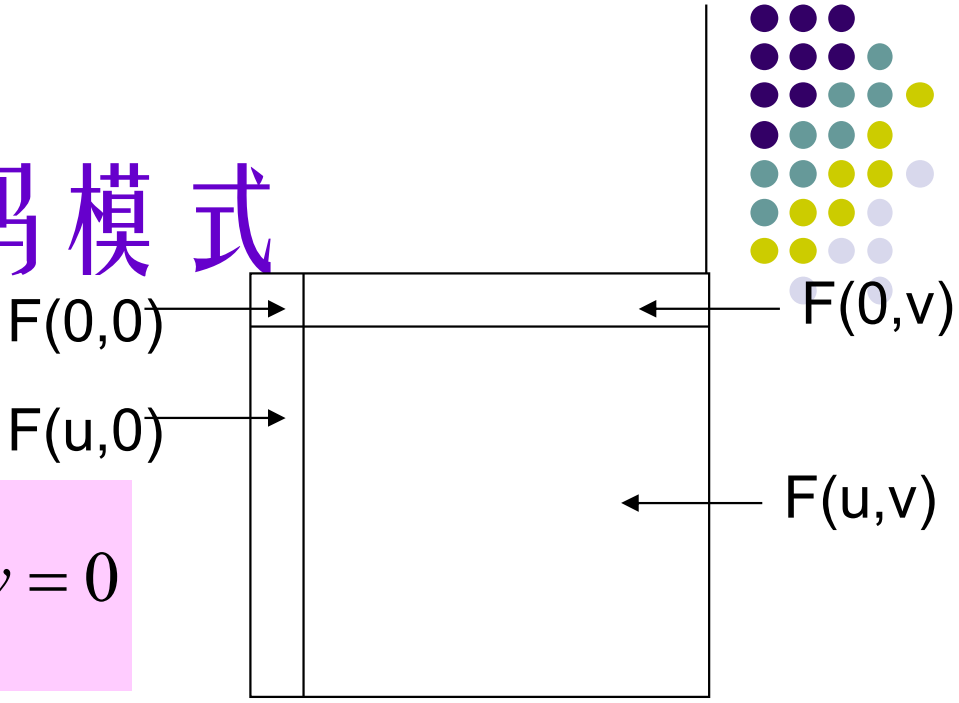
- 一维离散余弦变换

  $f(x)$为一维离散函数，$x = 0,1,\cdots,\ N-1$

$$F(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x), \qquad u = 0$$

$$F(u) = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi}{2N}(2x+1)u\right], \quad u = 1,2,\cdots,N-1$$

基于DCT的顺序编码模式



- 二维离散余弦变换

$$F(0,0)=\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y),\qquad u=0,v=0$$

$$F(u,0)=\frac{2}{\sqrt{N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2x+1)u\right],\quad v=0,\ u=1,2,\cdots,N-1$$

$$F(0,v)=\frac{2}{\sqrt{N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2y+1)v\right],\quad u=0,\ v=1,2,\cdots,N-1$$

$$F(u,v)=\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\cos\left[\frac{\pi}{2N}(2y+1)v\right]$$

$$u,v=1,2,\cdots,N-1$$

基于DCT的顺序编码模式

- 二维离散余弦变换
  - 反变换

$$f(x,y)=\frac{1}{N}F(0,0)$$
$$+\frac{2}{\sqrt{N}}\sum_{u=1}^{N-1}F(u,0)\cos\left[\frac{\pi}{2N}(2x+1)u\right]$$
$$+\frac{2}{\sqrt{N}}\sum_{v=1}^{N-1}F(0,v)\cos\left[\frac{\pi}{2N}(2y+1)v\right]$$
$$+\frac{2}{N}\sum_{u=1}^{N-1}\sum_{v=1}^{N-1}F(u,v)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\cos\left[\frac{\pi}{2N}(2y+1)v\right]$$

基于DCT的顺序编码模式

- 二维离散余弦变换
  - 变换矩阵*C*为

$$C=\sqrt{\frac{2}{N}}\begin{bmatrix}\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & \cdots & \sqrt{\frac{1}{2}}\\ \cos\frac{\pi}{2N} & \cos\frac{3\pi}{2N} & \cdots & \cos\frac{(2N-1)\pi}{2N}\\ \vdots & \vdots & \vdots & \vdots\\ \cos\frac{(N-1)\pi}{2N} & \cos\frac{3(N-1)\pi}{2N} & \cdots & \cos\frac{(2N-1)(2N-1)\pi}{2N}\end{bmatrix}_{N\times N}$$

  - 取N=8即可

基于DCT的顺序编码模式

- Luminance

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	36	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

- Chrominance

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

$$Y^{Q}(x,y) = IntegerRound[Y(x,y)/Q(x,y)]$$

基于DCT的顺序编码模式

- Luminance

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	36	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

- Chrominance

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

量化表： 根据心理视觉加权函数得到的

量化:DCT变换系数除以量化步长，四舍五入取整

简单压缩例子

- 缺省的量化方式

139	144	149	153	155	155	155	155
144	151	153	156	159	156	156	156
150	155	160	163	158	156	156	156
159	161	162	160	160	159	159	159
159	160	161	162	162	155	155	155
161	161	161	161	160	157	157	157
162	162	161	163	162	157	157	157
162	162	161	161	163	158	158	158

(a) source image samples

235.6	-1.0	-12.1	-5.2	2.1	-1.7	-2.7	1.3
-22.6	-17.5	-6.2	-3.2	-2.9	-0.1	0.4	-1.2
-10.9	-9.3	-1.6	1.5	0.2	-0.9	-0.6	-0.1
-7.1	-1.9	0.2	1.5	0.9	-0.1	0.0	0.3
-0.6	-0.8	1.5	1.6	-0.1	-0.7	0.6	1.3
1.8	-0.2	1.6	-0.3	-0.8	1.5	1.0	-1.0
-1.3	-0.4	-0.3	-1.5	-0.5	1.7	1.1	-0.8
-2.6	1.6	-3.8	-1.8	1.9	1.2	-0.6	-0.4

(b) forward DCT coefficients

简单压缩例子

- 缺省的量化方式

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

(c) quantization table

15	0	-1	0	0	0	0	0
-2	-1	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(d) normalized quantized coefficients

简单压缩例子

- 缺省的量化方式

240	0	-10	0	0	0	0	0
-24	-12	0	0	0	0	0	0
-14	-13	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(e) denormalized quantized coefficients

144	146	149	152	154	156	156	156
148	150	152	154	156	156	156	156
155	156	157	158	158	157	156	155
160	161	161	162	161	159	157	155
163	163	164	163	162	160	158	156
163	164	164	164	162	160	158	157
160	161	162	162	162	161	159	158
158	159	161	161	162	161	159	158

(f) reconstructed image samples

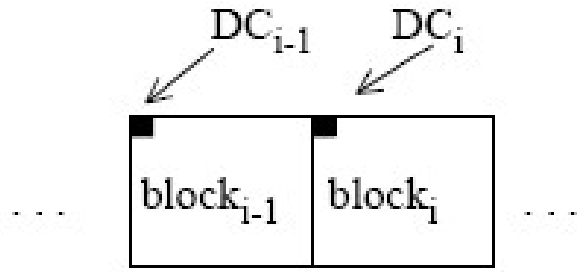
基于DCT的顺序编码模式

- DC系数和AC系数的编码方式
  - DCT变换后，能量集中在左上角。
  - 由于两个相邻的8×8子块的DC系数相差很小，采用DPCM对直流(DC)系数单独编码。
  - 其它63个元素是交流(AC)系数，采用行程编码。
  - 问题: 如何排列这63个系数？

    为了保证低频分量先出现，高频分量后出现，同时增加连续“0”的个数，采用Zig-Zag的排列方法。

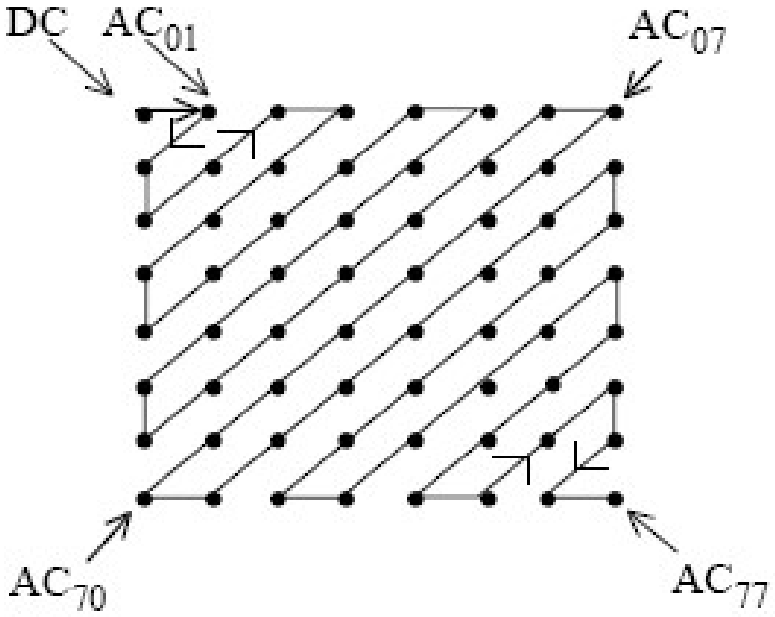
基于DCT的顺序编码模式

- DC系数和AC系数的编码方式



DIFF = DC$_i$ - DC$_{i-1}$

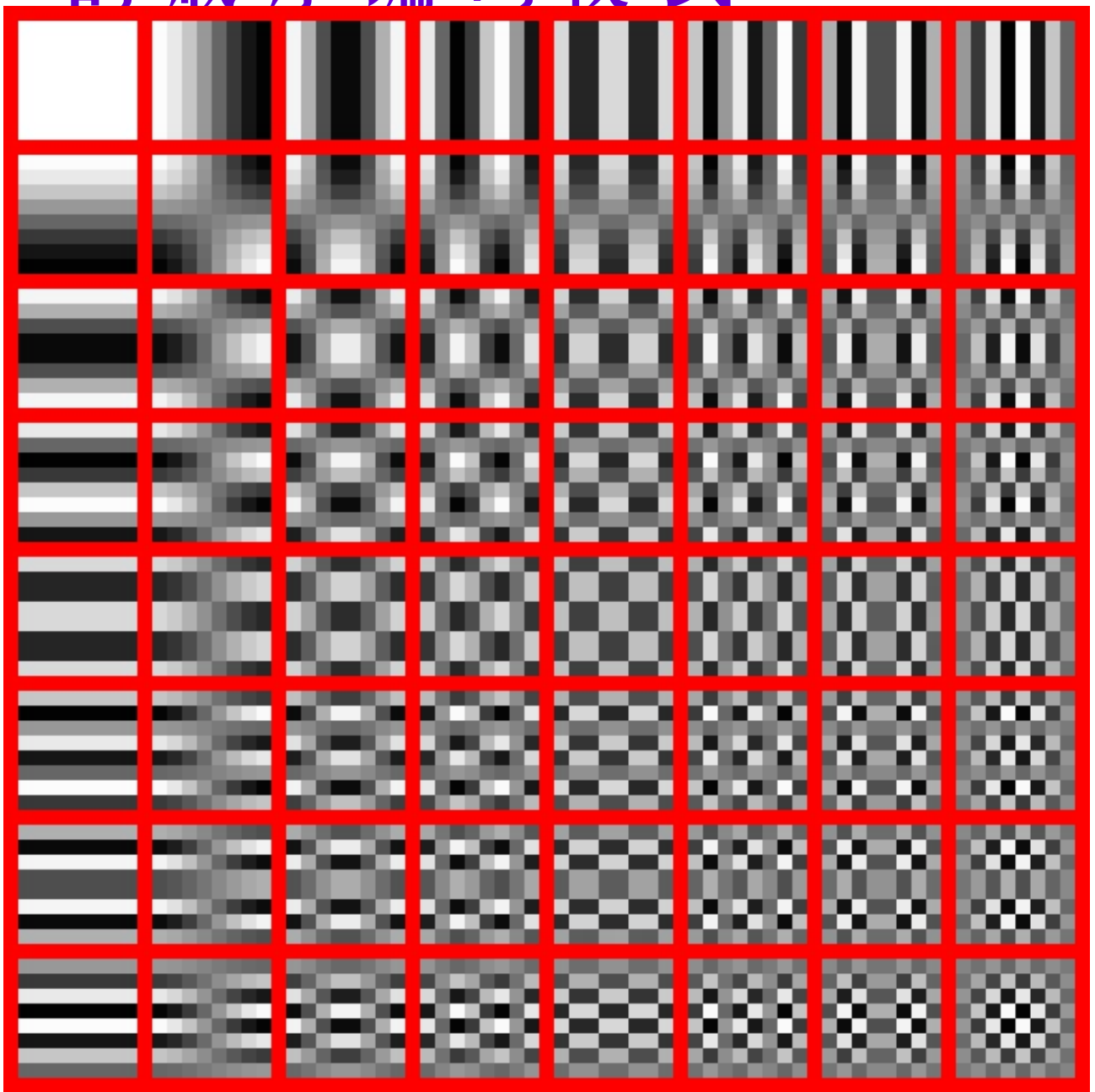
Differential DC encoding



Zig–zag sequence

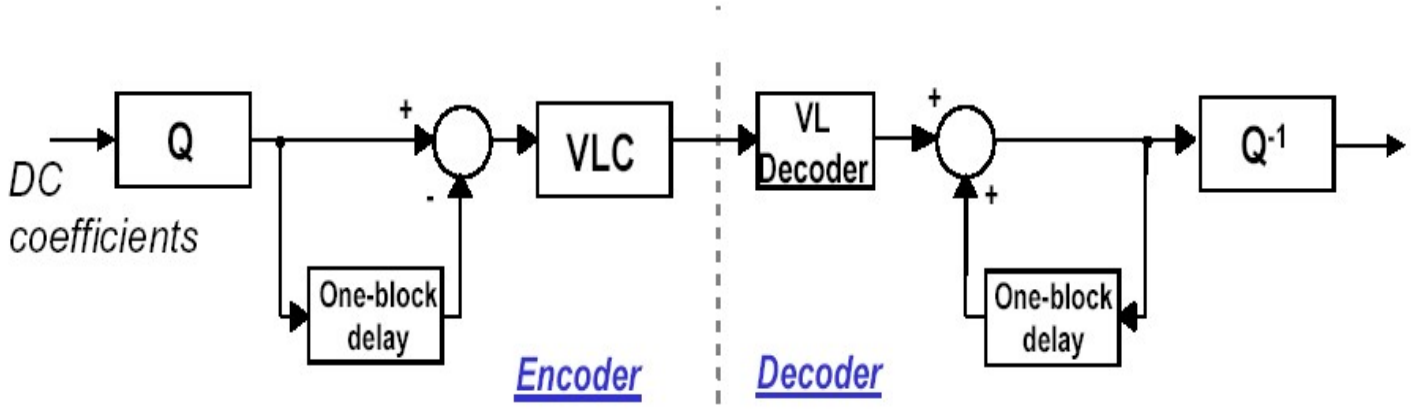
基于DCT的顺序编码模式

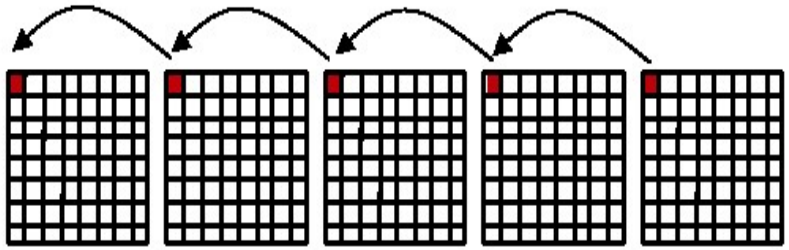
- JPEG
- 单频
- 图像



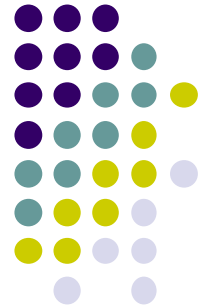
基于DCT的顺序编码模式

- DC系数和AC系数的编码方式



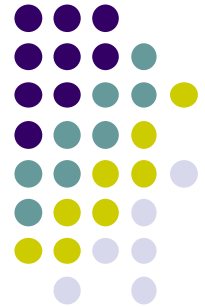


基于DCT的顺序编码模式



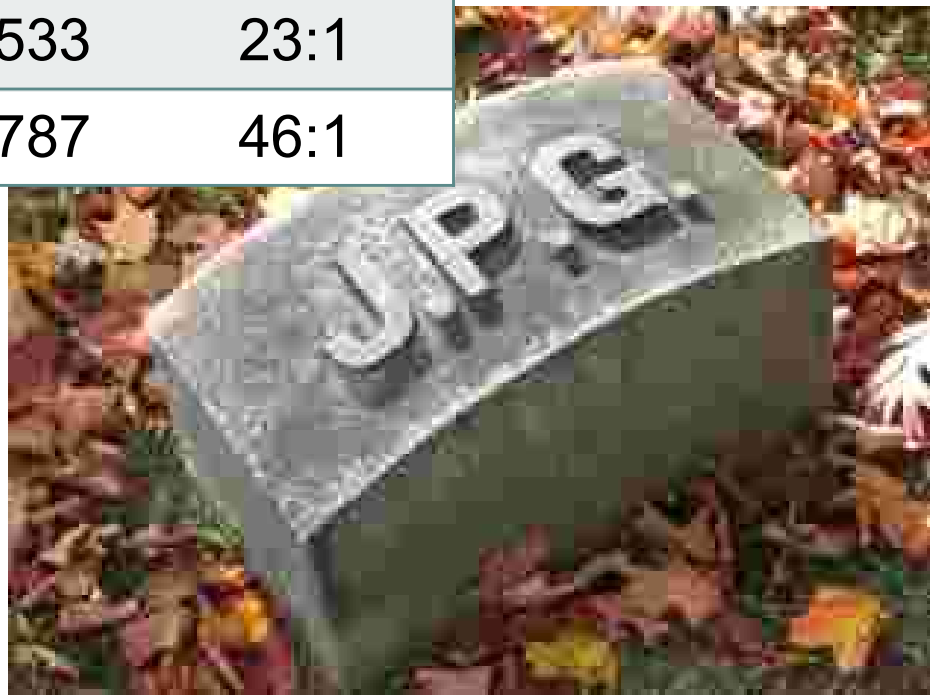
- 熵编码
  - JPEG标准规定了两种熵编码算法：
    - 哈夫曼编码
    - 自适应算术编码
  - 哈夫曼编码一般采用的是固定的哈夫曼表。
  - 对亮度分量和色度分量采用了不同的哈夫曼表。

基于DCT的顺序编码模式



- 质量因子
  - JPEG通过设定一个质量控制因子Q，在量化时用该因子与标准量化表相运算作为实际的量化步长
- 注意
  - JPEG图像中，并未存储Q，而是量化表
  - 实际情况中，Q值大部分为估计值

顺序	Q值	图像大小	压缩比
左上	100	83,261	2.6:1
右上	50	15,138	15:1
左下	25	9,533	23:1
右下	10	4,787	46:1



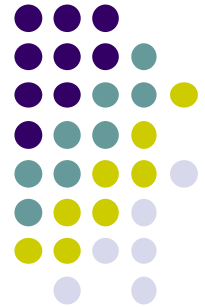
JPEG格式图像信息隐藏

- LSB(BMP---JPEG)

DCT系数特征

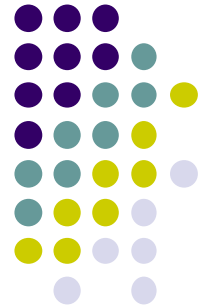
- DCT系数
  - 左上角为直流和低频系数，右下角为高频系数中间区域为中频系数
  - 低频代表图像之间慢变化，高频代表像素之间的快变化
- 中低频部分包含了图像的大部分能量，对人的视觉最重要的信息部分，都集中在中低频

DCT系数特征



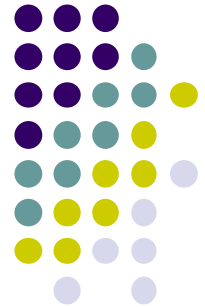
- 一般图像的压缩和处理，为了保持图像的可视性，都保留了图像的中低频部分(高频部分大多为0)
- 低频部分的改变有可能引起图像较大的变动
- 一般都将隐藏信息嵌入在载体的中频部分

典型JPEG图像信息隐藏算法



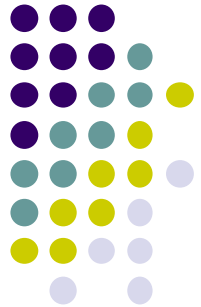
- JSteg
- Outguess算法
- F5
- MB
- PQ
- YASS

典型JPEG图像信息隐藏算法



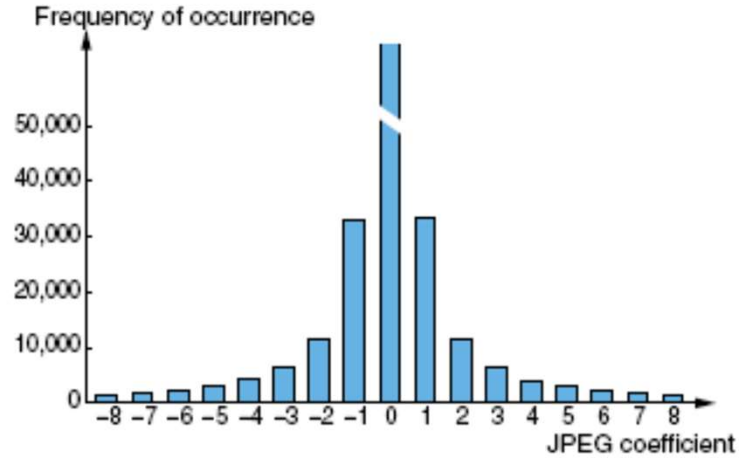
- JPEG格式图像在网络中大量传输
  - 应用普遍性
  - JPEG图像编码算法的公开性
- 引起的怀疑相对较小
  - ？

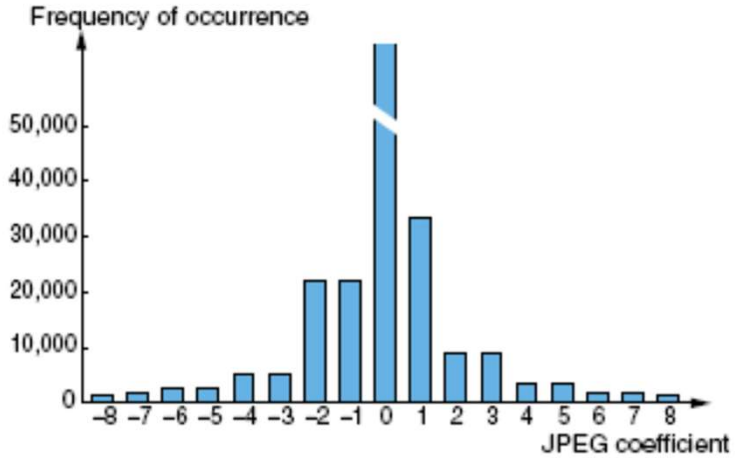
JSteg隐写算法

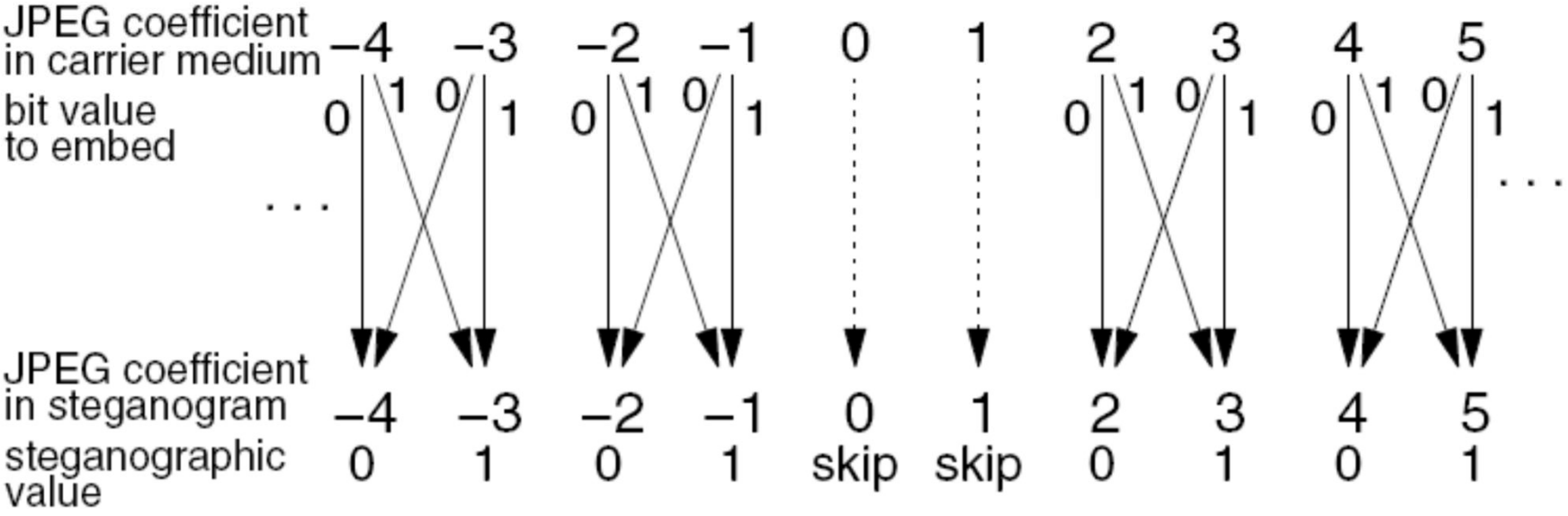


- 基本思想
  - 用秘密信息比特直接替换JPEG图像中量化后DCT系数的最低比特位，但若量化后DCT系数为0或者1，则不进行处理

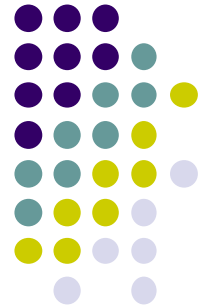
JSteg隐写算法


Frequency of occurrence
50,000
40,000
30,000
20,000
10,000
0
−8 −7 −6 −5 −4 −3 −2 −1 0 1 2 3 4 5 6 7 8
JPEG coefficient


Frequency of occurrence
50,000
40,000
30,000
20,000
10,000
0
−8 −7 −6 −5 −4 −3 −2 −1 0 1 2 3 4 5 6 7 8
JPEG coefficient

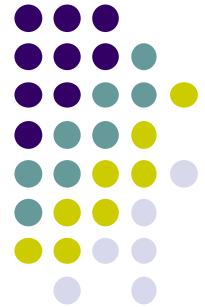

JPEG coefficient in carrier medium
bit value to embed
JPEG coefficient in steganogram
steganographic value
−4 −3 −2 −1 0 1 2 3 4 5
0 1 0 1 0 1 0 1 0 1
. . .
−4 −3 −2 −1 0 1 2 3 4 5
0 1 0 1 skip skip 0 1 0 1
. . .

JSteg隐写算法



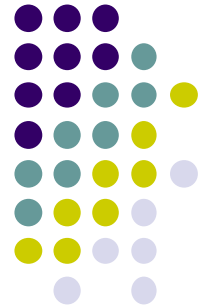
- 嵌入
  - 先获得图像量化后的DCT系数矩阵
  - 对于不为0、 1的DCT系数，用秘密信息取代其LSB，即完成嵌入过程
- 提取
  - 将含密图像中不等于0, 1的量化DCT系数的LSB取出
- 实质是将LSB嵌入法应用到量化后的DCT系数
  - 优点：实现简单
  - 缺点：直方图异常(出现“对效应”)，x2分析可以容易检测
  - 安全性不好

OutGuess隐写算法



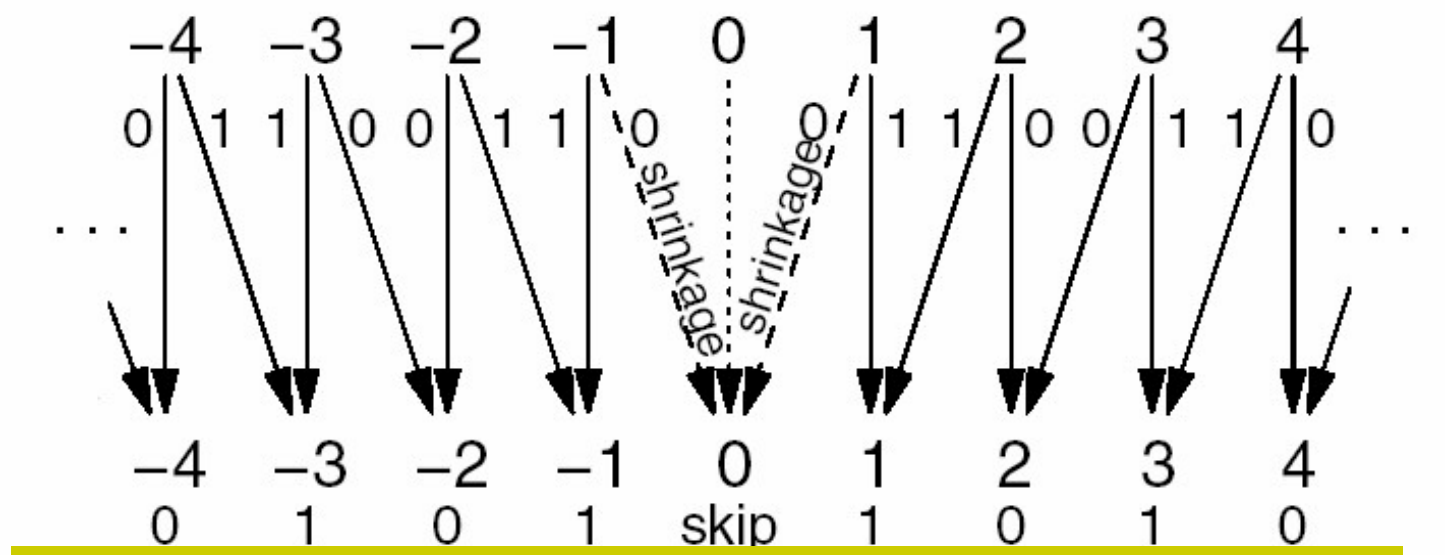
- Niels Provos针对Jsteg类算法的缺陷提出的一种方法，主要分两个部分
  - 嵌入过程
    - 不修改值为0，1的DCT系数，
    - 用伪随机数发生器产生间隔以决定下一个要嵌入的DCT系数的位置（随机间隔）
  - 纠正过程
    - 消除对效应的出现
    - 利用未被修改的DCT系数进行修改来维持直方图保持不变
- 基本原理：量化后DCT系数的LSB+纠正过程

F5隐写算法

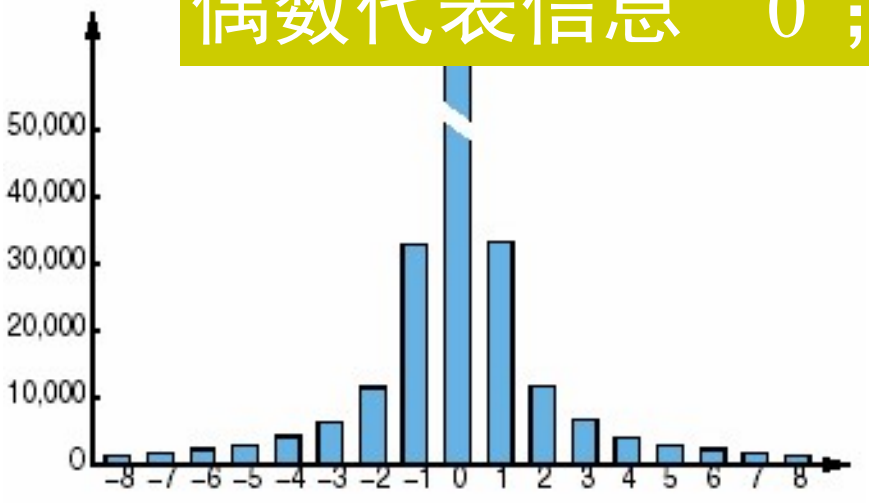


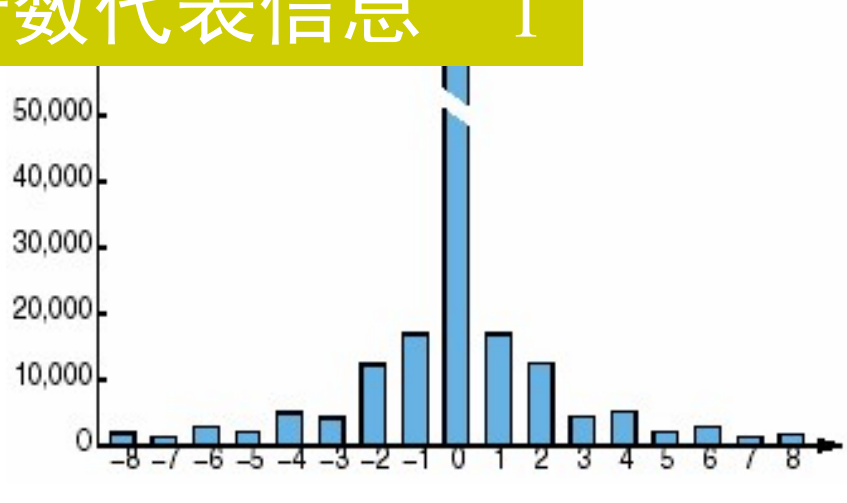
- 由德国Pfitzmann和Westfeld在2001年提出
- 一种针对JPEG图像，可以提供较大的嵌入容量、抗x^2检测的隐写算法
- F5的算法过程
  - 用户输入密码产生一组随机序列，利用该随机序列来随机选择量化DCT系数的非零交流系数
  - 利用矩阵编码，对选中的DCT系数分组，每组包含2^k-1个DCT系数，在最多修改1个DCT系数情况下用以嵌入k比特信息。
- 在F3和F4隐写基础上发展而来

F5隐写-F3

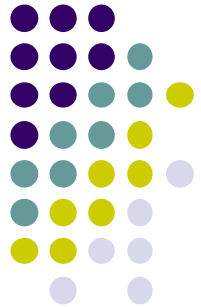


偶数代表信息“0”；奇数代表信息“1”





F5隐写-F3

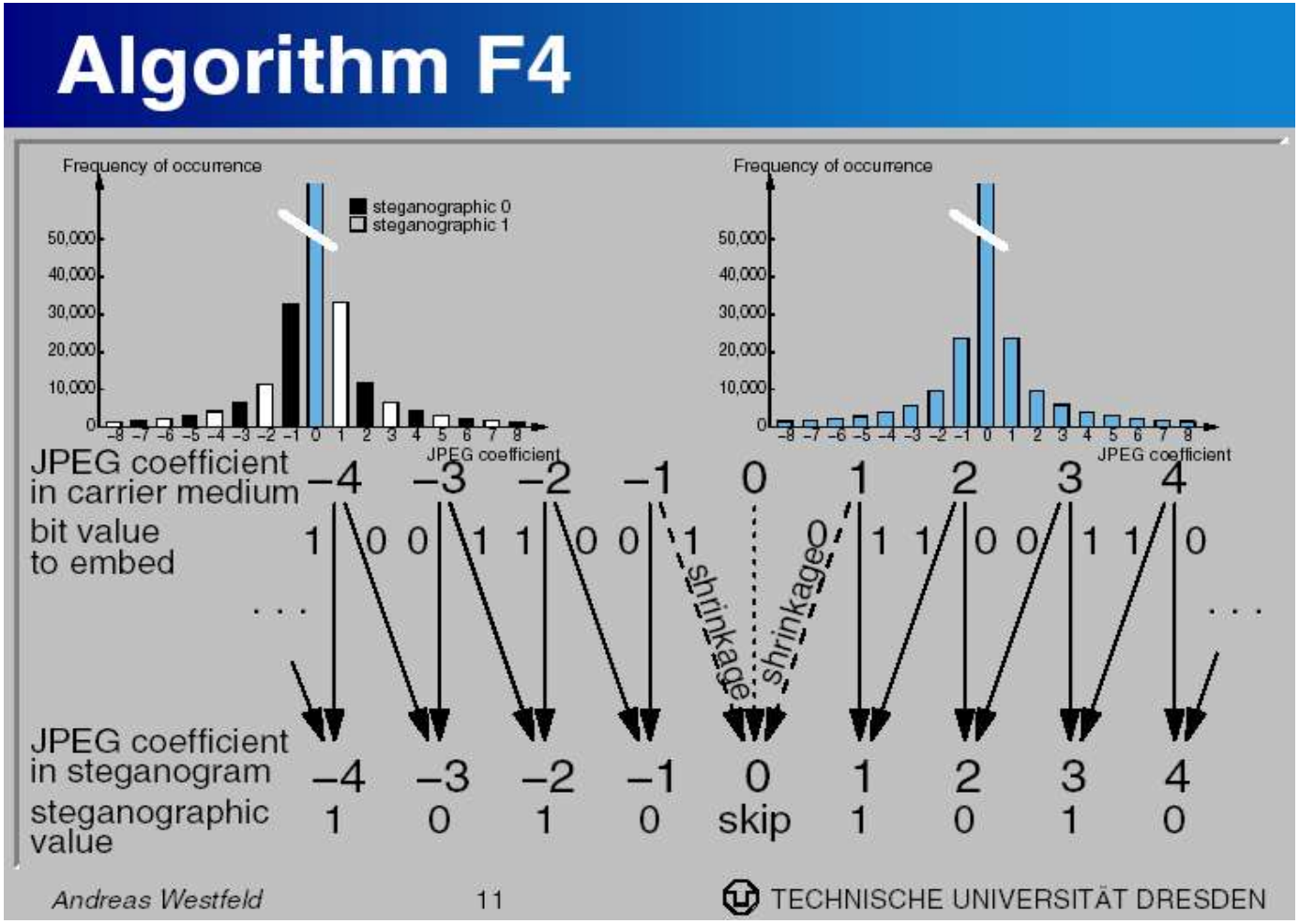


- 嵌入
  - 若DCT系数LSB秘密信息比特相同，则不做改动；否则将该DCT系数的绝对值减1
  - 0系数不嵌入信息，当嵌入使非零系数变为零时，此次嵌入无效，在下一个系数中重新嵌入
- 提取
  - 提取非0系数的LSB

F5隐写-F4

- 与F3类似
  - 正奇系数和负偶系数代表1
  - 正偶系数和负奇系数代表0
  - 0系数仍不负载秘密信息
- 绝对值减1

F5隐写-F4


Algorithm F4
Frequency of occurrence
steganographic 0
steganographic 1
JPEG coefficient
Frequency of occurrence
JPEG coefficient
JPEG coefficient in carrier medium
bit value to embed
shrinkage
shrinkage
JPEG coefficient in steganogram
steganographic value
skip
Andreas Westfeld
11
TECHNISCHE UNIVERSITÄT DRESDEN

F5隐写

- F3缺陷：零收缩,顺序嵌入

  偶数的数目大于奇数数目

- F4缺陷：零收缩,顺序嵌入
- F5
  - F4基础上，引入混洗和矩阵编码技术随机嵌入
  - 混洗使得隐密图像的质量比较均衡
  - 矩阵编码减少嵌入对系数的修改

F5隐写-矩阵编码

- 矩阵编码
  - 由Ron Crandall于1998年提出
  - 目的是以少的修改嵌入多的信息

嵌入2比特信息x_1、x_2，需载体的3个LSB：$a1\ a2\ a3$
最多改动其中的一个a_i即可实现2比特数据的嵌入。

$x_1 = a_1 \oplus a_3, x_2 = a_2 \oplus a_3$

$a_1\ a_2\ a_3$不作任何改动

$x_1 \neq a_1 \oplus a_3, x_2 = a_2 \oplus a_3$

改动a_1

$x_1 = a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3$

改动a_2

$x_1 \neq a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3$

改动a_3

F5隐写-矩阵编码

- $(1, n, k)$码的性能指标
- 改变的比特的比例为
  - $\boldsymbol{D}(k)=1/(n+1)=1/2^k$
- 嵌入率为
  - $\boldsymbol{R}(k)=k/n=k/(2^k-1)$
- 嵌入效率为
  - $\boldsymbol{W}(k)=\boldsymbol{R}(k)/\boldsymbol{D}(k)=2^k*k/(2k-1)$

F5隐写-矩阵编码

- (1, n, k)码的改变比例和嵌入效率

k	1	2	3	4	5	6	7	8
n	1	3	7	15	31	63	127	255
改变比例(%)	50.0	25.0	12.5	6.25	3.12	1.56	0.78	0.39
嵌入率(%)	100	66.67	42.86	26.67	16.13	9.52	5.51	3.14
嵌入效率	2.00	2.67	3.43	4.27	5.16	6.09	7.06	8.03

F5隐写

- 嵌入过程
  - 获取载体图像，得到量化后的DCT系数
  - 对AC系数进行混洗，该方法作为密钥（置乱）
  - 对可用AC系数计数，并根据欲嵌入的秘密信息长度计算得到嵌入信息所使用的三元组(1, n, k)
  - 取出混洗后的非0的AC 系数及欲嵌入的比特信息，采用矩阵编码进行嵌入

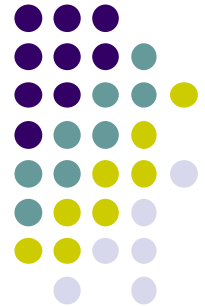
F5隐写

- 经过更改后的数据，判断是否产生了新的值为0的系数，若有，则此次嵌入无效，重新取出n比特数据(包含上次嵌入中没有改变的n-1比特和1比特的新数据)，重新嵌入，直到秘密信息全部嵌入
- 逆混洗，恢复DCT系数为原来的顺序

F5隐写

- 缺点
  - F5隐写算法嵌入秘密信息会发生系数收缩现象，DCT系数中的0会显著增加，块间的不连续性增加

MB(Model-Based)隐写



- Sallee于2004年提出
- 是隐写安全性研究与隐写方法设计的良好结合
- 基本思想
  - 将载体信号建模为由两部分组成的随机变量$X=(X_{\text{det}}, X_{\text{indet}})$，其中$X_{\text{det}}$和$X_{\text{indet}}$分别表示确定的和非确定的部分。隐写时，将只更改$X_{\text{indet}}$，从而保持它的分布不变，而且将确保隐密对象的非确定部分服从一定的分布模型。

MB隐写

- 计算确定部分的概率，并根据假设的模型，计算非确定部分相对确定部分的条件概率

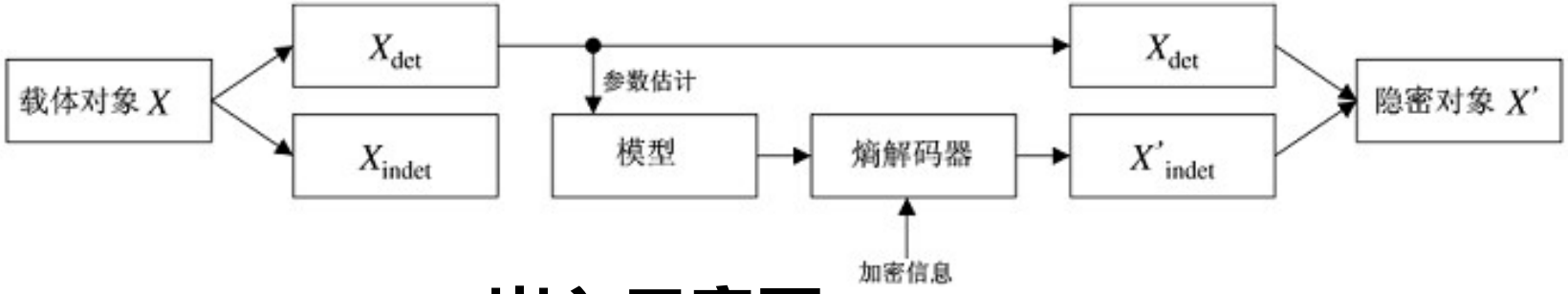
$$p(X'_{\text{indet}} \mid X_{\text{det}} = x_{\text{det}})$$

- 用熵解码器把均匀分布的秘密信息比特解码成服从上述条件概率分布的数据
- 用得到的数据替换X中的非确定部分，得到隐密对象

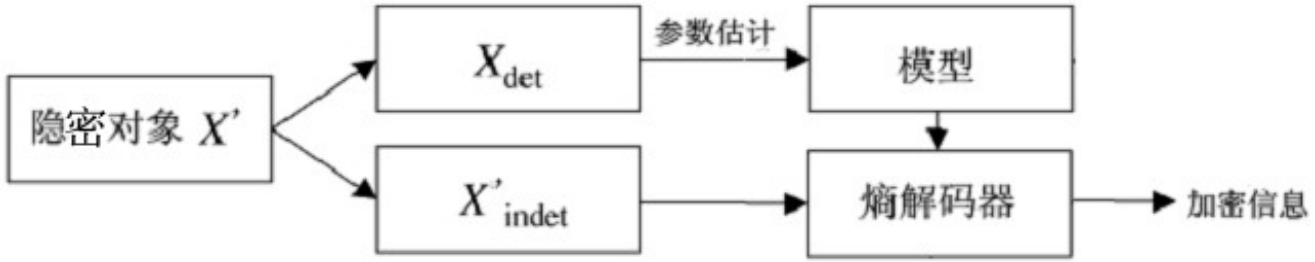
MB隐写

- MB隐写的平均最大容量为条件分布的熵：

$$H(X'_{\text{indet}} \mid X_{\text{det}} = x_{\text{det}}) = -\sum_{x'_{\text{indet}}} p_{X'_{\text{indet}}|X_{\text{det}}}(x'_{\text{indet}} \mid x_{\text{det}}) \log_2 p_{X'_{\text{indet}}|X_{\text{det}}}(x'_{\text{indet}} \mid x_{\text{det}})$$

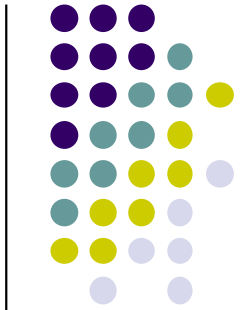


嵌入示意图



提取示意图

其它隐写



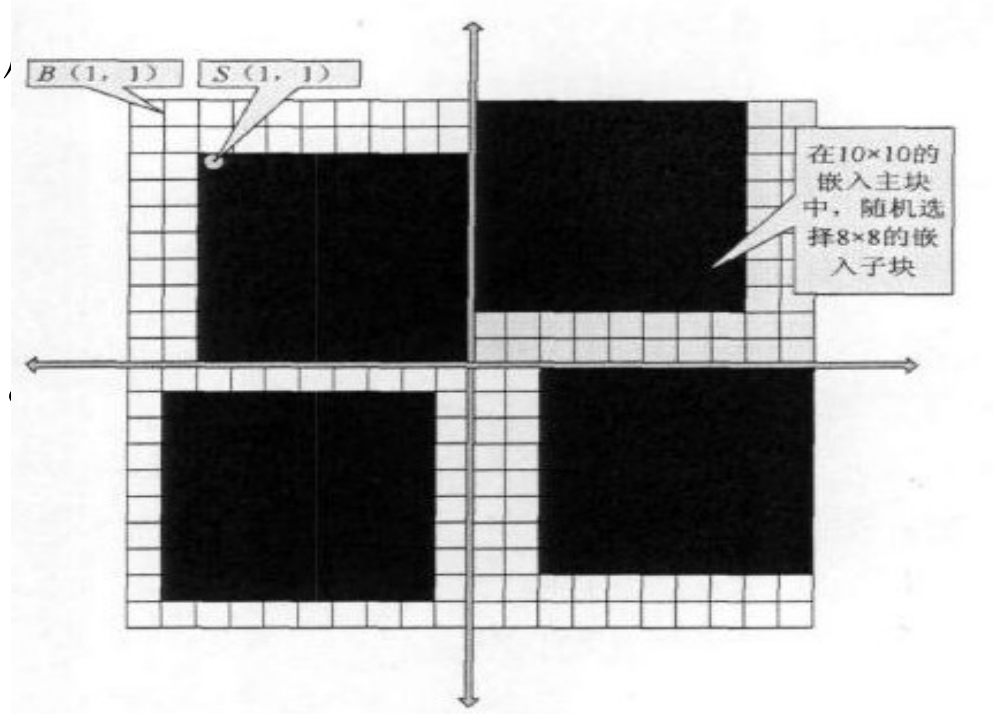
- -F5
  - 绝对值+1（F5，-1）
- nsF5（no-shrinkage F5）
  - 使用湿纸编码代替矩阵编码
- Steghide
  - 交换DCT系数（系数大小排列）

其它隐写

- 利用重量化的量化误差
- PQ（Perturbed Quantization）
  - PQe（energy-adaptive PQ）
  - PQt（text-adaptive PQ）
  - 湿纸编码
- MMx（Modified Matrix Encoding）
  - 矩阵编码

其它隐写

- **YASS（Yet Another Steganography Scheme)**
  - 不在DCT域嵌入(采用非8X8分块,随机嵌入)
  - 随机选n*n(n>8)块，在其中选择8*8嵌入后进行DCT变换
  - 可以抵抗用剪切的方法估计
- **YASS 隐藏方法不足：**
  - 影响密文的可靠提取
  - 重压缩方法，可以实现检测



需掌握的内容

- JPEG图像数据的数据组织形式是怎样的?
- JPEG图像信息隐藏分为哪几类?
- 当载体为JPEG图像时,为什么不用零系数嵌入?

休息中。。。

欢迎大家继续讨论！