2018-2019秋季
信息隐藏课程
第2讲 图像编码与基本嵌入方法

中国科学院信息工程研究所
INSITUTE OF INFORMATION ENGNEERING CAS

SKLOIS
信息安全国家重点实验室

赵险峰

中国科学院信息工程研究所
信息安全国家重点实验室

2018年9月

纲要

1. 图像编码格式
   - 空间编码格式
   - 变换域编码格式
2. 基本嵌入方法
3. 文献阅读推荐

1-1 空域编码图像

- 空域编码是指在图像空间域进行编码，也就是直接针对图像像素进行编码
- 主要分为光栅格式与调色板格式两种
- 一个图像编码标准往往包括多类编码方法，一个图像仅仅是其一类方法的实例。例如，常见的BMP（Bitmap）、TIFF（Tagged Image File Format）、PNG（Portable Network Graphics）均支持光栅格式与调色板格式编码，对这两种格式编码分别又支持多种具体编码方法
- 各类光栅图像往往还借助无损压缩减少图像尺寸。如，TIFF格式可以存储很多类型的图像，当存储彩色图像时，支持采用LZW压缩，当存储二值图像时，支持采用RLE（Run Length Coding）压缩；PNG采用DEFLATE压缩，它是LZ77与Huffman编码的结合

1-2 空域编码图像：光栅格式（1）

- 直接用数字阵列的形式存储图像像素，但对每个像素的色彩或亮度表示方法有明确的规定
- RGB色彩模型：每个彩色像素可以用对应红、绿、蓝三色的向量(R,G,B)表示，其中每个分量也称为通道。
  - 假设用 n 比特存储一个颜色分量，则$(R,G,B) \in \{0,1,\cdots,2^n-1\}^3$。典型地，常见的BMP、PNG与TIFF图像允许用8比特表示一个颜色分量，此时色彩总数为$2^{3\times 8}$，色深为3×8 比特；PNG与TIFF图像也允许采用16比特的颜色分量，此时的色彩总数为$2^{3\times 16}$
- 灰度图像与二值图像采用单通道的像素表达形式，因此，这类图像仅仅表达了亮度信息。根据三基色确定亮度的方法是
  - $Y = 0.299R + 0.587G + 0.114B$

1-3 空域编码图像：光栅格式（2）

- YUV模型：同时存在亮度分量Y和色度分量U、V，有利于直接显示灰度信号（$U = 0.492(B - Y)$，$V = 0.877(R - Y)$）

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

注：以上是ITU-T BT.601的定义，其他标准的同类模型有不同

- RGB每个分量用8比特表示，则取值范围在$[0,255]$之间，但是，以上YUV中除了Y分量在此范围取值外，U与V均可取负整数和正整数。为了统一取值范围为$[0,255]$，使得可以用1个8比特字节表示，定义以下YC_bC_r模型（TIFF、JPEG等采用）

$$\begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} = \begin{pmatrix} 0 \\ 128 \\ 128 \end{pmatrix} + \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.5 \\ 0.500 & -0.419 & -0.081 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

注：以上是JPEG等图像标准采用的YC_bC_r模型，其他标准的同类模型有不同

1-4 空域编码图像：调色板格式

- 对于卡通图、计算机图像等一些对色彩总数量要求较低的图像，采用调色板格式编码更加合适
- 这类编码方法也比较简单，特点是需要构造一个调色板，它是包括了全部色彩RGB表示的一张表，每个色彩按照排列次序有个索引值可以标定，图像像素仅仅包含相应色彩的索引值
  - 例如，当前调色板一般最多允许256个颜色，这样，**每个彩色像素用8比特存储索引值即可**
- 常用的调色板格式图像包括GIF格式，TIFF格式标准也包括调色板格式的存储形式

由索引值组成的像素

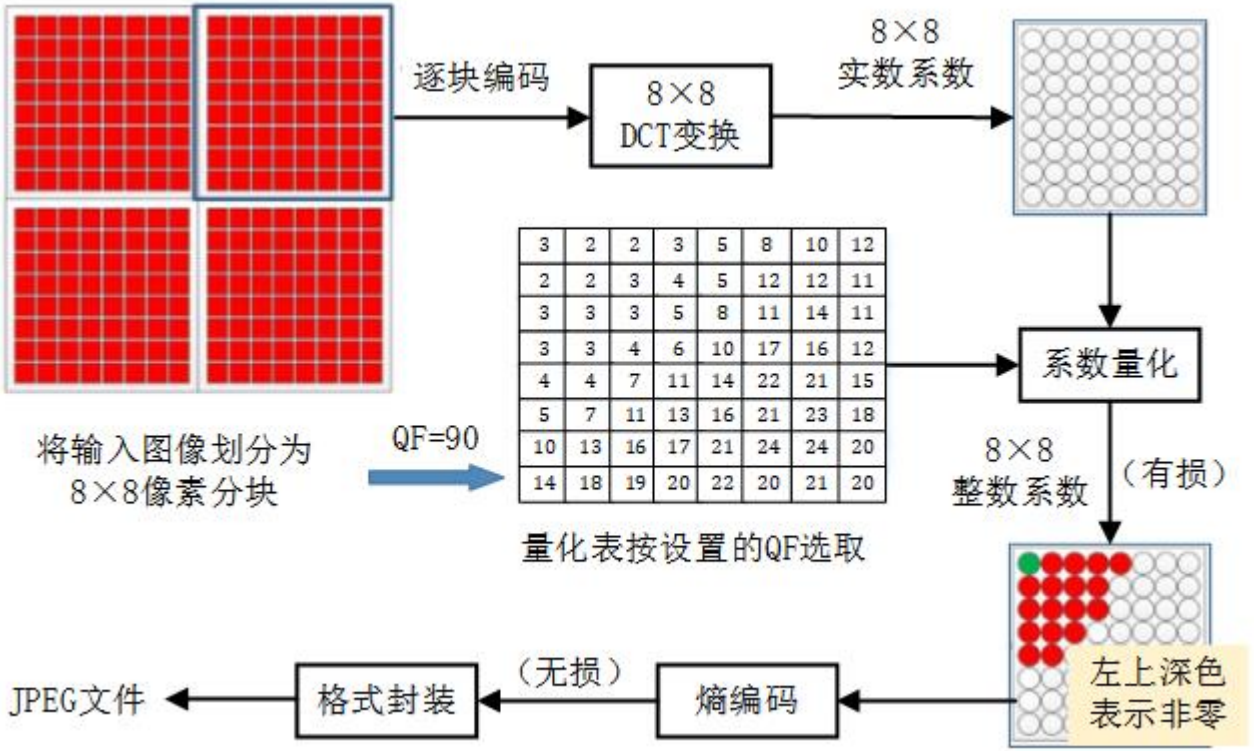
101	106	101	110	105	100
99	121	118	116	115	99
98	121	111	109	102	99
90	101	101	92	93	95
88	86	83	80	83	87

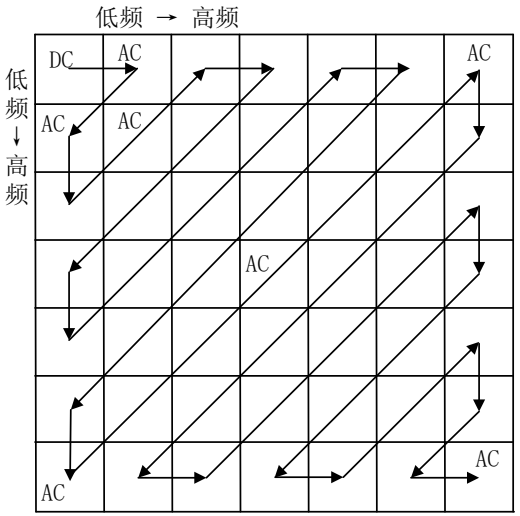
调色板

索引	RGB值
01	(R_1, G_1, B_1)
02	(R_2, G_2, B_2)
03	(R_3, G_3, B_3)
04	(R_4, G_4, B_4)
:	:
:	:
:	:
N	(R_N, G_N, B_N)

1-5 变换域编码JPEG图像：编码流程

- 变换域编码使用最多的是JPEG标准，它是联合图像专家组（Joint Picture Expert Group）制定的图像编码标准，特点是在变换域有损压缩编码，并采用无损压缩编码得到最后结果





1-6 变换域编码JPEG图像：编码步骤（1）

- YC_bC_r**格式化。JPEG编码的输入是**YC_bC_r**格式的空域图像信号，若输入不是该格式的图像则进行转换**
- **图像分块。将空域图像各个分量按照**8×8**像素的尺寸进行分块，如果图像不是分块尺寸的整数倍，需要向外扩充，这部分解码时不显示；考虑到人眼对亮度的敏感程度大于色彩，根据编码配置，编码器可对**C_b**与**C_r**分量进行下采样，使得一个**16×16**的宏块中包含4个Y分块，1、2或4个**C_b**或**C_r**分块，以进一步压缩尺寸（Y分量是常用的嵌入域）**
- **DCT（Discrete Cosine Transform）变换。将每个输入值从[0,255]的范围平移到[-128,127]，对每个分块进行**8×8**的二维DCT变换，得到**8×8**的DCT系数分块。分块中最右上角为直流（Direct Current，DC）系数，其他系数为交流（Alternating Current，AC）系数**

1-7 变换域编码JPEG图像：编码步骤（2）

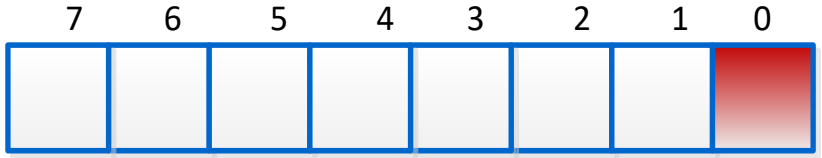
- **量化**。根据质量参数设置，将DCT系数按照相应的量化表进行量化，得到整数DCT系数分块；量化采用量化表，量化表中元素数值越大，对应着更大程度的有损压缩。由于高频系数数值较小，一般在这一步处理中有很多系数变为0，这是有损编码的核心步骤，它为提高下面无损压缩的压缩率打下了基础
- **无损压缩**。按照Zig-zag次序将64个DCT系数排列成一维序列，之后，对这个序列包含的比特流无损压缩：
  - 由于相邻块的DC系数接近，采用差分编码（DPCM）节省存储，只记录相邻块AC系数差
  - 对于63个AC系数，由于连续的数值多，采用行程编码；最后，对以上DPCM与行程编码再进行Huffman编码，加上文件头后，得到JPEG图像最终的文件存储形式
- LibJPEG开源工具包为操作JPEG文件提供了方便

纲要

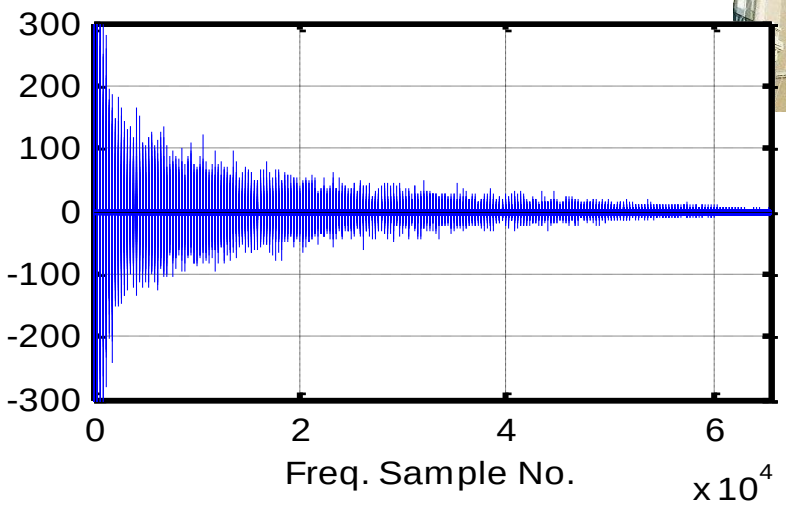
1. 图像编码格式
   - 空间编码格式
   - 变换域编码格式
2. 基本嵌入方法（尚达不到隐写安全需求）
   - LSBR
   - LSBM
   - 调色板图像嵌入
   - QIM
3. 文献阅读推荐

2-1 隐藏到哪儿？——嵌入域（整数、实数）

- 空间域像素（图像）、时间域样点（音频）



- 变换域系数（实数）



- 有损编码域（信号变换+系数量化+无损编码），如JPEG中的量化（整数化）后的分块DCT系数

需要有嵌入整数域或者实数域中的基本方法

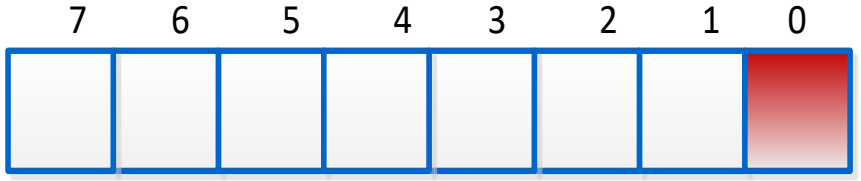
2-2 LSB替换嵌入：操作（二元嵌入编码）

- LSB替换（LSB Replacement，LSBR）是指，直接将载体嵌入域样点的LSB用待隐藏的秘密消息替换。JSteg是互联网上可下载的隐写软件，它在JPEG量化DCT系数上采用LSBR嵌入消息
- 若 $x=(b_n,\cdots,b_2,b_1)$表示一个载体样点值，其中b_1即为它的LSB，记 $\mathrm{LSB}(x)=b_1$，$x'=(b_n,\cdots,b_2,b_1')$为嵌入消息后的样点。若 w 表示待隐藏信息的一个比特，LSBR嵌入一个比特的操作可以用二进制运算表示为 $b_1'=w$，也可以用整数运算与GF(2)上运算分别表示为

$$x'=\begin{cases}x+w, & x\equiv 0(\mathrm{mod}\ 2)\\ x+w-1, & x\equiv 1(\mathrm{mod}\ 2)\end{cases} \qquad x,w\in Z$$

$$x'=\begin{cases}x+w, & x=0\\ x+w+1, & x=1\end{cases} \qquad x,w\in GF(2)$$

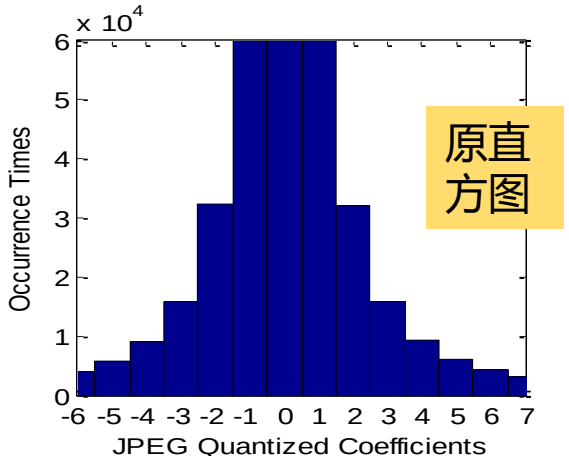
- 二元嵌入编码：x 被嵌入后，可能的状态有2个

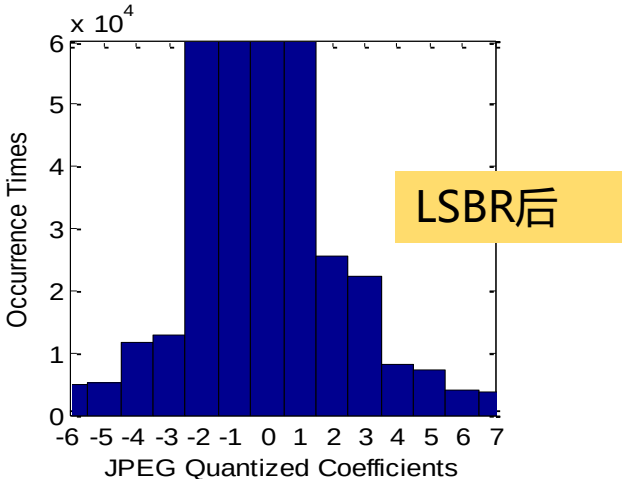


2-3 LSB替换嵌入：性质分析

- 由于多媒体在生成以及编码中均会引入噪声，使得LSB具备较强的随机性。这些噪声隐蔽了LSBR嵌入引入的噪声，使得在负载率一定的情况下，LSBR具有一定的安全性
- 但LSBR嵌入引入的统计特征变化也很明显：在载体的偶值点上数值只增不减，在奇值点上只减不增，如果负载率较高，这个特性使得相邻数值样点的个数接近，以后介绍的卡方（χ^2）特征将很准确地刻画这个变化；这样的奇偶相邻数值称为“值对”，例如对原始数值样点2与3，LSBR后，2只可能变为3，3只可能变为2，总有一个流入多于流出，使相邻数值更接近
- LSBR嵌入的嵌入效率约是2b/次修改

注：一个嵌入效率可以对应不同的负载率，例如，在以上2b/次嵌入效率下，隐写方案可以仅仅按照密钥选择100%或者50%的样点用于承载信息，则负载率分别是1bpp或者0.5bpp





2-4 LSB替换嵌入的变异

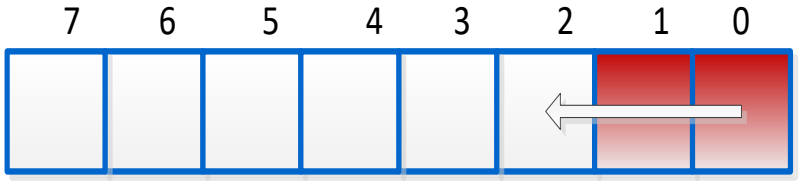
- 在以上嵌入中，一个偶数与其邻值奇数形成值对，其中，偶数的绝对值小，奇数的绝对值大，在一些情况下，需要反过来，这样，在需要修改的时候，可以对奇数绝对值加1，对偶数绝对值减1，称这样的LSBR为奇小偶大值对LSBR
- 实例：
  - JPEG量化系数是经常使用的嵌入域，其中，系数值有正有负，0值分布较多，为了不显著改变0值的出现频次，一般0、1与−1都不用于嵌入，这样最小的值对是2与3、−2与−3，奇小偶大值对LSBR的直接好处是，它可以使得1与2、−1与−2为最小值对，从而利用了分布较密的1与−1。下一讲将会看到，基于模型的隐写（MB，Model Based）采用了奇小偶大值对LSBR
- 显然，奇小偶大值对LSBR与原LSBR在主要性质上等价

2-5 LSB匹配嵌入：操作（三元嵌入编码）

- LSB匹配（LSB Matching，LSBM）嵌入有助于克服出现以上的 χ^2 特征。在LSBM嵌入中，也是用最后的LSB承载秘密消息，但是，当需要修改LSB的值时，LSBM嵌入时通过对样点值做随机的加减1。设$\pm$ 表示随机加减1，则有：

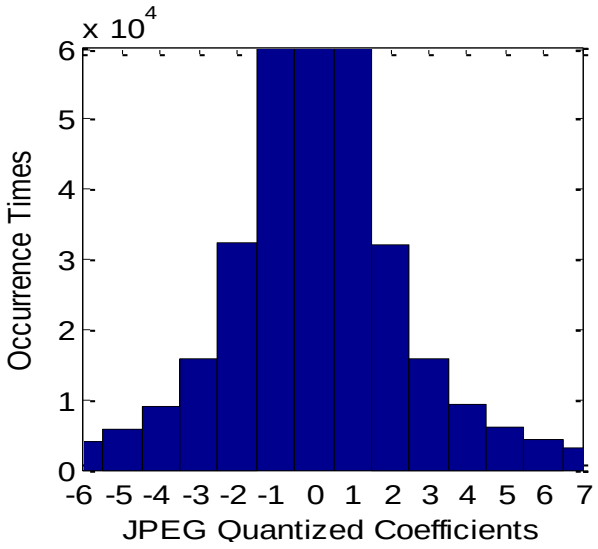
$$x' = \begin{cases} x \pm 1, & x \equiv 0(\mathrm{mod}\ 2),\ w = 1 \\ x \pm 1, & x \equiv 1(\mathrm{mod}\ 2),\ w = 0 \\ x, & x \equiv 0(\mathrm{mod}\ 2),\ w = 0 \\ x, & x \equiv 1(\mathrm{mod}\ 2),\ w = 1 \end{cases} \qquad x, w \in Z$$

- 虽然以上操作可能会影响次LSB（Second LSB）或者更高位平面的值，但是，修改的信号幅度仍与LSBR一样是1
- 三元嵌入编码： x 被嵌入后，可能的状态有3个

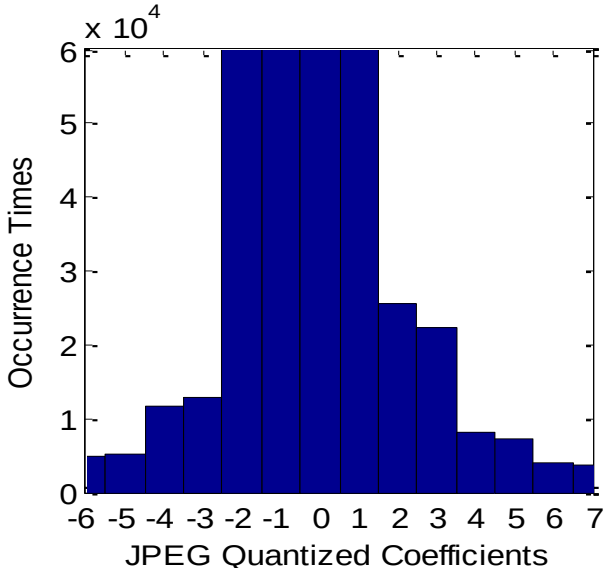


2-6 LSB匹配嵌入：性质分析

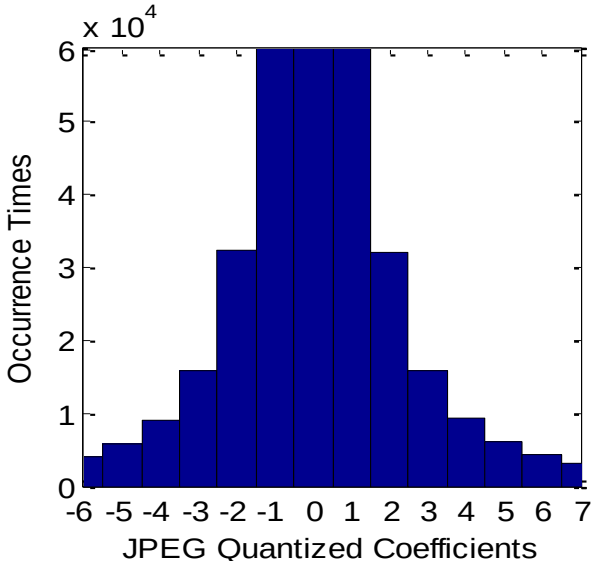
- 由于避免了相邻数值样点个数相互接近，在同等负载率下，LSBM隐写的安全性优于LSBR
- 但是，它们的嵌入效率都是2b/次。



原直方图



LSBR后



LSBM后

SKLOIS 信息安全国家重点实验室

2-7 调色板图像嵌入：初期方法

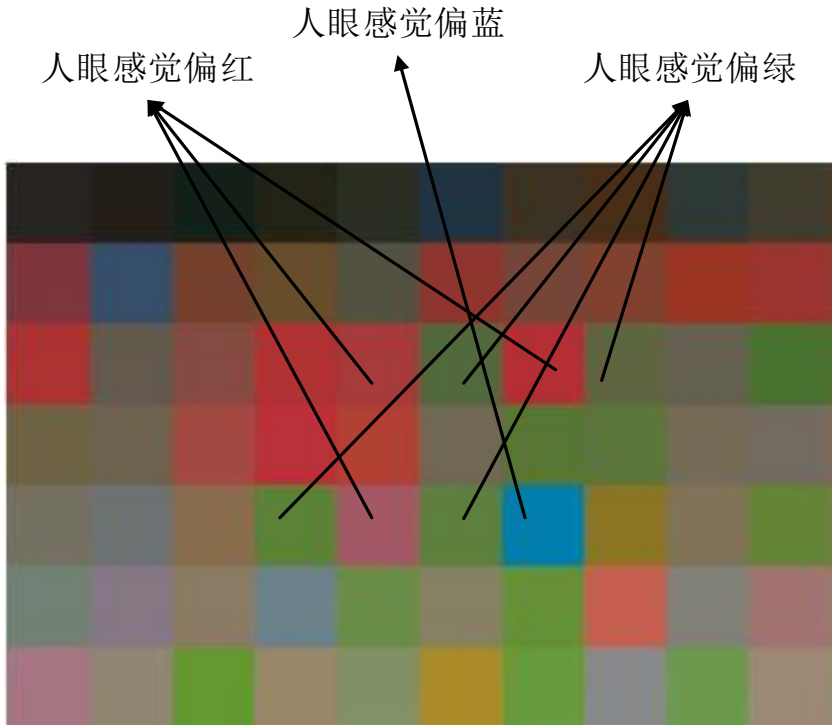
- Gifshuffle：直接用调色板中色彩的排列顺序表达消息，设调色板中颜色数为N，则可以表达的信息量为 $\log_2 N!$
  - 当 N=256，能够传输的消息长度约为210字节
  - 分析：一般调色板中颜色排序有一定规律，如参照了亮度、出现频度等因素，而以上随机排序使得调色板有显著的被处理特征
- 朴素的调色板项（索引值）奇偶分配，以支持类似的LSBR（问题归结奇偶分配问题）
  - 将调色板中初始颜色数量控制在128个，在对索引值进行LSBR中，为每个修改后的索引生成一个相邻颜色与索引编号，约定其与原来的颜色具有相反的奇偶性，这样颜色数量仍然不多于256个
  - 分析：大多数颜色一般在一个由2个数量更接近颜色组成的分组中
  - EzStego：先按照亮度排序调色板，再对索引值进行LSBR，实际亮度序号的奇偶性就是颜色的奇偶性
  - 分析：亮度值相邻的颜色可能很不相同，因此，隐写后的图像在色彩上存在显著的跳跃

2-8 调色板图像嵌入：分量和方法

- 显然需要更好地分配调色板颜色的奇偶性
- 分量和隐写定义了调色板颜色的距离，在需要修改的情况下，选择距离最短并且分量和最低位奇偶性不同的颜色替换

$$d_{\mathrm{RGB}}(c_i, c_j) = \sqrt{(r_i - r_j)^2 + (g_i - g_j)^2 + (b_i - b_j)^2}$$

- 但是，以上不能确保是用最邻近颜色的索引值替换



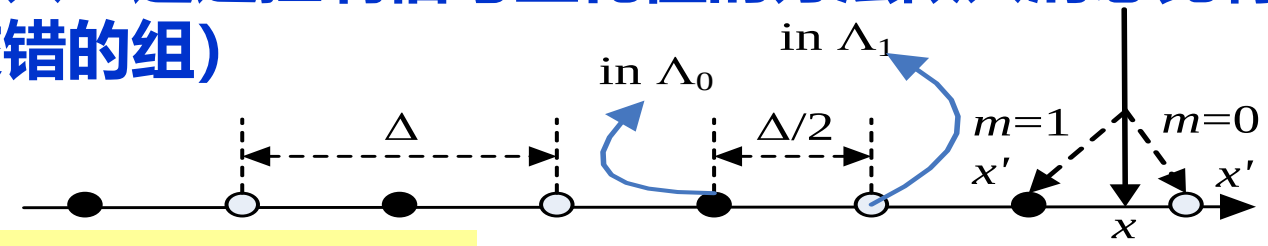
2-9 调色板图像嵌入：OPA方法

- c_i 的奇偶性以 $P(c_i)$ 表示，距 c_i 最近的颜色用 s_i 表示；OPA隐写通过以下奇偶分配使得 c_i 与 s_i 必定奇偶性不同：
- 最佳奇偶分配（Optimum Parity Assignment，OPA）隐写

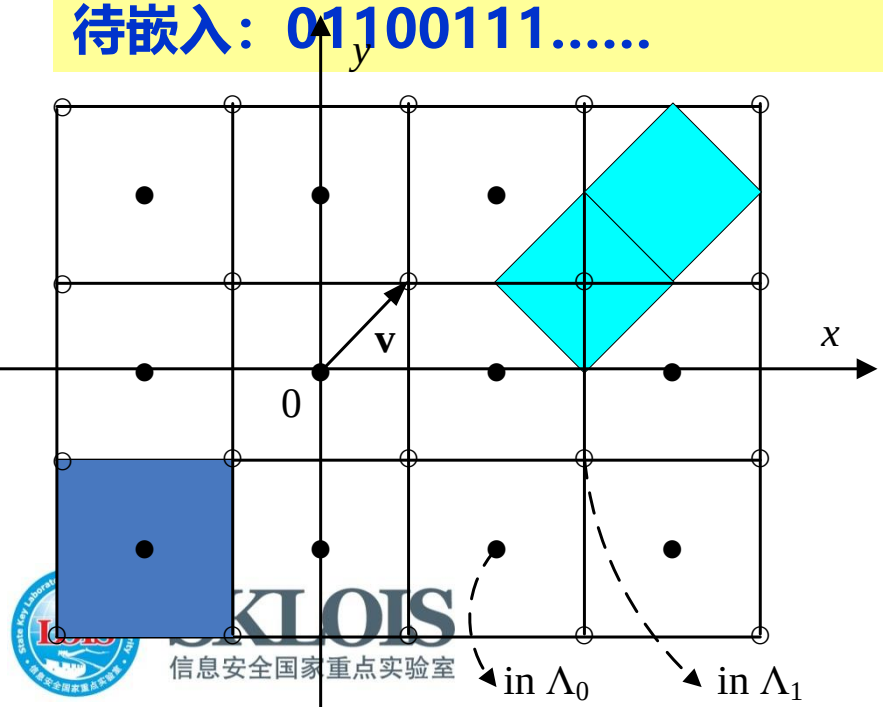
- 用以上公式计算所有颜色的距离 $d[i,j] \triangleq d_{RGB}(c_i, c_j)$；令P $= \{\emptyset\}$。
- 排序全部 $d[i,j]$，得到非递减序列 D $= \cdots d[u,v] \le d[k,l] \cdots$；对相等的距离，采用一定的方法使得 D 为唯一排序，例如按照颜色索引值的大小对相等距离排序。
- 反复执行以下步骤直到调色板中全部 N 个颜色都进入 P 中：
- 在 D 中选择下一个 $d[i,j]$，其中，$c_i \notin$ P 或者 $c_j \notin$ P，若没有这样的 $d[i,j]$ 了，说明 P 中已经包含了全部 N 个颜色，算法结束；否则：
- (a) 如果$c_i \notin$ P 且 $c_j \notin$ P，分配相反的奇偶属性给 c_i 与 c_j，P $=$ P $\cup \{c_i\} \cup \{c_j\}$。
- (b) 如果$c_i \notin$ P 且 $c_j \in$ P，则令 $P(c_i) = 1 - P(c_j)$，P $=$ P $\cup \{c_i\}$。
- (c) 如果$c_i \in$ P 且 $c_j \notin$ P，则令 $P(c_j) = 1 - P(c_i)$，P $=$ P $\cup \{c_j\}$。

2-10 量化调制嵌入：思想

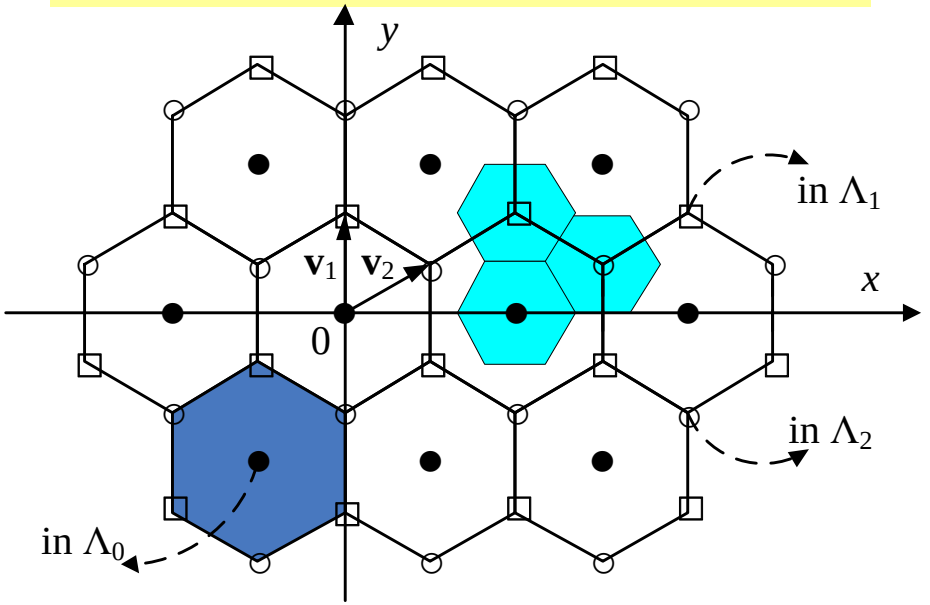
- 在信号量化中，格的作用是用最接近的格点值代替采样得到的实数信号值，实现用离散的样点代替连续信号；标量量化与矢量量化（信号量化中各个点作用一样）
- 量化调制嵌入：通过控制信号量化值的方法嵌入消息比特（分为不同类点交错的组）



待嵌入：01100111.....

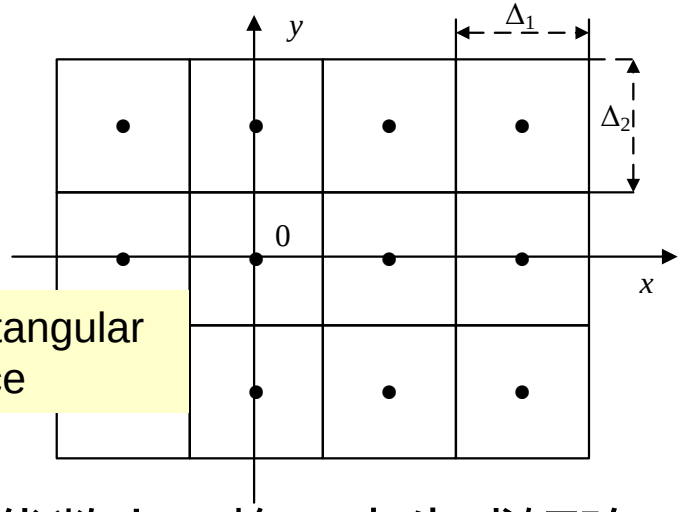


待嵌入：011202102 .....

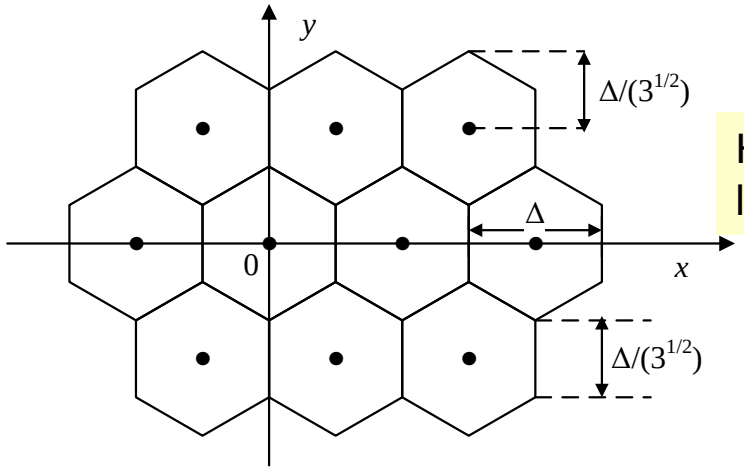


2-11 基础：格（Lattice）与量化（Quantization）

- 几何上，格由欧式空间中连续堆砌的形状单元（Voronoi cells）中心点组成。针对一个输入，量化器选择一个最近的格点作为输出



Rectangular lattice



Hexagonal lattice

- 代数上，格可由生成矩阵 G 定义

$$\boldsymbol{x} = (z_1, \cdots, z_L) \cdot \begin{pmatrix} \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_L \end{pmatrix} = \boldsymbol{z} \cdot G \in \Lambda$$

一个格的**G**是确定的

2-D Hexagonal lattice

$$\mathbf{g}_1 = (\Delta, 0) \quad \mathbf{g}_2 = (\Delta/2, \Delta\sqrt{3}/2)$$

L-D Rectangular lattice

$$\mathbf{g}_1 = (\Delta_1, \cdots, 0),\ \mathbf{g}_2 = (0, \Delta_2, \cdots, 0),\ \cdots,\ \mathbf{g}_L = (0, \cdots, \Delta_L)$$

2-12 量化调制嵌入：格、子格与陪集

- 格（Lattice）是N维欧式空间R^N中数值点组成的加群，由有规律分布于整个空间的离散点组成
- 每个点是一个基本单元（Voronoi Cell）的中心，这些单元规则排列并均匀覆盖整个空间，其中，相邻格点的距离相同，一般称为量化阶（Step Size），记为 Δ
- 为了利用量化调制嵌入 p 元编码信息，需要将一个格分化为 p 个子格（Sublattice）陪集（Coset）：
  - 若在格 Λ_{All} 中均匀等距地取格点组成子集 Λ_0，若Λ_0是加群，则它是一个子格；若果存在距离偏移 $\{\boldsymbol{v}_0 = \mathbf{0}, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{p-1}\}$，使得p个 $\Lambda_i = \Lambda_0 + \boldsymbol{v}_i$ 等距交错，并且它们是Λ_{All}的划分，则 Λ_i （包括Λ_0）是Λ_0的陪集

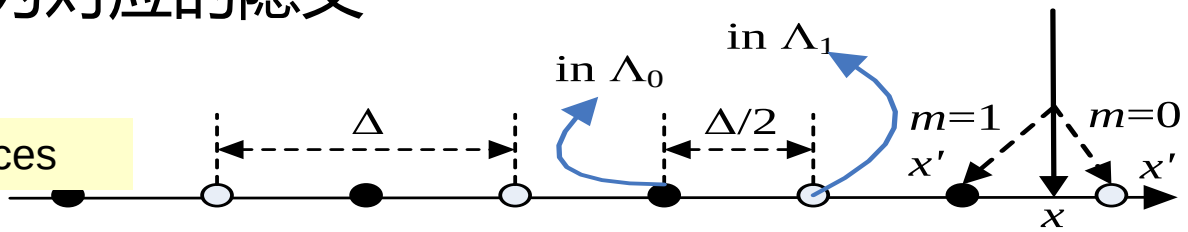
2-13 基本的量化嵌入——QIM

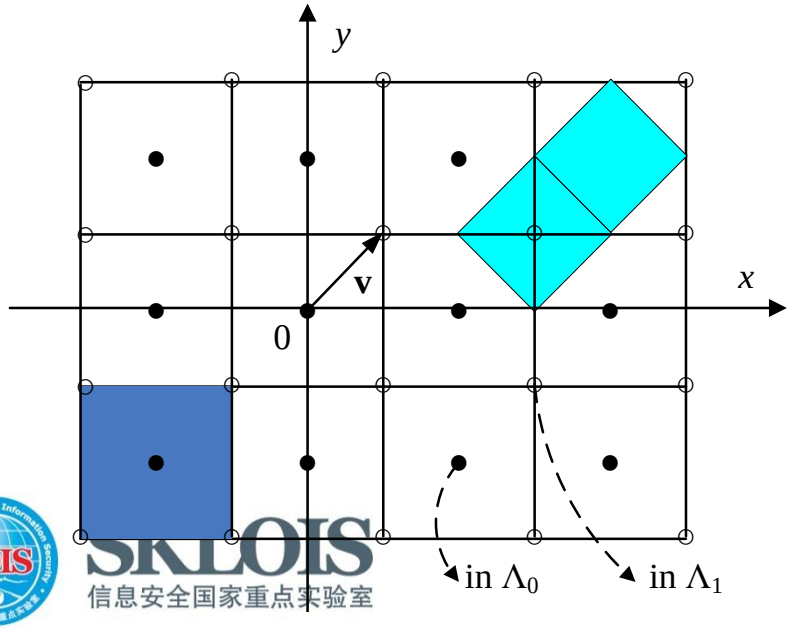
- 若c是一个原载体向量（分组），s 是相应的含密分组，QIM (Quantization Index modulation)采用 p 个格分别嵌入 p 个符号:

$$\mathbf{s} = Q_m(\mathbf{c}),\ m \in \mathcal{M} = \{0, 1, \cdots, p-1\}.$$

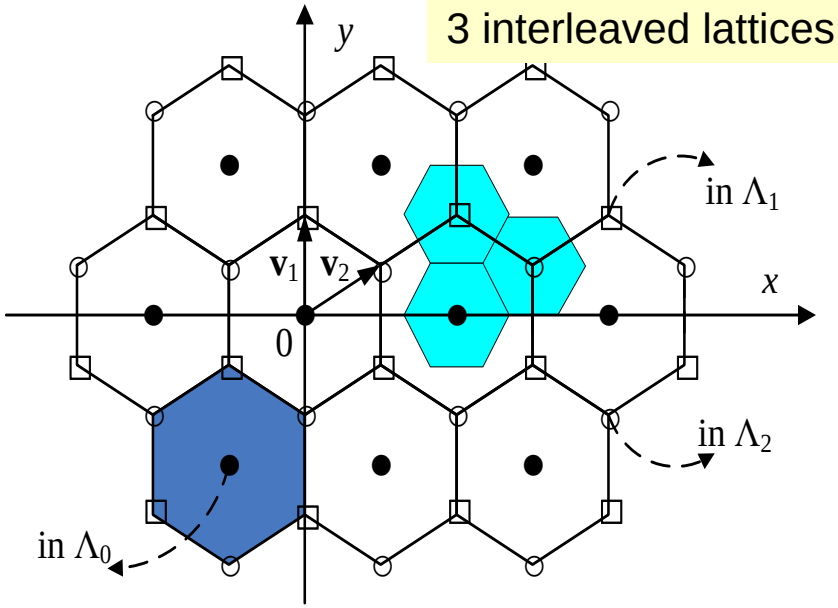
$Q_m(\cdot)$： 专门用于嵌入 m。 针对输入 c，它选择格Λ_m中离 $\boldsymbol{c}$ 最近的点 $\boldsymbol{s}$ 作为对应的隐文

2 interleaved lattices





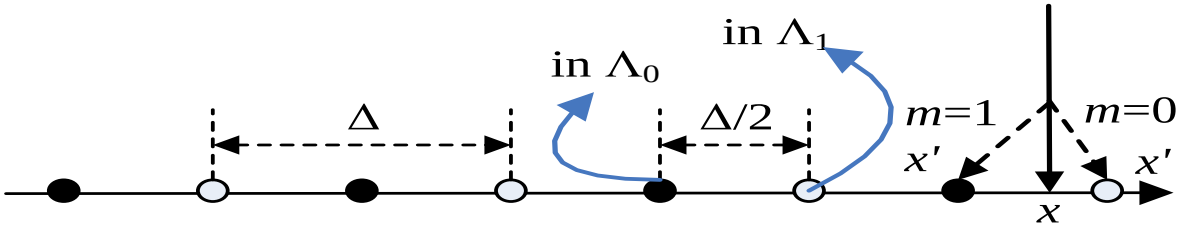
3 interleaved lattices

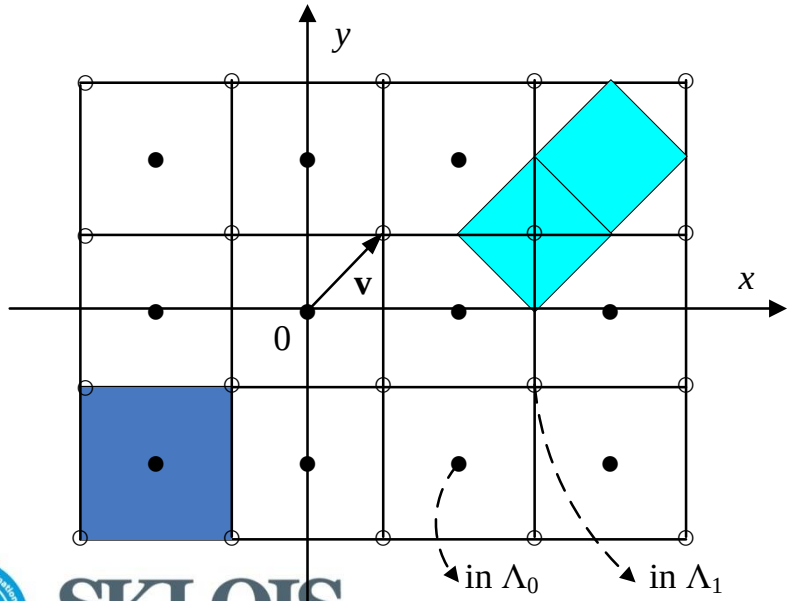


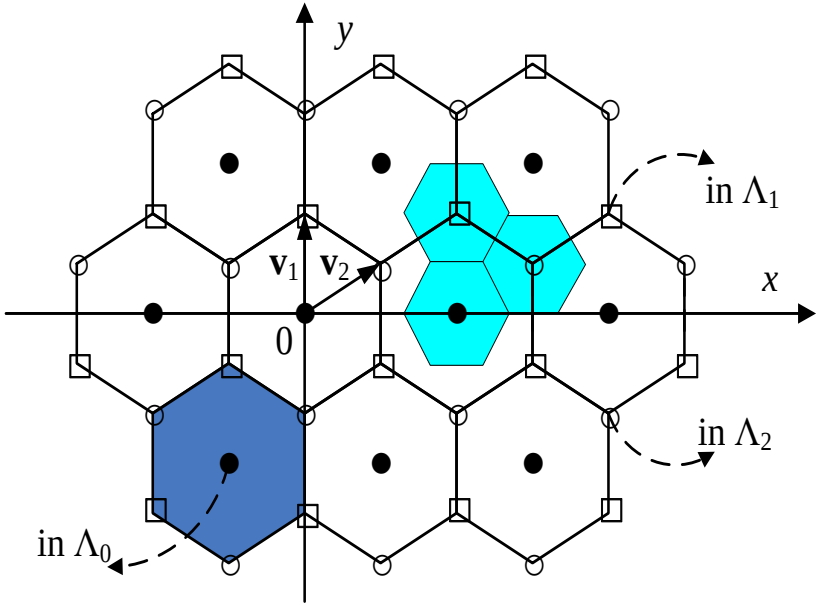
2-14 QIM嵌入的提取

- 若 y 是接收到的 s, 提取操作首先确定距离 y 最近的格Λ_m ， 输出m作为本次操作提取的消息符号

$$\hat{m} = \arg_{m \in \mathcal{M}} \min \ \mathrm{dist}\left(\mathbf{y}, \Lambda_m\right),$$

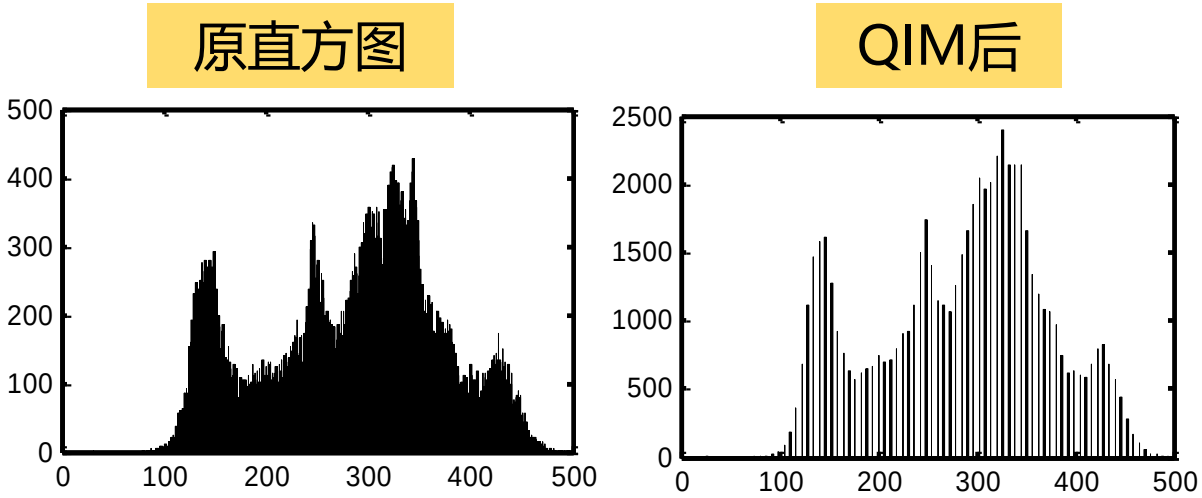






2-15 量化调制嵌入：QIM性质及其提高

- QIM理论具有很强的一般性意义
- QIM引入量化效应，数值数量下降，可以认为是一种隐写特征



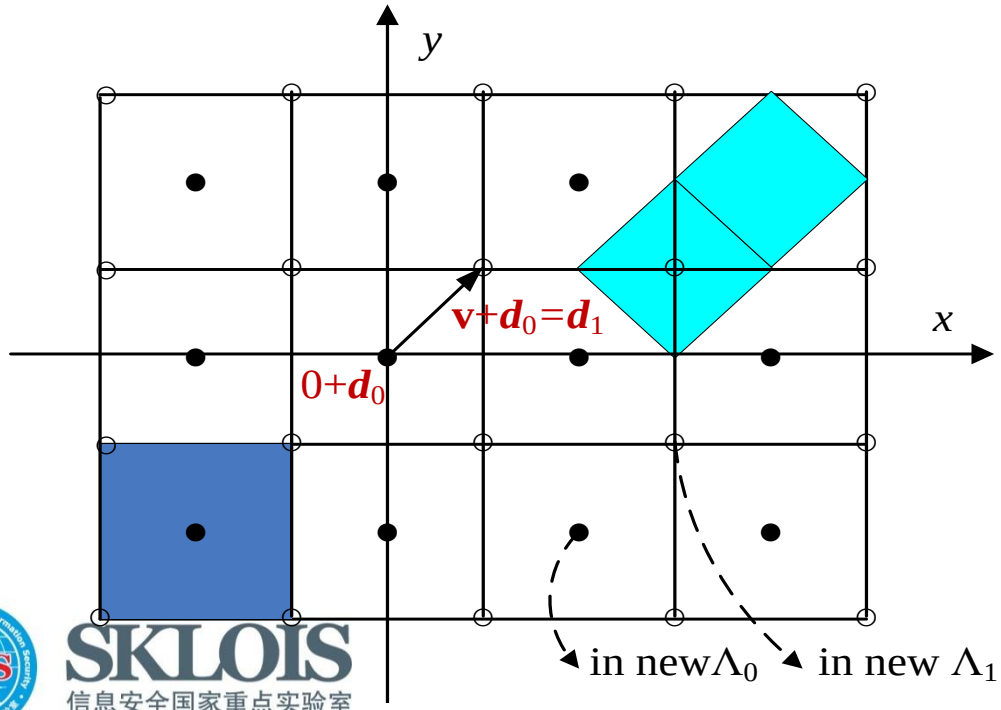
- DM（Dither Modulation）与DC-DM （Distortion Compensated DM）通过保密平滑移动格位置与加回部分量化噪声等手段，加强了QIM的安全以及其在安全性与鲁棒性间的平衡能力

2-16 提高的QIM, Dither Modulation (DM)

- 由于$s \in \Lambda_m$, QIM减少了样点值数量, 很容易被发现存在隐写，量化步长也容易估计；非授权者甚至可提取嵌入的秘密消息
- DM通过将格秘密移动 $\boldsymbol{d}_m$（抖动向量），克服了以上缺点

$$\mathbf{s} = Q_m(\mathbf{c}) = Q(\mathbf{c} - \mathbf{d}_m) + \mathbf{d}_m,\ m \in \mathcal{M},$$

在提取中，Λ_m 是移动后的格. $\hat{m} = \arg_{m\in\mathcal{M}} \min\ \mathrm{dist}(\mathbf{y}, \Lambda_m)$,



为了保持几何特性，抖动向量之间的差需要保持一定。因此只有一个$\boldsymbol{d}_m$可以作为密钥

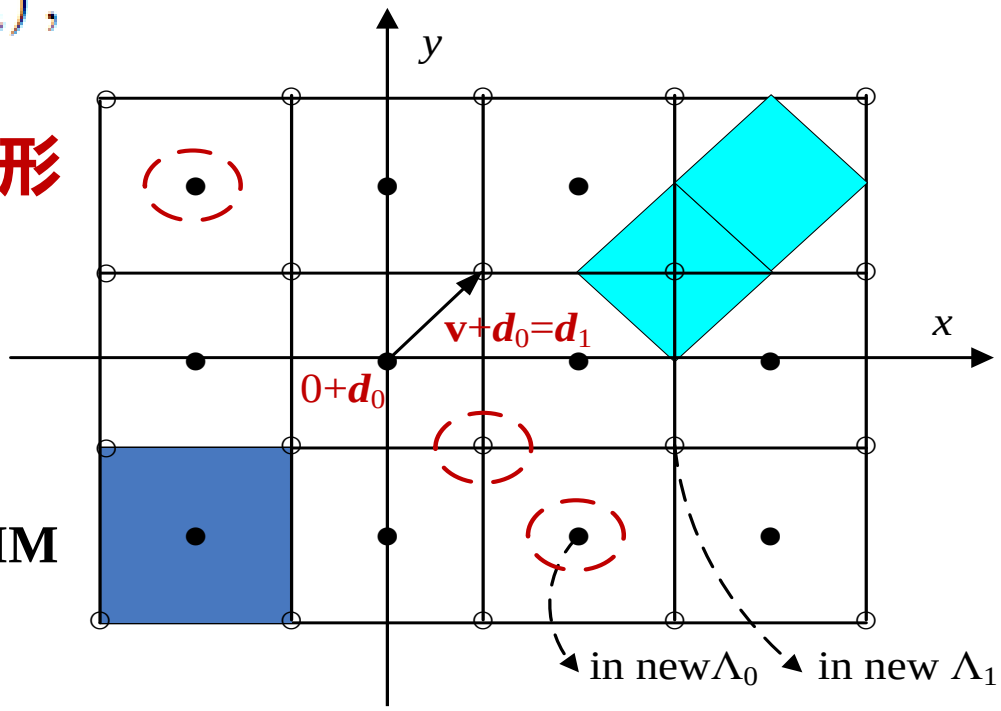
2-17 DC (Distortion Compensation)-QIM 或者 -DM

- 在QIM 或 DM中, 最后添加的信号是量化噪声 $\boldsymbol{q} = Q_m(\boldsymbol{c}) - \boldsymbol{c}$. 为了在感知代价与鲁棒性之间有一定的平衡，DC 仅仅添加一部分量化噪声 $\alpha\boldsymbol{q}$:

$$\begin{aligned}\mathbf{s} &= Q_m(\mathbf{c},\alpha) = Q_m(\mathbf{c}) + (1-\alpha)[\mathbf{c} - Q_m(\mathbf{c})] \\ &= \mathbf{c} + \alpha(Q_m(\mathbf{c}) - \mathbf{c}).\end{aligned}$$

$$\hat{m} = \arg_{m\in\mathcal{M}} \min \operatorname{dist}(\mathbf{y}, \Lambda_m),$$

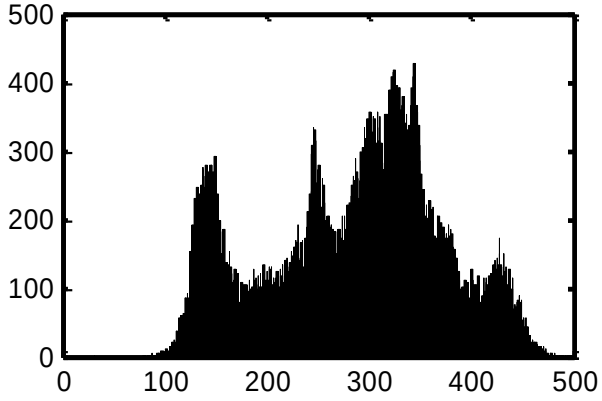
- **DC-DM 是量化嵌入的一般形式:**
  - 若 $\boldsymbol{\alpha = 1}$, **DC-DM 是 DM**
  - 若 $\boldsymbol{\alpha = 1}$ 且 $\boldsymbol{d_0 = 0}$, **DC-DM 是 QIM**
  - 若 $\boldsymbol{d_0 = 0}$, **DC-DM 是 DC-QIM**



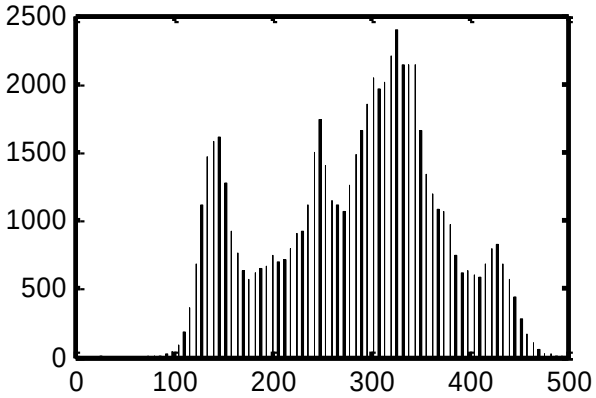
2-18 量化调制嵌入：QIM性质及其提高

- 理论具有很强的一般性意义
- QIM引入量化效应，数值数量下降
- DM（Dither Modulation）与DC-DM （Distortion Compensated DM）通过保密平滑移动格位置与加回部分量化噪声等手段，加强了QIM的安全以及其在安全性与鲁棒性间的平衡能力

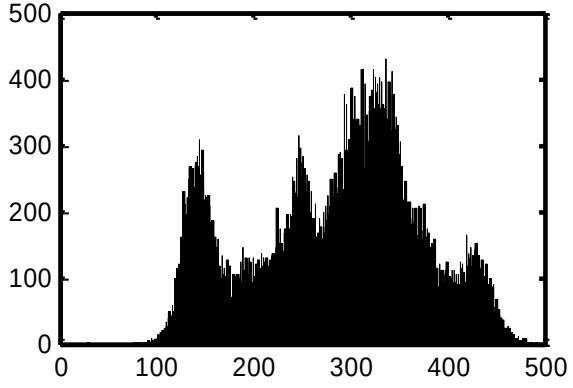
原直方图



QIM后



DM后



3 文献阅读推荐

- 教材第2章
- 推荐参考书的相关内容
- 关于图像格式的资料： JPEG File Interchange Format (JFIF)
- B. Chen, G. W. Wornel. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans. Info. Theory, 47(4): 1423–1443, May 2001
  - 注：描述了量化索引调制（QIM）及其提高方法

谢谢！

中国科学院信息工程研究所
INSITUTE OF INFORMATION ENGNEERING CAS

SKLOIS
信息安全国家重点实验室