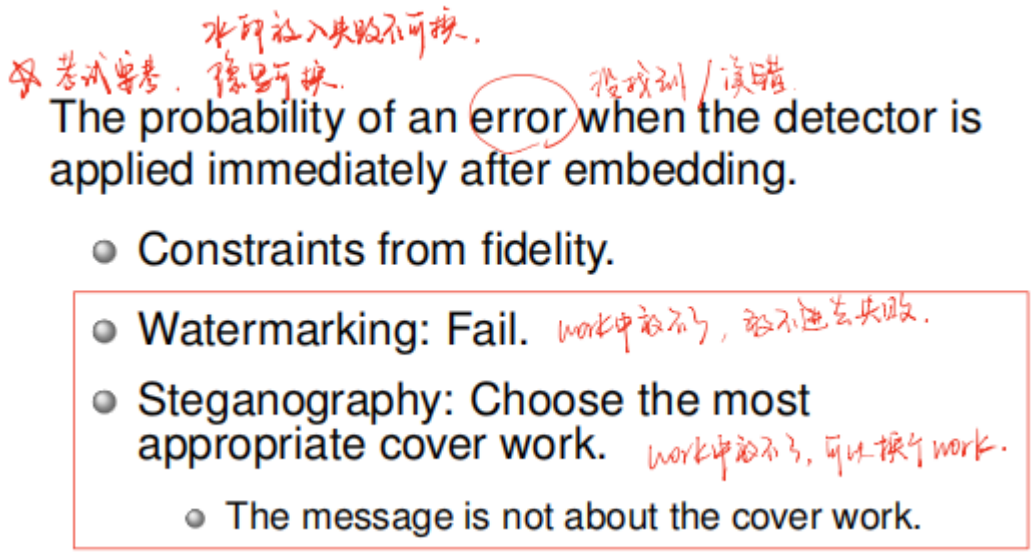
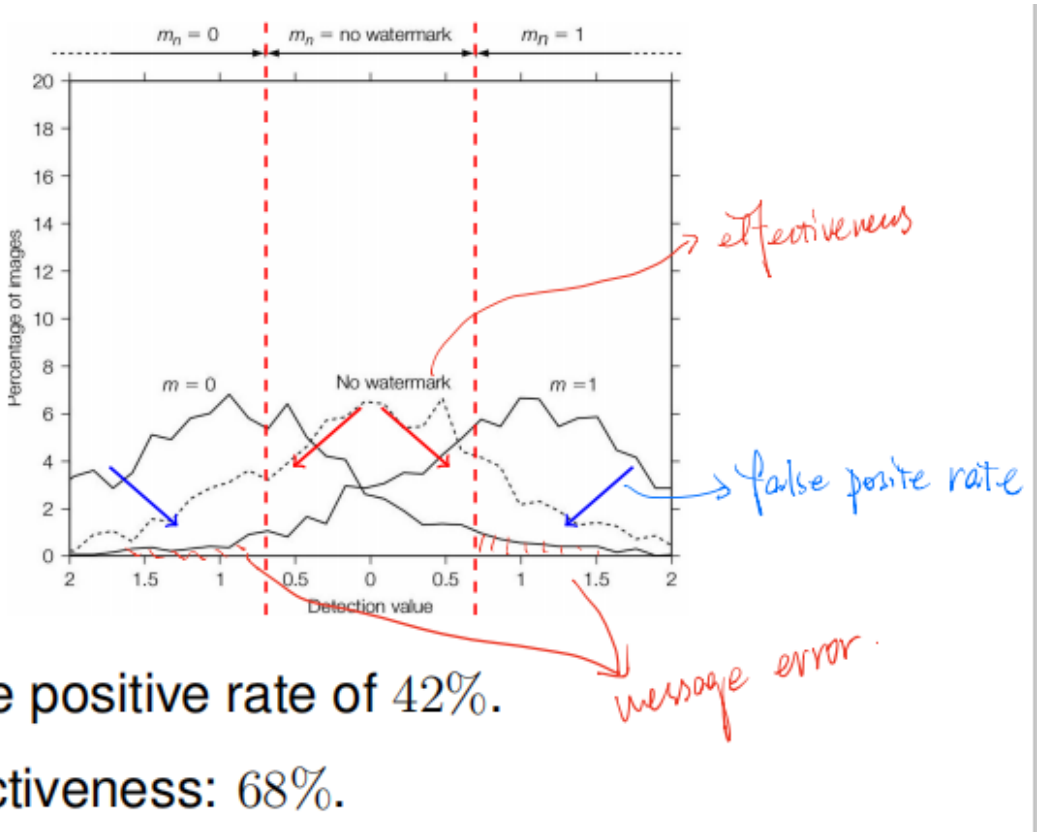
水印REVIEW

上课强调的考点

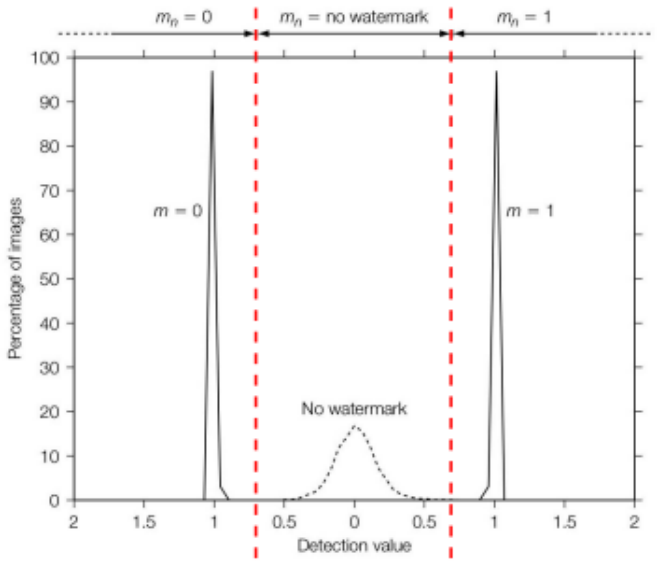
- 水印和work有关联，隐写术和work无关联
-



- 看图，画fpr effectiveness merror区域



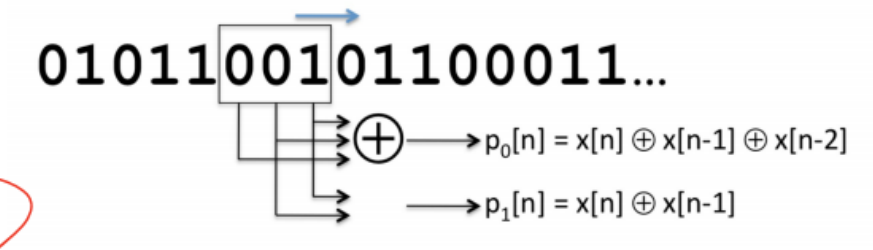
- 判断题如下图，fpr与编码方式无关

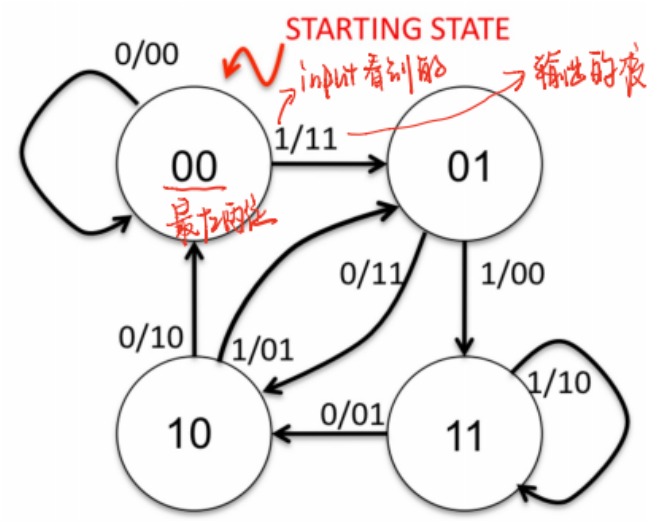


- False positive rate of 0.01%.
- Effectiveness: 100%.

- What is the minimal length of a sequence that can be used as ECC for a length L binary sequence with h bit error tolerance.

- Trellis code

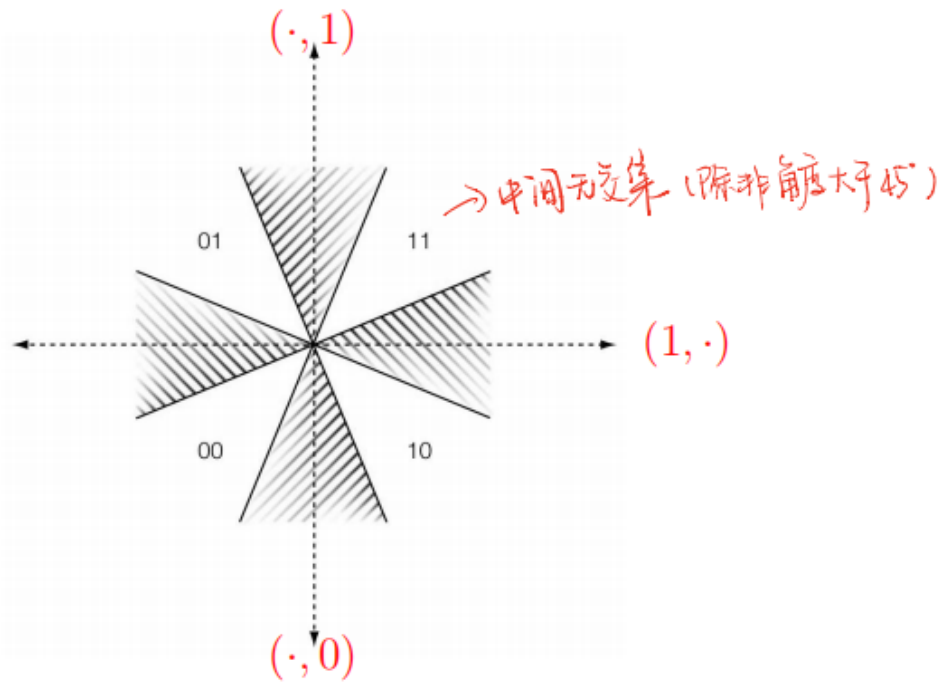




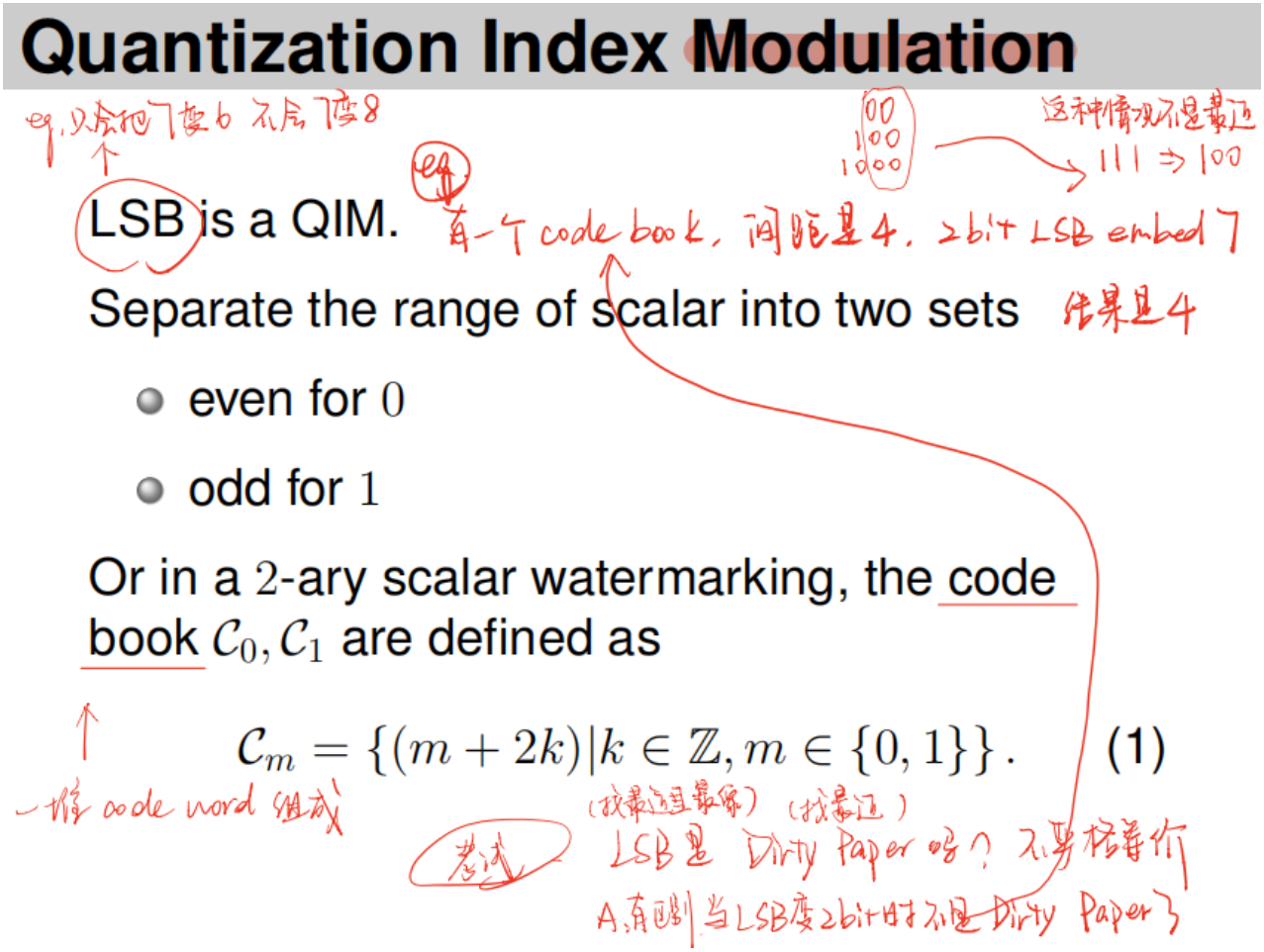
- 解释无交集原因

Large threshold: no overlap for the cones.

- No detectable 2-bit message.



- 考试中可能会不是考计算而是考（对水印和work都用高斯白噪声，得到fpr曲线图，问图更适合描述随机水印还是随机work）
- effectiveness=100%不代表detector=100%，传输过程中会有噪声

- 给出几张performance图，分类robustness side information embed（哪个图的robustness比较好，给出直观解释包括大体画出投影点）
- 

- 考试会有LSB和QIM

Question: QIM

Encoding 2-bit message.

	163	434	249	174
0				
1				
3				

The left most column is the message, the top row is the cover. Fill the embedding results.

直播 "IH" 。

N-Dimensional Lattice

考试：LSB 对应的是什么 lattice code。

A：LSB 中 reference pattern 是一个 bit 1 其余都是 0

Can be 2^N messages

- Encoded as length N binary sequences.

How about use template sub-lattice $(h\mathbf{w}_{\mathbf{r}1}, \cdots, h\mathbf{w}_{\mathbf{r}N})$ for $h = 3$?

3^N

考试：设计 lattice code book.

2-Dimensional Case

- Choosing two bases $\mathbf{X}_1, \mathbf{X}_2$.
- Get coordinates x_1, x_2.
- Evaluate the length and angle:

$$r = \sqrt{x_1^2 + x_2^2}, \quad \theta = \arctan(x_1/x_2).$$

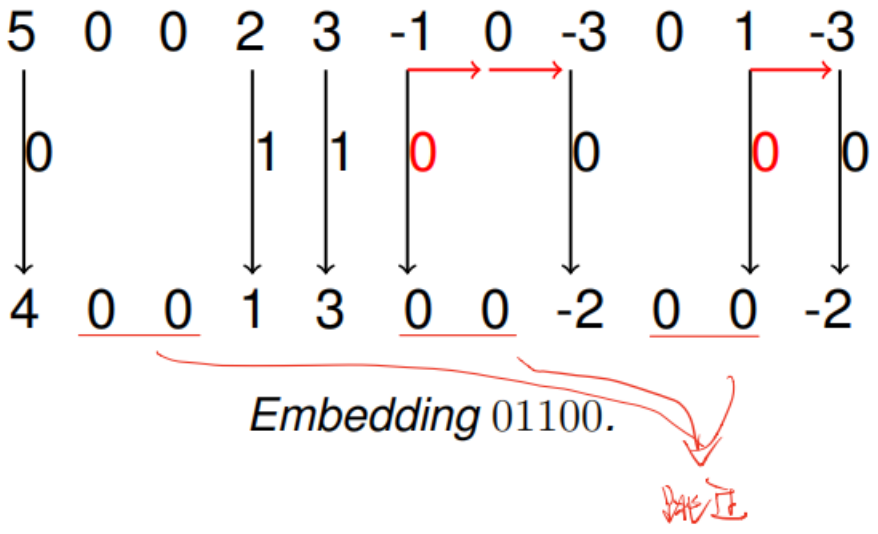
- Angle QIM:

$$\theta^Q = Q_{m,\Delta}(\theta) = \left\lfloor \frac{\theta + m\Delta}{2\Delta} \right\rfloor 2\Delta + m\Delta.$$

- Restore:

$$x_1' = r\cos(\theta^Q), \quad x_2' = r\sin(\theta^Q).$$

F3 Algorithm



More Efficiency?

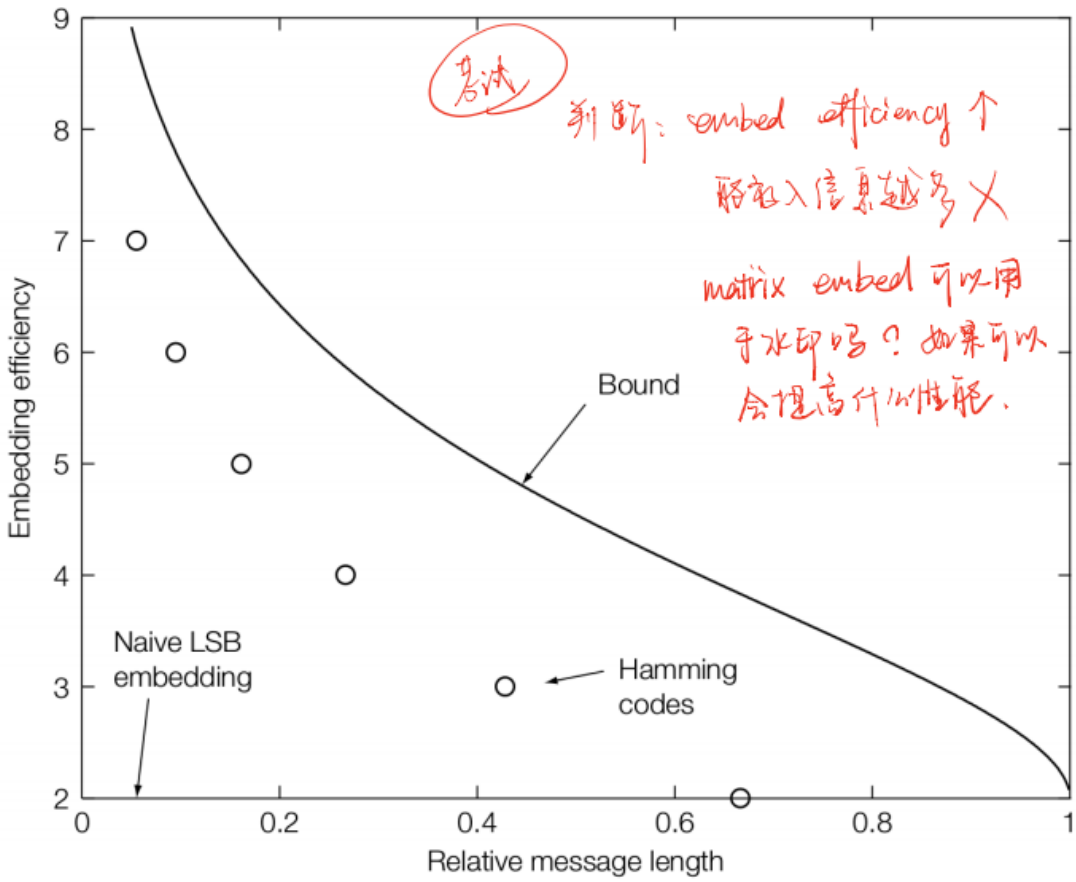
考：5% shrinkage 那实际上会有多少 change
A: 5% + 95%/2 = 52.5%.

Example: Embedding 1736 bits

- F4: 1157 changes.
- F5: 459 changes by matrix encoding.
  - Embedding efficiency: 3.8 bits per change.

可能考F5.

Illustration



考试

判断：embed efficiency 个
嵌入信息越多 X

matrix embed 可以用
于水印吗？如果可以
会提高什么性能.

考试 不会解方程，记到 H 即可 or 简单数字.

$$\mathbf{Dv} = \mathbf{m} - \mathbf{Dx} = \mathbf{z}$$

$$(\mathbf{DP}^{-1})(\mathbf{Pv}) = \mathbf{z}$$

$$(\mathbf{H} \quad \mathbf{K}) \begin{pmatrix} \mathbf{u} \\ 0 \end{pmatrix} = \mathbf{z}$$

$$\mathbf{H}_{m \times |\mathcal{J}|}\mathbf{u} = \mathbf{z}.$$

线代 m >> 了 无解 ⇔ 信息多，drop

水印

Choosing the solution with the minimal number of changes.

CHAPTER 1 Introduction

水印和隐写术的定义

- Watermark: imperceptible message about the work.

水印 每个人都能看出来 信息和work强相关

- Steganology: undetectable and secret message in the work.

隐写 不可检测出来 信息和work不一定相关

四类信息隐藏

	Cover Work **Dependent**	Cover Work **Independent**
Existence **Hidden**	Covert Watermarking	Steganology
Existence **Known**	Overt Watermarking	Overt Embedded Communications

应用场景&为什么不用加密技术

- Watermarking
  - Copy prevention and copy-right protection.
  - Why not cryptography? it can protect content in transit, but once decrypted, the content has no further protection. 解密后可拿到原版.
  - ...
- Steganology
  - Terrorists
  - Crime
  - Political

CHAPTER 2 Applications and Properties

1. Features/performance

Features/performance of watermarking

- Features: Compare to other descriptors (e.g. bar code, meta info etc.).
  - Imperceptible.
  - Inseparable.
  - Transform along with the work.
- Performance: Importance depends on the application.
  - Robustness: how well watermarks survives.
  - Fidelity: how imperceptible the watermarks are.
  - ...

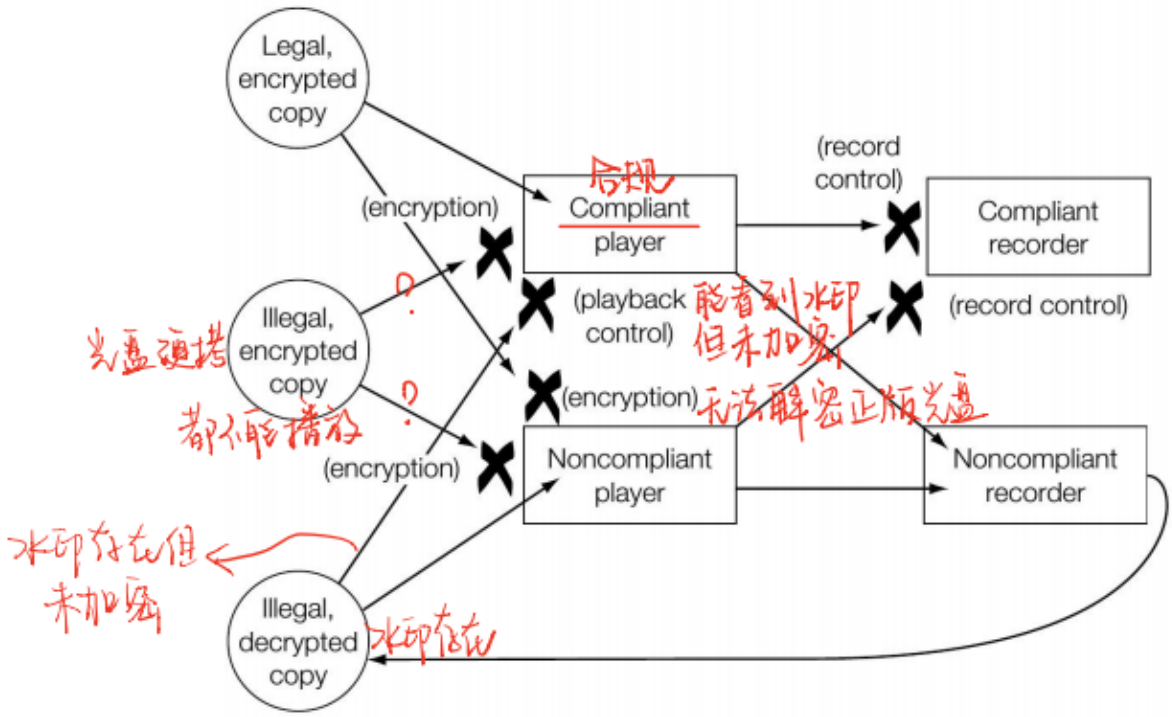
Features/performance of steganography

- Features: Compare to encryption.
  - Hiding the presence/communicating
- Performance: The balance depends on the application.
  - Statistical undetectability: how difficult it is to detect the existence.
  - Steganographic capacity: the maximum payload without causing statistically detectable artifacts.
  - ...

---

2. 应用

- Watermark
  - Broadcast Monitoring （passive/active）
  - Owner Identification
  - Proof of Ownership （别人不能轻易移除，也不能轻易检测出来，eg. 公私钥）
  - Transaction Tracking（英国内阁那个例子）
  - Content Authentication（没有被篡改）
  - Copy Control（没有被刻录）



解决盗版办法：水印 → 破解水印 → 申请专利

- Device Control（和设备兼容，eg. 水印控制音画同步，interactive TV）

- Steganography
  - Dissidents（知道自己被监控）：加密（逮捕）；匿名发送（保护发送方）；隐写（benign）
  - Criminal（不知道自己被监控）：加密（推断同谋）；匿名发送（法律）；隐写（查封计算机）【更容易实现隐写术】

---

3. 属性

- Watermark
  - Embedding：fidelity；Data Payload
  - Detection
    - Blind/Informed（blind无原图，informed有原图）
    - false positive（关于pre，随机水印比随机work准确率高的原因：水印模式人为生成规律比较简单，work模式是自然界照片or图像，找模式规律比较难）
    - Robustness

      benign对应robustness，hostile对应security
  - Security
    - watermark角度

      Unauthorized removal: active attacks Unauthorized embedding: active attacks Unauthorized detection: passive attack
    - cover work角度

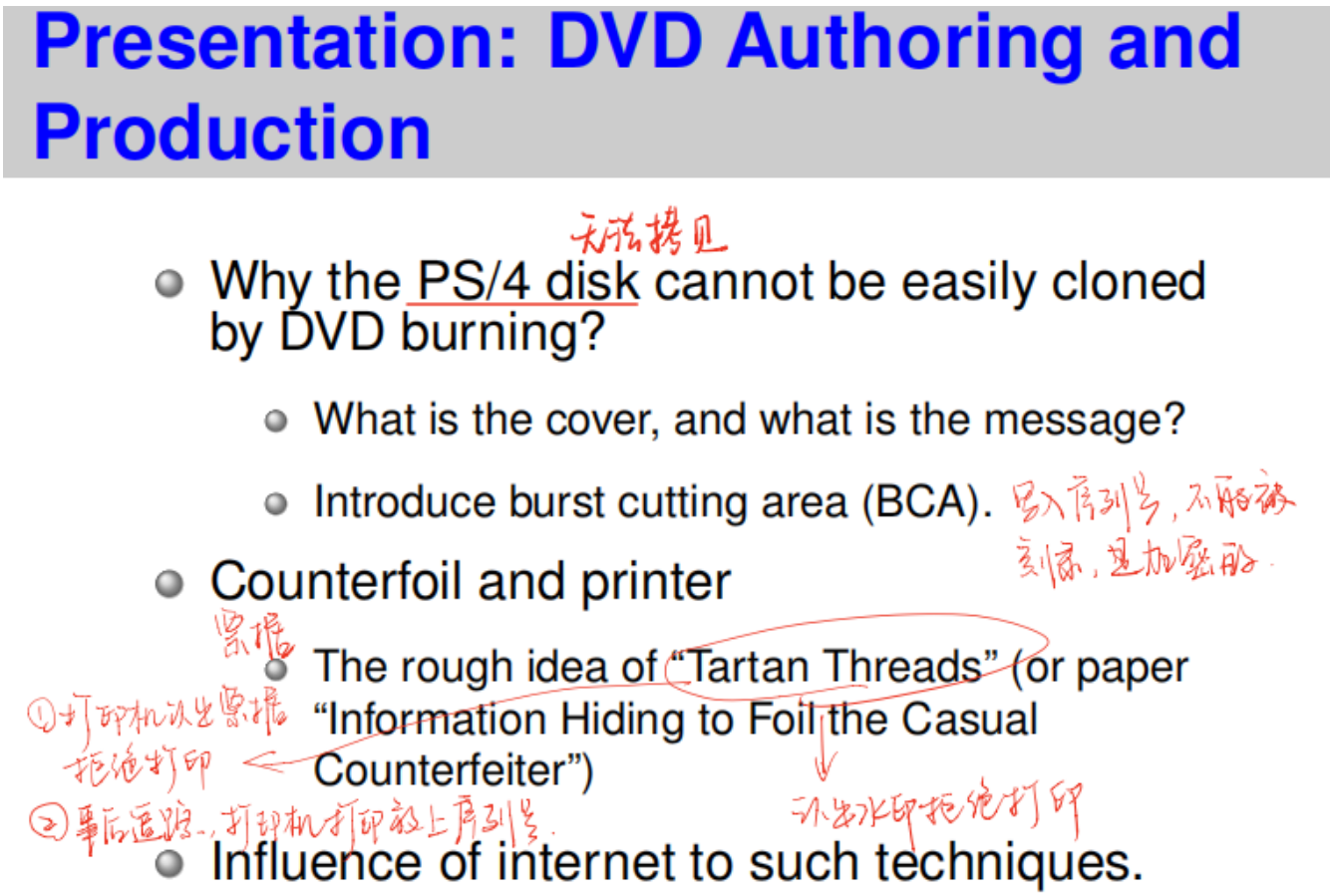
      Active attacks: modify the cover work. Passive attacks: do not modify ...
- Steganographic

- Embedding（**考点：**和水印的区别，水印添加失败即失败，因为水印和work有关；隐写添加失败可以换一个work添加，因为隐写和work无关）

  capacity：放多容易被找到，放少效率不高
- Detection：Steganalysis systems 比较适用于 informed

  targeted，flase alarm rate（水印里叫false positive rate）
- Security，Stego Key（密钥长度不重要）

PRE



CHAPTER 3 Models of Watermarking

Secure Transmission

- Passive: Aims at the message

  Message layer: cryptography
- Active: Aims at the transmission

  Transport layer: spread spectrum communication

COMMUNICATION

cover work可以视作三种存在：

- As noise

informed —— 把原图也传输过去；

blind —— E_BLIND/D_LC（算法原理：两个向量间隔进点积大；高维随机向量之间几乎垂直）

- 复习：注意modulation的意思，表示把message变成物理信道上能走的信号
- # Blind Embedding (E_BLIND)

One bit only message $m \in 0, 1$:

- A **reference pattern** (key) $\mathbf{w}_r$. 和 C_o 一样大
- Encoding into to **message pattern**:

$$\mathbf{w}_m = (2m - 1)\mathbf{w}_r.$$

防止加上去会越过 0 这个点.

- Modulate to **added pattern**: $\mathbf{w}_a = \alpha \mathbf{w}_m$.
- Embedding: $\mathbf{c}_w = \mathbf{c}_o + \mathbf{w}_a$.

- $$\begin{aligned} z_{lc} &= \frac{1}{N}(\mathbf{c}_o + \mathbf{w}_a + \mathbf{n}) \cdot \mathbf{w}_r \\ &= \frac{1}{N}(\mathbf{w}_a \cdot \mathbf{w}_r + (\mathbf{c}_o + \mathbf{n}) \cdot \mathbf{w}_r) \\ &= \frac{1}{N}(\mathbf{w}_a \cdot \mathbf{w}_r) + \varepsilon \\ &= \frac{1}{N}(\alpha(2m-1)\mathbf{w}_r \cdot \mathbf{w}_r) + \varepsilon \\ &= (2m-1)\left(\alpha \frac{\|\mathbf{w}_r\|^2}{N}\right) + \varepsilon. \end{aligned}$$

高维随机向量几乎都是相垂直

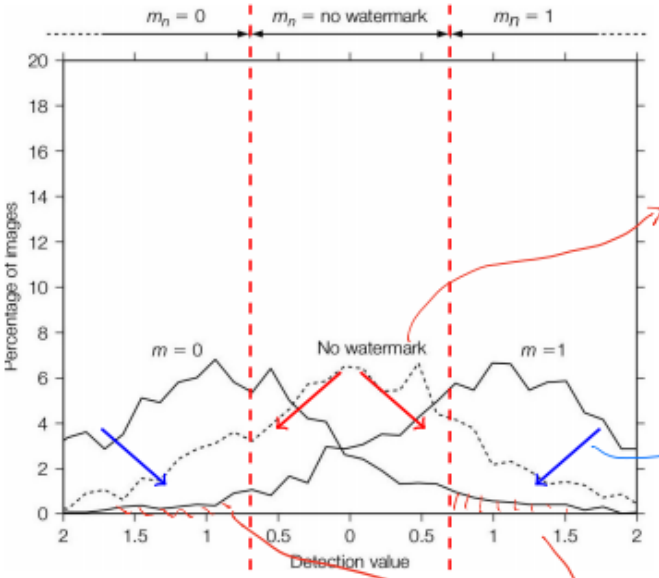
与均值和方差有关

-

Decoder outputs

$$m_n = \begin{cases} 1 & z_{lc} > \tau_{lc} \\ \text{no} & -\tau_{lc} \leq z_{lc} \leq \tau_{lc} \\ 0 & z_{lc} < -\tau_{lc}. \end{cases}$$

- **考点** 看图，画fpr effectiveness merror区域



- False positive rate of 42%.
- Effectiveness: 68%.

  - 为什么低频Wr effectiveness会变差：图像和噪音都是低频，Wr·Co变大

- As side information

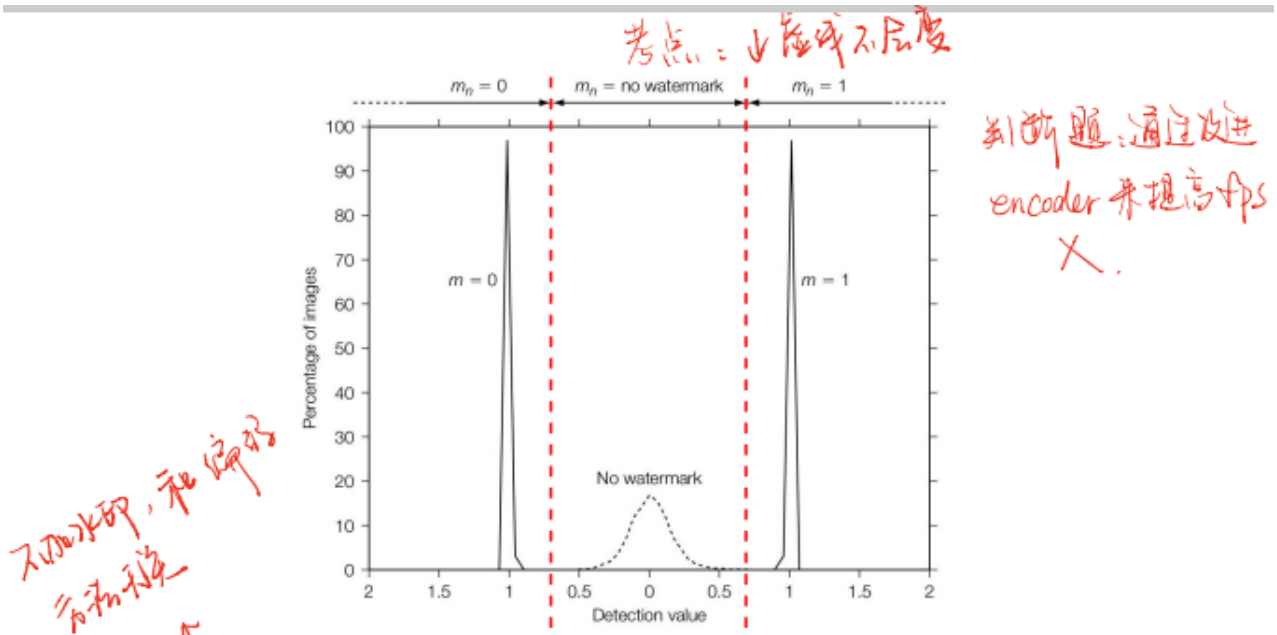
  解决方案：寻找α范围使得effectiveness变为100%（**E_FIXED_LC**）

Adaptive strength α:

- Correlation must be large enough:

$$\tau_{lc} < \tau_{lc} + \beta = z_{lc}(\mathbf{c}_w, \mathbf{w}_m)$$
$$= \frac{1}{N}(\mathbf{c}_o + \alpha \mathbf{w}_m) \cdot \mathbf{w}_m.$$
$$\Longrightarrow \alpha = \frac{N(\tau_{lc} + \beta) - \mathbf{c}_o \cdot \mathbf{w}_m}{\mathbf{w}_m \cdot \mathbf{w}_m}.$$

考点 fpr不会变，判断题如下图，fpr与编码方式无关



- False positive rate of 0.01%.
- Effectiveness: 100%.

强行改动c（会降低fidelity）

fpr不会变为0

- The second message

  人看低频信息，机器看高频信息（不同频率上放不同信息达到Multiplexed Communications）

Geometric

Points in Space

- Media space
- Marking space（eg. 直方图）

用region表示概念：

$$100\%\ \text{effectiveness}$$

$$\Longleftrightarrow$$

$$\text{embedding region} \subset \text{detection region}.$$

embeding region ∩ unwatermark regin ⇒ fpr

Marking space的方法（降低计算复杂度，效率更高，更小的reference key）

Embedding in marking space

$$\mathbf{v} = \mathcal{T}(\mathbf{c}),\ \mathbf{v}_w = g(\mathbf{v}, \mathbf{w}(m)),\ \mathbf{c}_w = \mathcal{T}^{-1}(\mathbf{v}_w, \mathbf{c}).$$

算法：E_BLK/D_CC

BLK：

$$\mathbf{v}[i,j] = \frac{1}{64}\sum_{x=0}^{w/8}\sum_{y=0}^{h/8}\mathbf{c}[8x+i, 8y+j].$$

D_CC：

- D_CC: Correlation coefficient.
  - Better (will show later).
  - Normalize (mean and variance) $\mathbf{v} \to \mathbf{v}'$:

$$\tilde{\mathbf{v}} = \mathbf{v} - \mu_{\mathbf{v}}\mathbf{1} \triangleq \mathbf{v} - \bar{\mathbf{v}},$$
$$\mathbf{v}' = \tilde{\mathbf{v}}/\|\tilde{\mathbf{v}}\|.$$

  - Correlation:

$$-1 \le z_{cc}(\mathbf{v}, \mathbf{w}_r) = \mathbf{v}' \cdot \mathbf{w}'_r \le 1.$$

embed:

$$\mathbf{c}_w = \mathcal{T}^{-1}(\mathbf{v}_w, \mathbf{c}_o):$$

- Changes on mark $\mathbf{v}$:

$$\Delta_w = \mathbf{v}_w - \mathbf{v}_o = \mathbf{w}_m.$$

- Add to cover c:

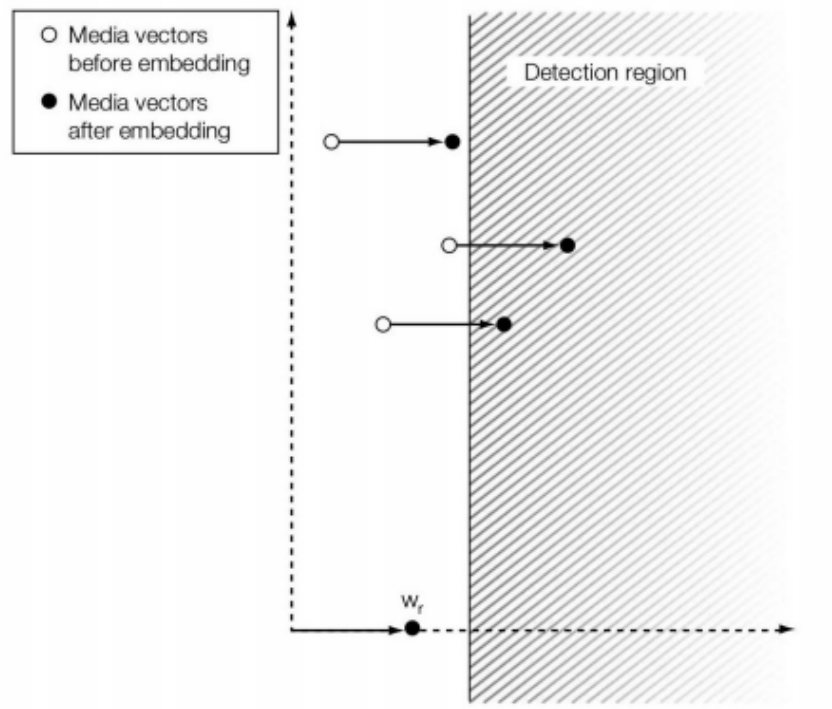
$$\mathbf{c}_w[x, y] = \mathbf{c}_o[x, y] + \Delta_w[x \bmod 8, y \bmod 8].$$

三种检测方法：

- Linear correlation

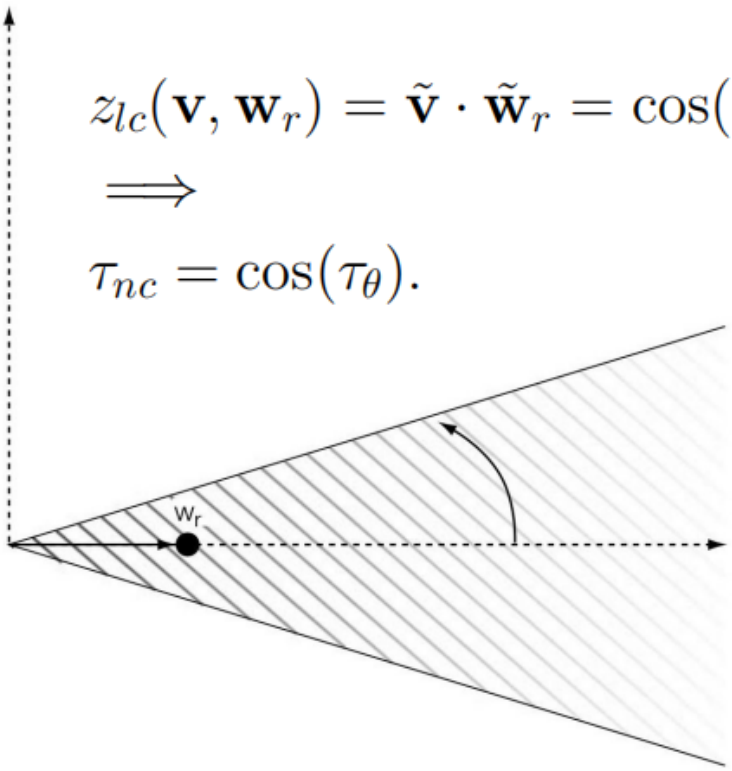
Project $\mathbf{v}$ onto $\mathbf{w}_r$

$$z_{lc}(\mathbf{v}, \mathbf{w}_r) = \frac{1}{N}\sum_i \mathbf{v}[i]\mathbf{w}_r[i] = \frac{1}{N}\mathbf{v} \cdot \mathbf{w}_r.$$



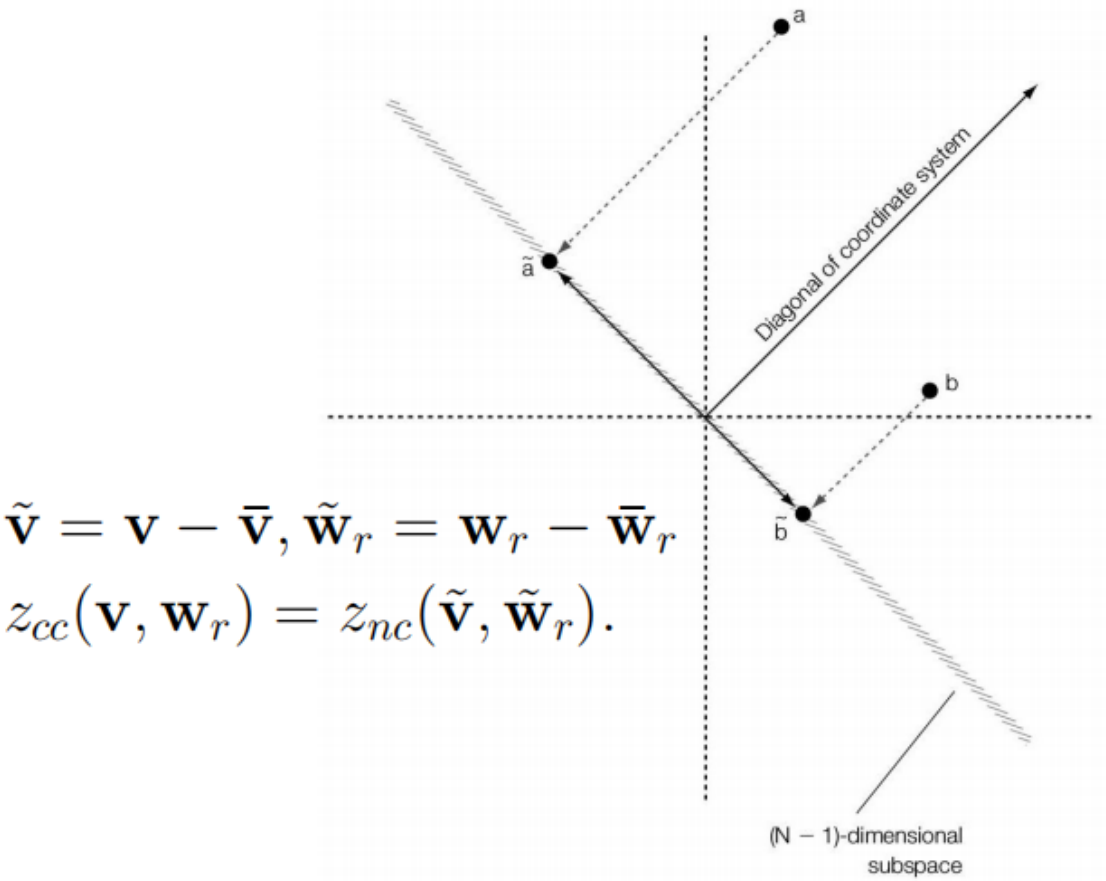
- Normalized correlation

Normalize length of $\tilde{\mathbf{v}} = \mathbf{v}/\|\mathbf{v}\|, \tilde{\mathbf{w}}_r = \mathbf{w}_r/\|\mathbf{w}_r\|$.



- Correlation coefficient

Centered and normalized:



$$\tilde{\mathbf{v}} = \mathbf{v} - \bar{\mathbf{v}}, \tilde{\mathbf{w}}_r = \mathbf{w}_r - \bar{\mathbf{w}}_r$$
$$z_{cc}(\mathbf{v}, \mathbf{w}_r) = z_{nc}(\tilde{\mathbf{v}}, \tilde{\mathbf{w}}_r).$$

CHAPTER 4 Basic Message Coding

主要讲多位message

Source coding: maps messages into sequences of **symbols**

Modulation: maps sequences of symbols into physical signals

不同位之间的W最好正交，同一位中不同信息之间负相关

减少多位信息检测时的比较次数：

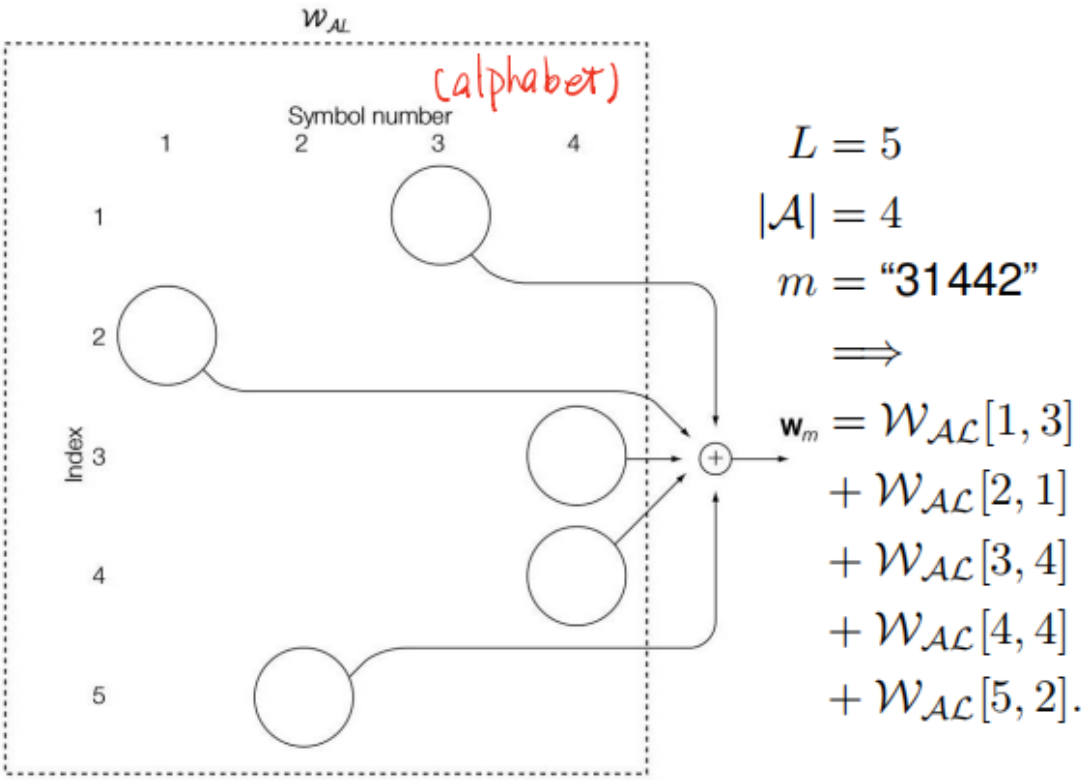
16 bit information

- $|\mathcal{A}|^1 = 65536$ for direct message coding.
- $|\mathcal{A}|^8 = 65536$ for 4-symbol 8-length coding.
  - For each index/order: compare with 4 marks.

添加多个水印的分布方式

- Time-division multiplexing：不同时间段
- Space-division multiplexing：同一张图不同位置
- Frequency-division multiplexing：不同频段（低频——高频）
- **Code-division multiplexing**

$L \times |\mathcal{A}|$ reference marks.



要求：不同行之间线性无关，同一行之间负相关

通过检测时，6种8bit信息放入2000张图中，会有检测错误，原因是不同8bit信息之间有相关性

- $L = 3, |\mathcal{A}| = 4, \mathcal{W}_{\mathcal{AL}}[i,j] \cdot \mathcal{W}_{\mathcal{AL}}[i,j] = N$
  - $\mathbf{w}_{312} = \mathcal{W}_{\mathcal{AL}}[1,3] + \mathcal{W}_{\mathcal{AL}}[2,1] + \mathcal{W}_{\mathcal{AL}}[3,2]$.
  - $\mathbf{w}_{314} = \mathcal{W}_{\mathcal{AL}}[1,3] + \mathcal{W}_{\mathcal{AL}}[2,1] + \mathcal{W}_{\mathcal{AL}}[3,4]$.
  - Inner product:

$$\begin{aligned} & \mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[j,b] = 0, \quad i \neq j \\ \Longrightarrow \quad & \mathbf{w}_{312} \cdot \mathbf{w}_{314} = \mathcal{W}_{\mathcal{AL}}[1,3] \cdot \mathcal{W}_{\mathcal{AL}}[1,3] \\ & \quad + \mathcal{W}_{\mathcal{AL}}[2,1] \cdot \mathcal{W}_{\mathcal{AL}}[2,1] \\ & \quad + \mathcal{W}_{\mathcal{AL}}[3,2] \cdot \mathcal{W}_{\mathcal{AL}}[3,4] \\ & \quad \geq N + N - N = N \end{aligned}$$

- h different symbols in a length L sequence

$$(L - 2h)N.$$

L-h 正
h 负

解决方案：汉明码，ECC

- Increase the length of sequence

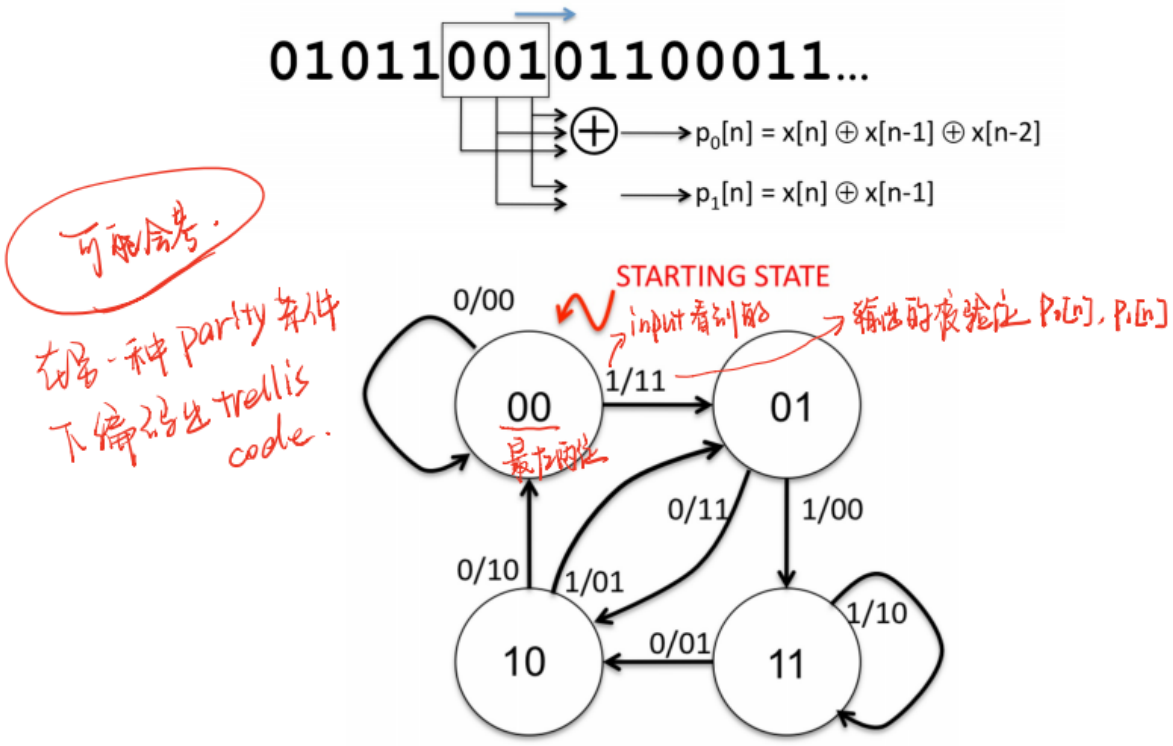
Increase the Length of Sequence

Sample

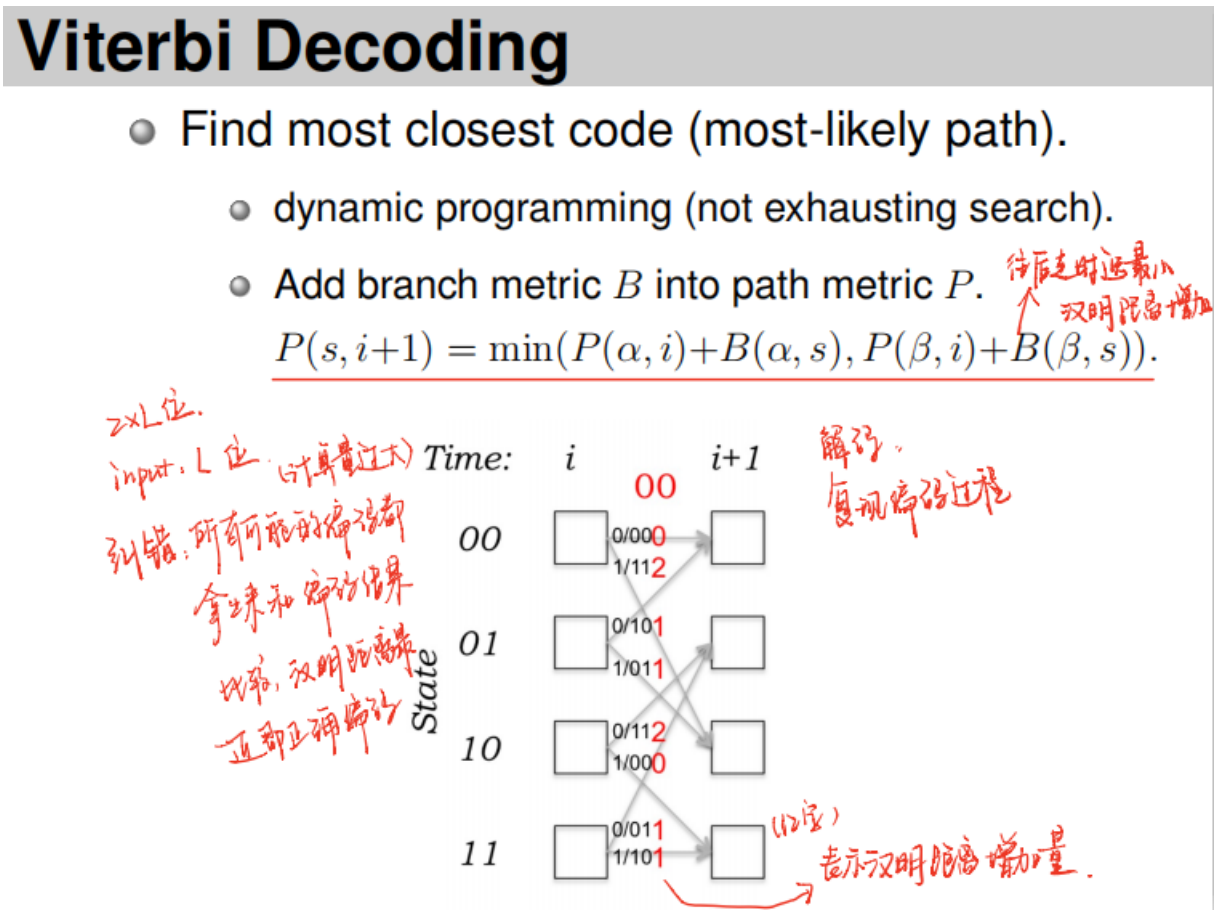
- 4-bits message set $\mathcal{M}$
  - Length 4 binary sequence, 16 messages.
- 7-bits word space $\mathcal{S}$ L=7 h=3
  - Length 7 binary sequence, 128 words.
  - $|\mathcal{S}_c| = |\mathcal{M}| = 16$.
  - $a, b \in \mathcal{S}_c, a \neq b$ have at less 3 different bits. L-h-h = L-2h = 7-2×3 = 1
  - Why 3? Flip one bit for each of the two.
  - Decode $s \in \mathcal{S}$: find $c \in \mathcal{S}_c$ has at most one different bit.

- Expand the Alphabet（eg. Trellis Code）

  编码：



  解码和纠错：



  会在trellis code后pad两位用来降低FPR

由于trellis code的纠错功能可能导致无水印的图也被认为有水印，所以采用

- **Valid Messages**

  前16位数据，后9位校验，FPR降低为原来的$\frac{1}{2^9}$

Normalized Correlation

信息长度L很大时表现差，因为Znc和L有关（前面有个 $\frac{\alpha}{\sqrt{8}}$ 就是对值做归一）

- Larger embedding strength $\alpha = 2$.
  - The message pattern is scaled to have unit standard deviation, thus $\alpha/\sqrt{8}$.
- Multiple-symbol embedding
  - $\mathbf{w}_{ri}$ orthogonal to each other and unit.

$$\mathbf{v}_L = \mathbf{v}_o + \sum_{i=1}^{L} \mathbf{w}_{ri}, \quad \|\mathbf{v}_L\| \approx \sqrt{L}.$$

  - Linear correlation: independent of L

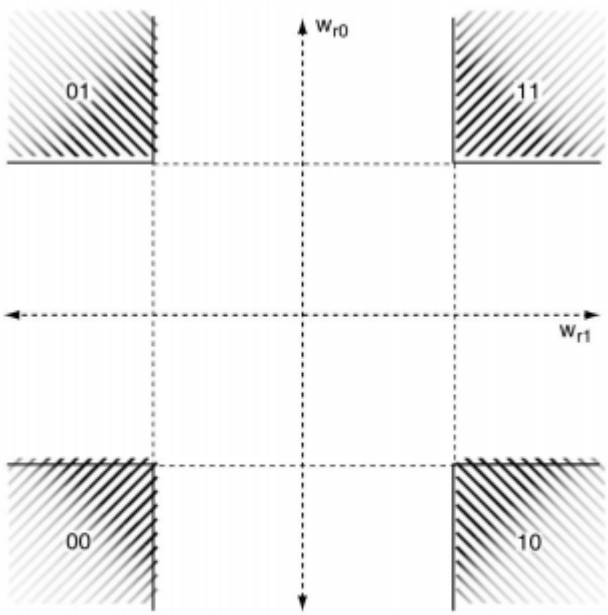
$$z_{lc}(\mathbf{v}_L, \mathbf{w}_{r1}) = \mathbf{v}_o \cdot \mathbf{w}_{r1} + \mathbf{w}_{r1} \cdot \mathbf{w}_{r1} = \varepsilon + 1.$$

  - Normalized correlation: difficult for larger L

$$z_{nc}(\mathbf{v}_L, \mathbf{w}_{r1}) = \frac{\mathbf{v}_L}{\|\mathbf{v}_L\|} \cdot \mathbf{w}_{r1} = \frac{\varepsilon + 1}{\sqrt{L}}.$$

Geometric Interpretation

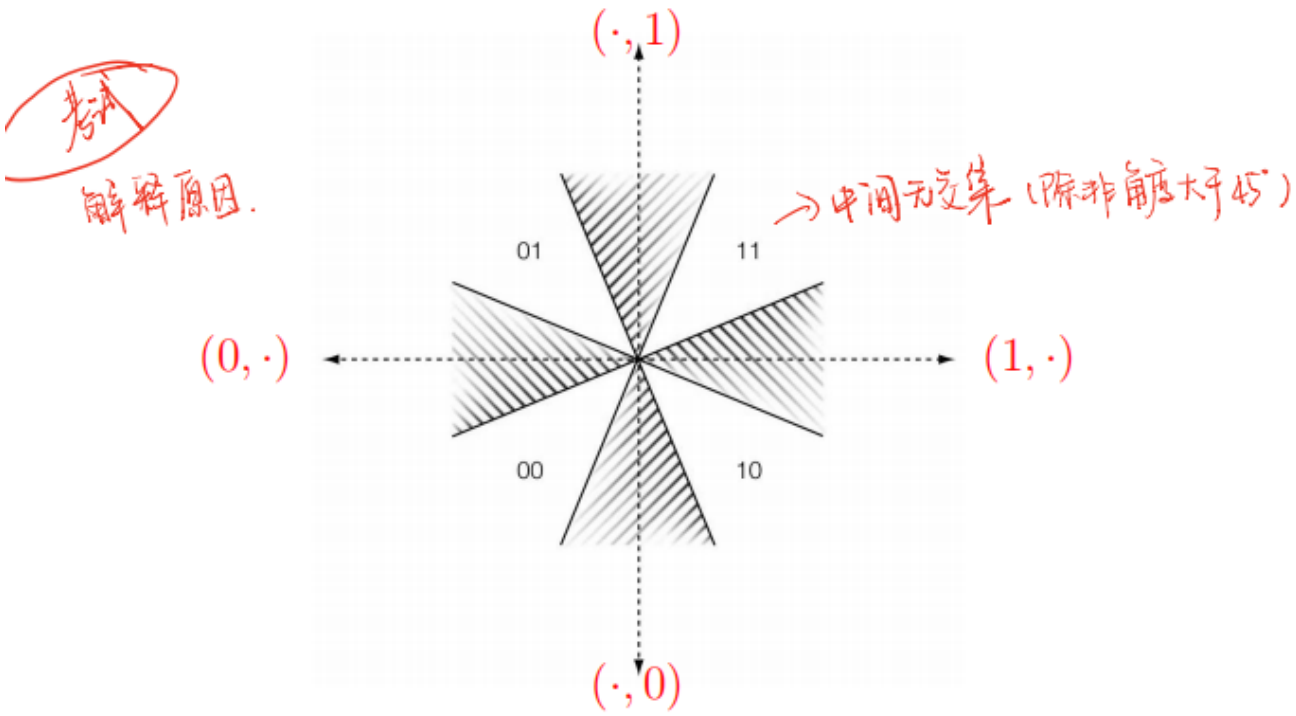
Linear correlation：



2-bit system in linear correlation.

Normalized Correlation **考点** 解释原因

- Large threshold: no overlap for the cones.
  - No detectable 2-bit message.

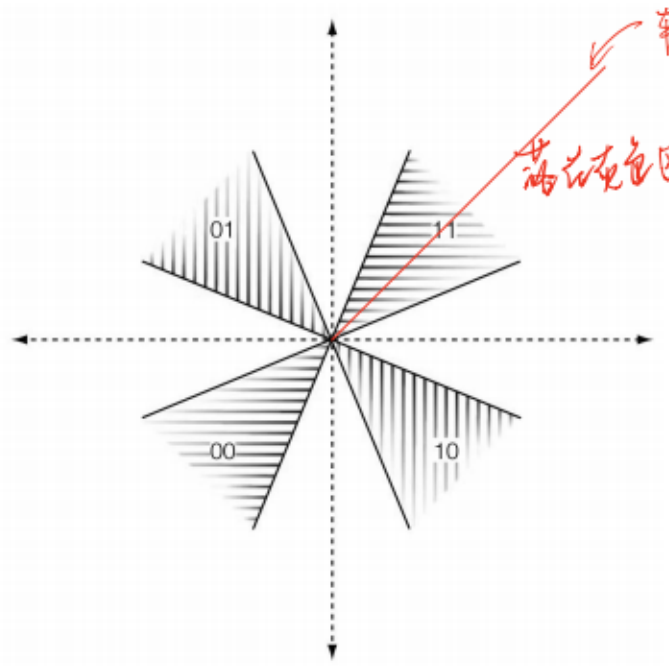


所以需要用到**Reencode**

不单独比较m中每一个bit而是比较整个m

Reencode

1. Extract message m.
2. Reencode m into mark $\mathbf{v}_m$.
3. Test the presence of $\mathbf{v}_m$



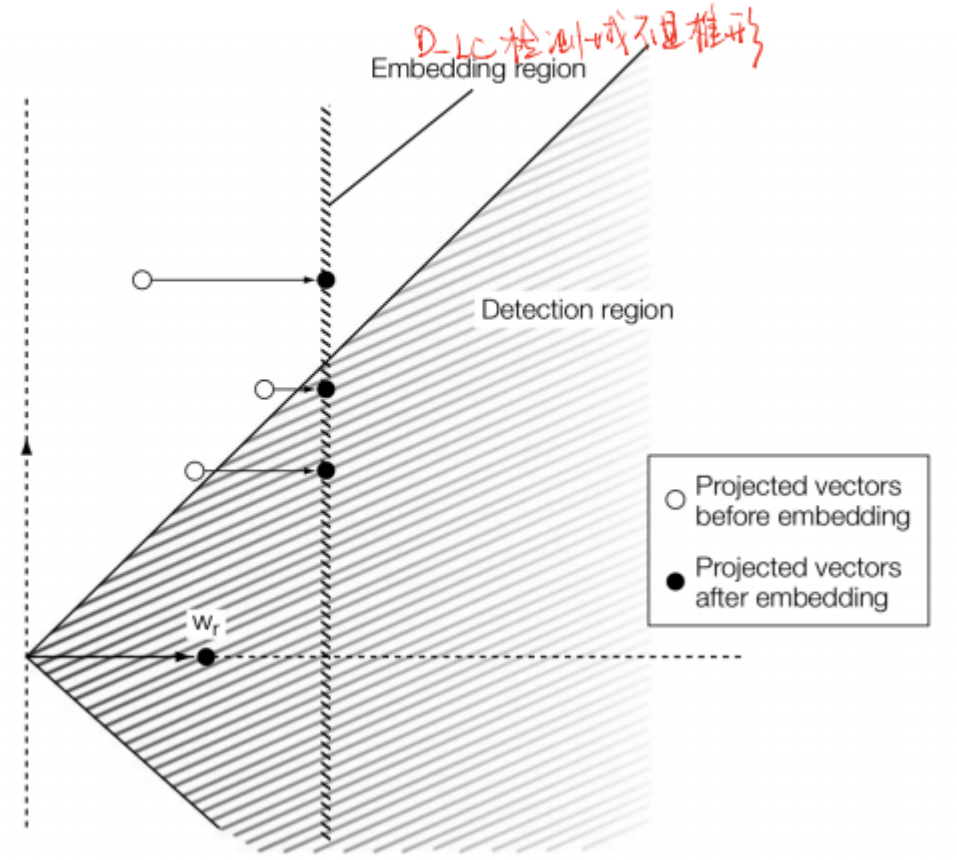
CHAPTER 5 Watermarking with Side Information

这章主要研究如何平衡fidelity和robustness

之前研究过控制α的取值范围来保证fidelity：E FIXED LC，但是只适用于Zlc

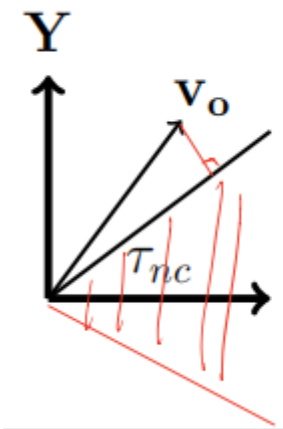
znc锥形空间：

E_FIXED_LC under z_{nc}



Zcc上的应用：

第一种类型，直接垂直映射到距离最近的检测边界中



$$X = \frac{w_r}{\|w_r\|}$$

$$Y = \frac{v_o - X(v_o \cdot X)}{\|v_o - X(v_o \cdot X)\|}.$$

Position of $\mathbf{v_o}$

$$x_{\mathbf{v_o}} = \mathbf{v_o} \cdot X, \quad y_{\mathbf{v_o}} = \mathbf{v_o} \cdot Y.$$

Upper border of the detection region (desired embedding region)

$$x(t) = t\cos(\theta_{nc}), \quad y(t) = t\sin(\theta_{nc}), \quad t > 0.$$

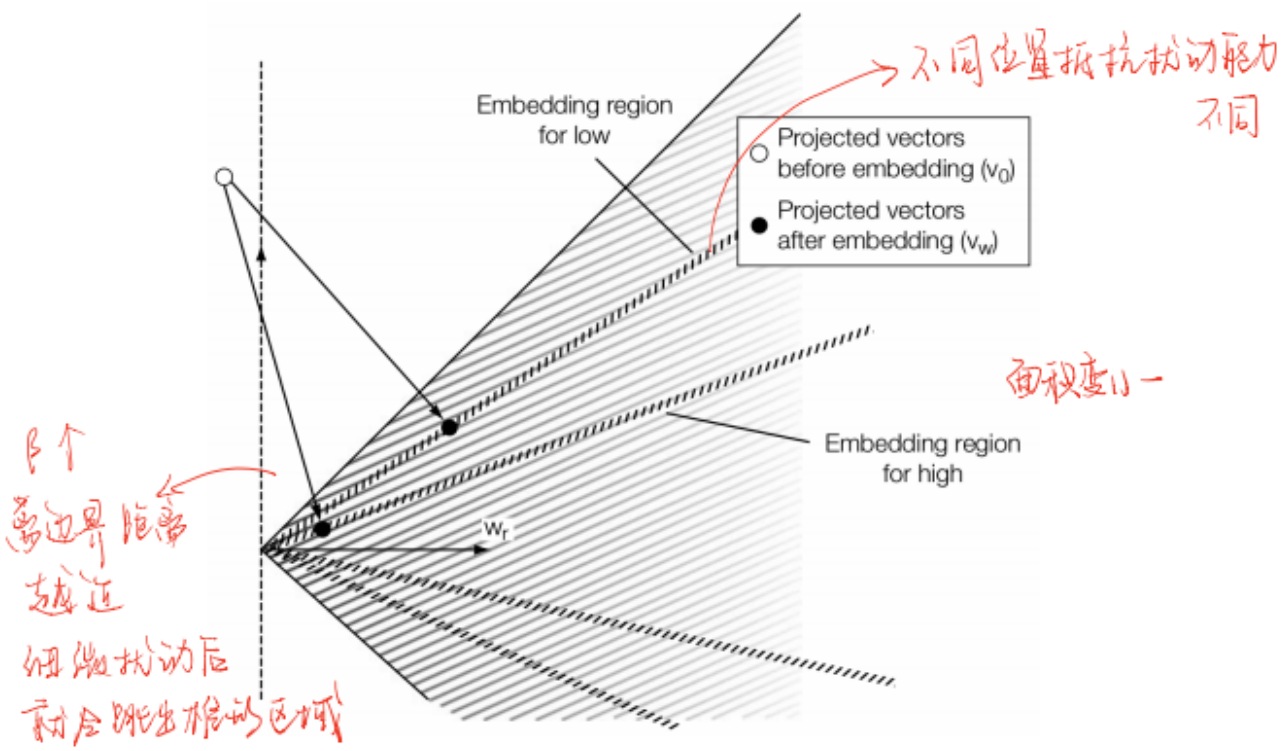
The distance from $\mathbf{v_o}$ to a point on the border:

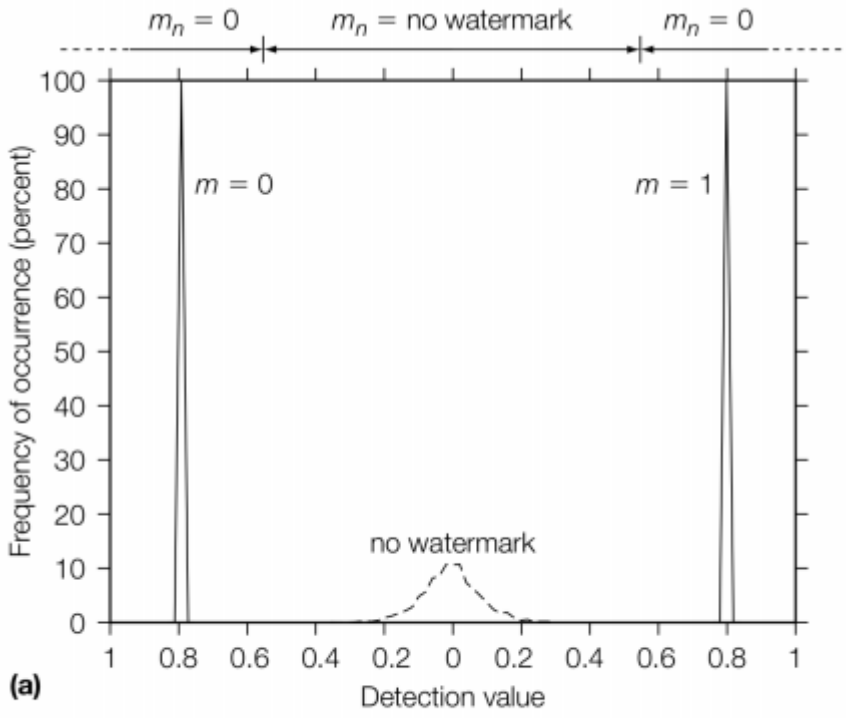
$$\begin{aligned} d^2(t) &= (x(t) - x_{\mathbf{v_o}})^2 + (y(t) - y_{\mathbf{v_o}}) \\ &= (t\cos(\tau_{nc}) - x_{\mathbf{v_o}})^2 + (t\sin(\tau_{nc}) - y_{\mathbf{v_o}}) \\ &= t^2 - 2\left(\cos(\tau_{nc})x_{\mathbf{v_o}} + \sin(\tau_{nc})y_{\mathbf{v_o}}\right)t \\ &\quad + (x_{\mathbf{v_o}}^2 + y_{\mathbf{v_o}}^2). \end{aligned}$$

So, the closest point $\mathbf{v_w}$ is $(x(t), y(t))$ with t

fidelity $\min_t d(t) \Longrightarrow t = \cos(\theta_{nc})x_{\mathbf{v_o}} + \sin(\theta_{nc})y_{\mathbf{v_o}}.$

表现情况有两点不好（1. 不同位置抗噪声干扰能力不同 2. β增加，会时夹角变小，在靠近顶点附近的点离边界近，细微扰动就不能被检测到）





$$\tau_{nc} = 0.55, \beta = 0.25, 85\% \textit{ correct.}$$

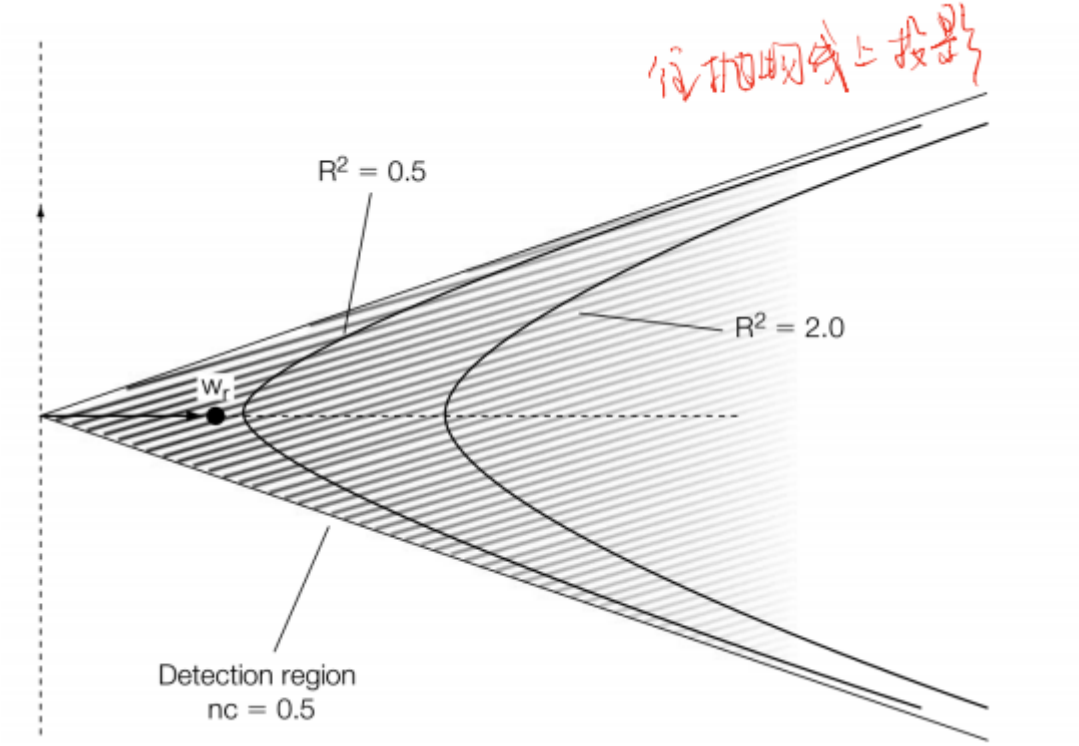
检测值的大小都差不多，因为都是通过最短距离直接映射到边界，所以检测值一样

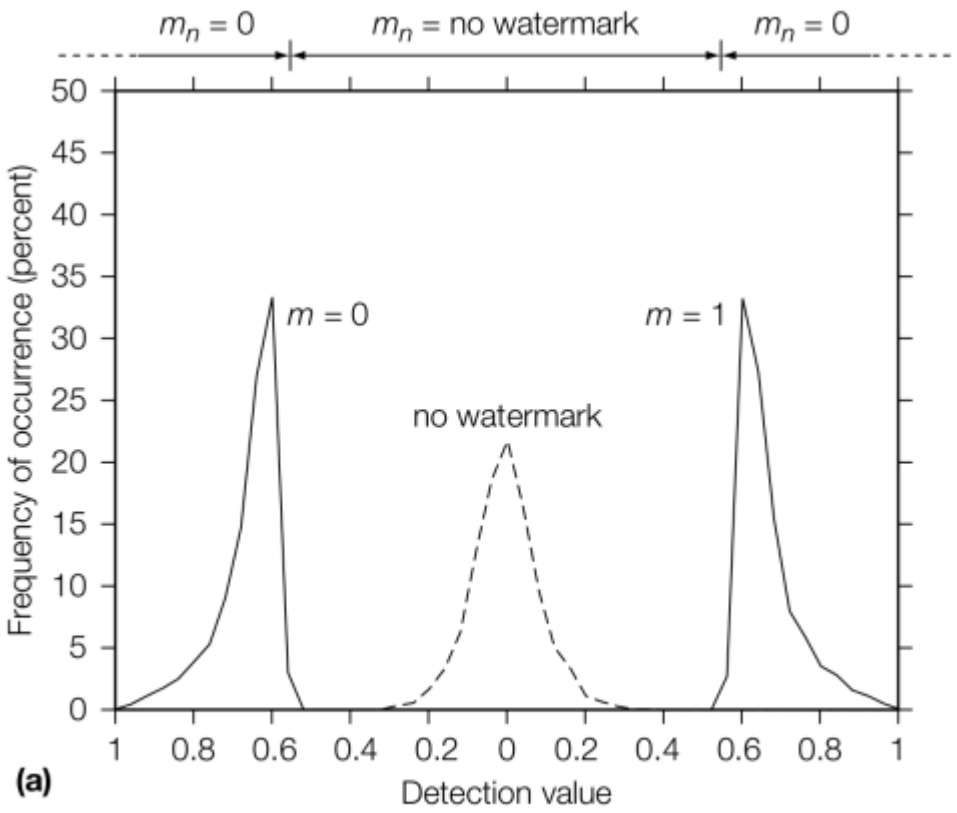
第二种方法，添加噪音后，直接计算噪音应该控制的范围大小（和Zlc的计算α类似）

$$z_{nc}(\mathbf{v_w}+\mathbf{n}) = \frac{(\mathbf{v_w}+\mathbf{n})\cdot\mathbf{w_r}}{\|\mathbf{v_w}+\mathbf{n}\|\|\mathbf{w_r}\|} \approx \frac{\mathbf{v_w}\cdot\mathbf{w_r}}{\sqrt{\mathbf{v_w}\cdot\mathbf{v_w}+\mathbf{n}\cdot\mathbf{n}}\|\mathbf{w_r}\|}$$

The noise causes $z_{nc} < \tau_{nc}$:

$$R^2 = \|\mathbf{n}\|^2 \leq \left(\frac{\mathbf{v_w}\cdot\mathbf{w_r}}{\tau_{nc}\|\mathbf{w_r}\|}\right)^2 - \|\mathbf{v_w}\|^2$$





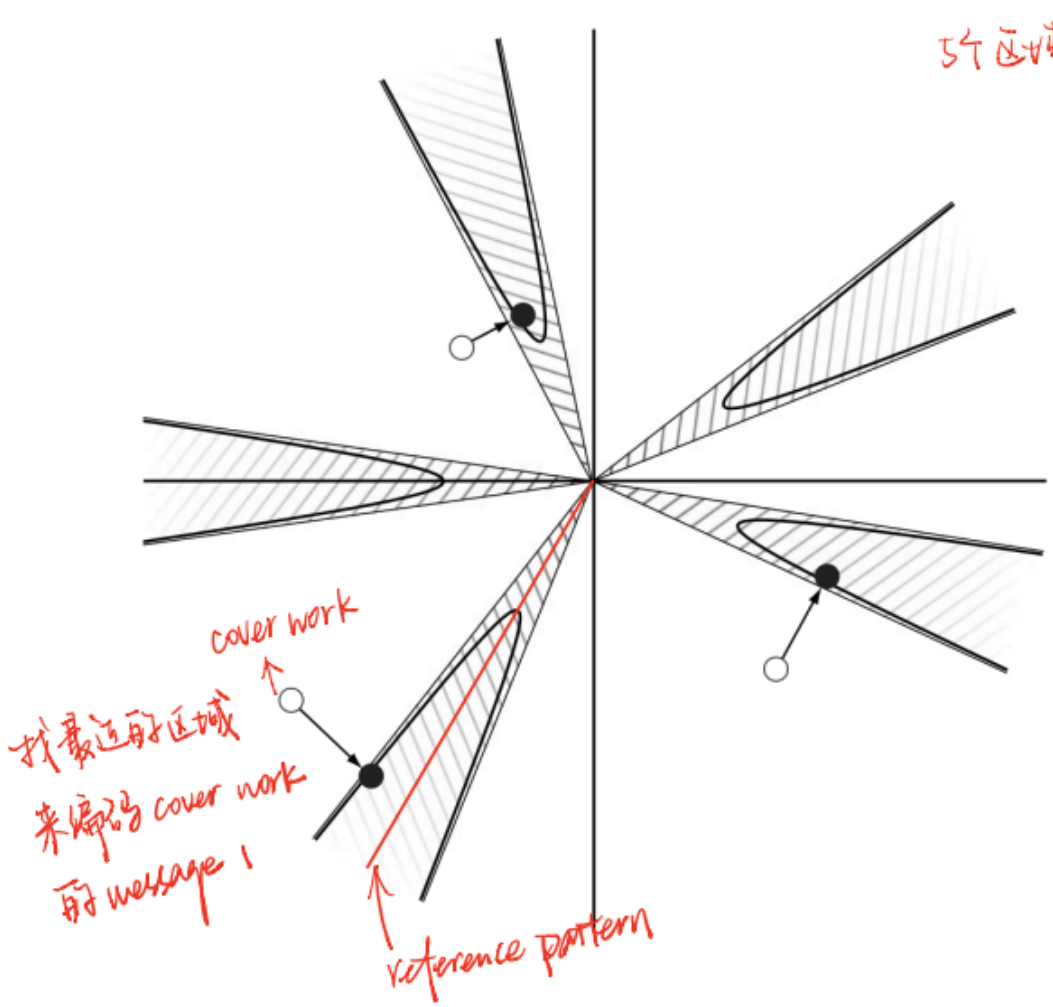
$$R^2 = 10.$$

检测值分布比较宽，检测值越小表示越靠近边界的区域，也就是抛物线图中右上角的位置（轻微扰动会变成no watermark）

考点 给出几张performance图，分类robustness side information embed（哪个图的robustness比较好）

主要讨论如何将原图（cover work）利用成side information【可以增加fidelity】

Dirty paper code：原来时code words，现在是一组code words。message每一位对应的可以有多种表示方法，根据cover work来选择最适用的（需要改动最小也就是和message最线性相关的一个code word）



由于阴影区域变多，所以fpr可能会增加，解决方案是减小每一个锥形区域的夹角

另一个缺点是，需要遍历每一个code word效率不是很高

Least significant bit (LSB)

Embed 10000011

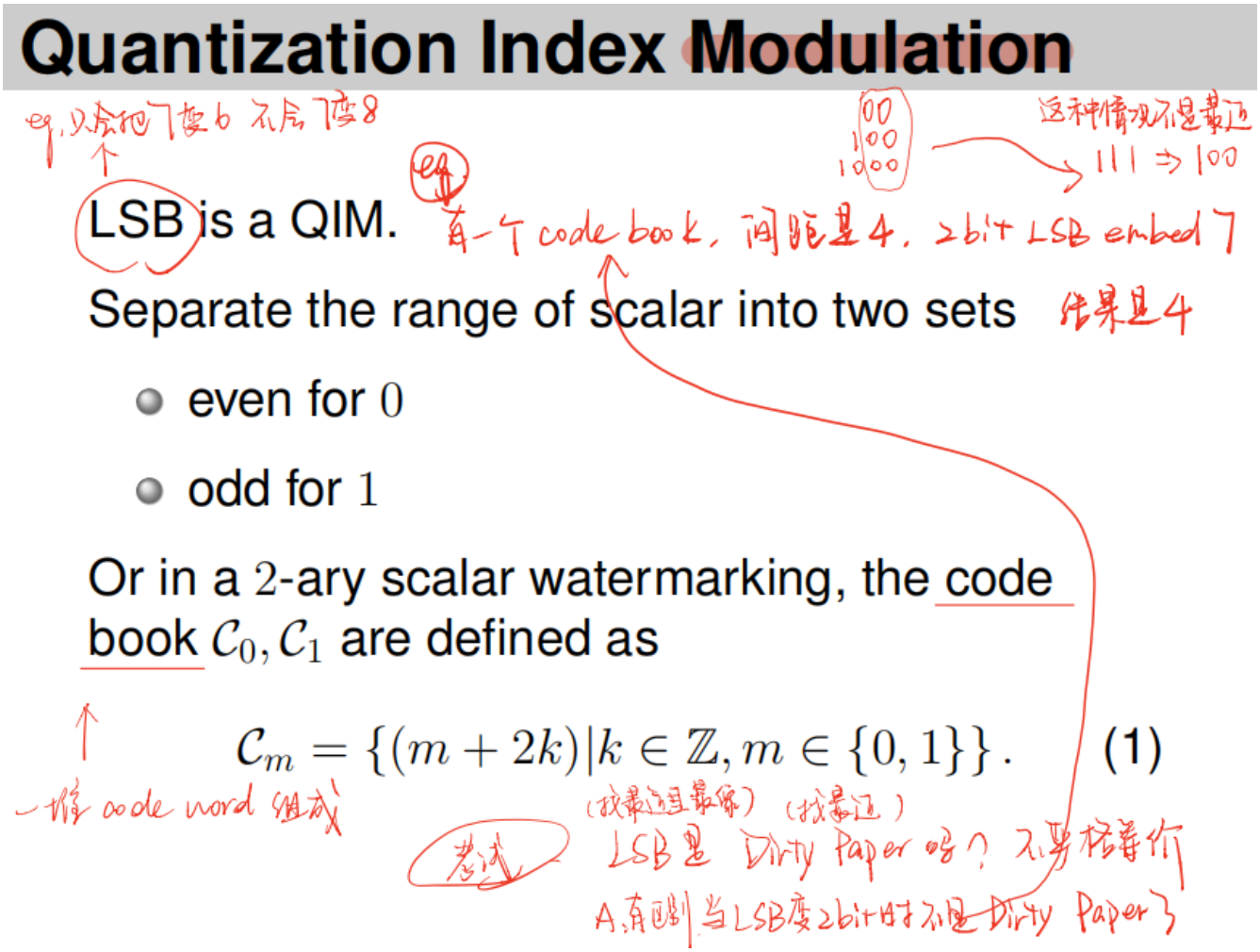
- Cover image $\Longrightarrow$ Watermarked image:

$$\begin{pmatrix} 00100111 \\ 11101001 \\ 11001000 \\ 00100111 \\ 11001000 \\ 11101001 \\ 11001000 \\ 00100111 \end{pmatrix} \Longrightarrow \begin{pmatrix} 00100111 \\ 11101000 \\ 11001000 \\ 00100110 \\ 11001000 \\ 11101000 \\ 11001001 \\ 00100111 \end{pmatrix}$$

优点：payload高，而且对1bit的信息传输fidelity好

缺点：robustness低；fpr高【解决方案是ECC；校验码，eg. pad，valid message】

Quantization Index Modulation

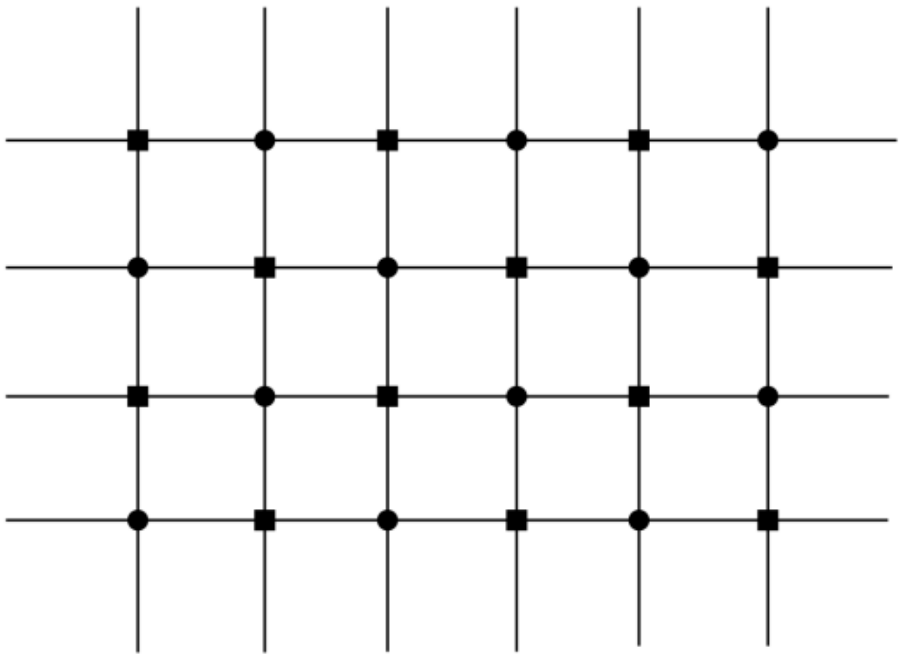


Lattice Codes

Lattice Codes

From one dimension to two dimension

$$\mathcal{C}_0 = \{(k_1 + k_2) \mod 2 = 0\}$$
$$\mathcal{C}_1 = \{(k_1 + k_2) \mod 2 = 1\}.$$



CHAPTER 6 Practical Dirty-Paper Codes

权衡fidelity和robustness

N-Dimensional Lattice

N unit orthogonal basis $\mathbf{w}_{\mathbf{r}1}, \cdots, \mathbf{w}_{\mathbf{r}N}$

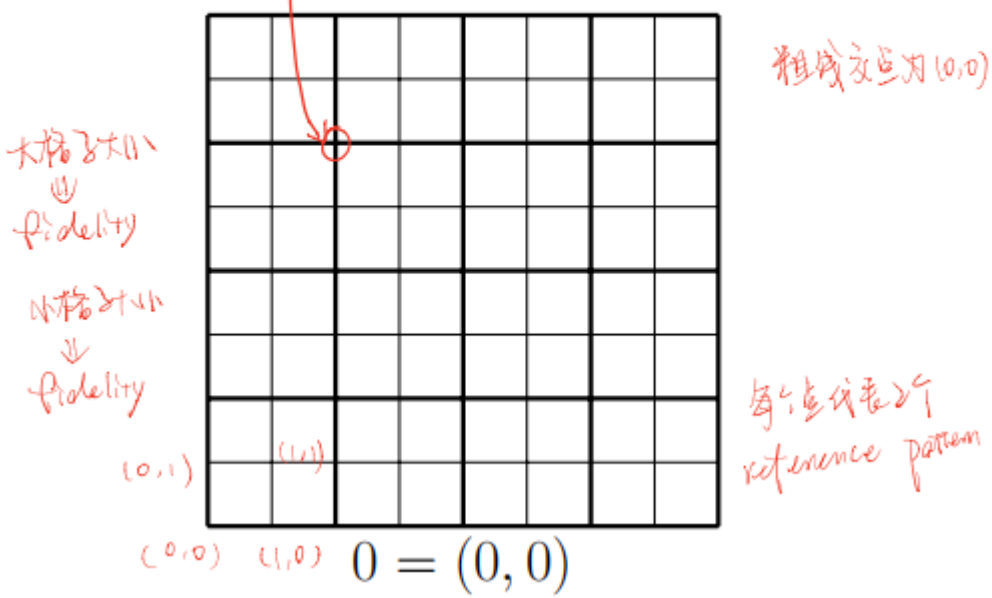
- Points in the lattice $\mathbf{p} = \sum_i k_i \mathbf{w}_{\mathbf{r}i}, k_i \in \mathbb{Z}$.
- A template sub-lattice $2\mathbf{w}_{\mathbf{r}1}, \cdots, 2\mathbf{w}_{\mathbf{r}N}$.
  - Points in the template sub-lattice:

$$\sum_i k_i (2\mathbf{w}_{\mathbf{r}i}), k_i \in \mathbb{Z}.$$

  - Shifting it along bases according to $(b_1, \cdots, b_n), b_i \in \{0, 1\}$.
  - Points in the sub-lattice with message $(b_1, \cdots, b_n)$:

$$\sum_i (b_i + 2k_i)\mathbf{w}_{\mathbf{r}i}.$$

Illustration



N-Dimensional Lattice

考试：LSB对应的是什么lattice code.

A：LSB中 reference pattern 是一个bit 1 其余都是0

Can be 2^N messages

- Encoded as length N binary sequences.

How about use template sub-lattice $(h\mathbf{w_{r1}}, \cdots, h\mathbf{w_{rN}})$ for $h = 3$?

3^N

考试：设计lattice code bank.

同时，如果只修改平行Wr部分，fidelity会比较低，如下：

A Question

Why not

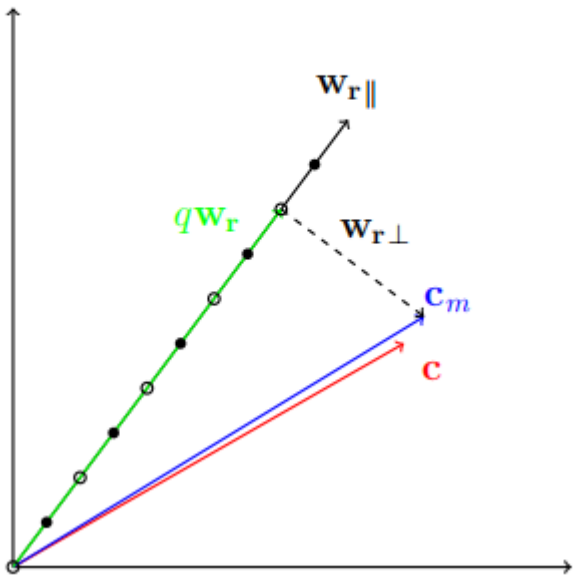
$$\mathbf{v}_m = \sum_i q[i]\mathbf{w}_{\mathbf{r}i}.$$

Number of basis is less than the dimension of $\mathbf{v}$.

Embedding one bit into $\mathbb{R}^2$ vector $(7, 4)$ with $w_r = [0.6, 0.8]$.

m	p	q	$\mathbf{v}_m$	$q\mathbf{w_r}$
0	7.4	8	(7.36, 4.48)	(4.8,6.4)

Illustration



所以，点积过后经过lattice code修改后的值需要重新映射到原来的向量上（也就是平行于Wr的部分通过lattice code进行更改，而垂直Wr的部分保留）

Embed a message $m = (b_1, \cdots, b_N)$ into $\mathbf{v}$:

- Project along each basis i:

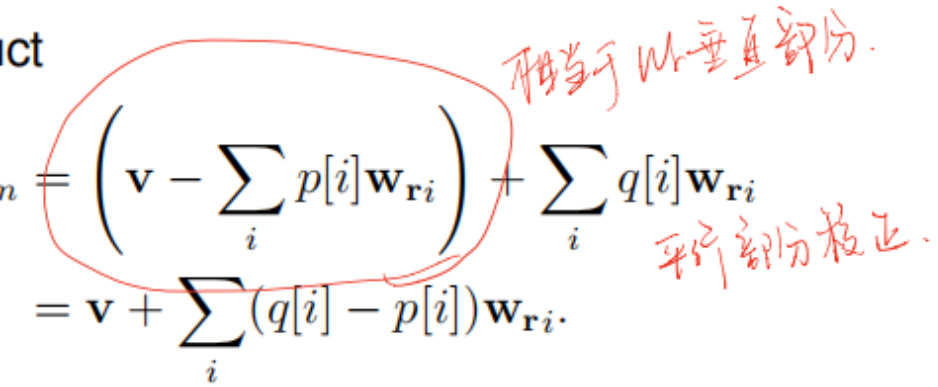
$$p[i] = \mathbf{v} \cdot \mathbf{w}_{\mathbf{r}i}.$$

- Quantize to the nearest code (Book has error):

$$q[i] = 2\left\lfloor \frac{p[i] - b_i + 1}{2} \right\rfloor + b_i.$$

- Reconstruct

$$\begin{aligned}\mathbf{v}_m &= \left(\mathbf{v} - \sum_i p[i]\mathbf{w}_{\mathbf{r}i}\right) + \sum_i q[i]\mathbf{w}_{\mathbf{r}i} \\ &= \mathbf{v} + \sum_i (q[i] - p[i])\mathbf{w}_{\mathbf{r}i}.\end{aligned}$$

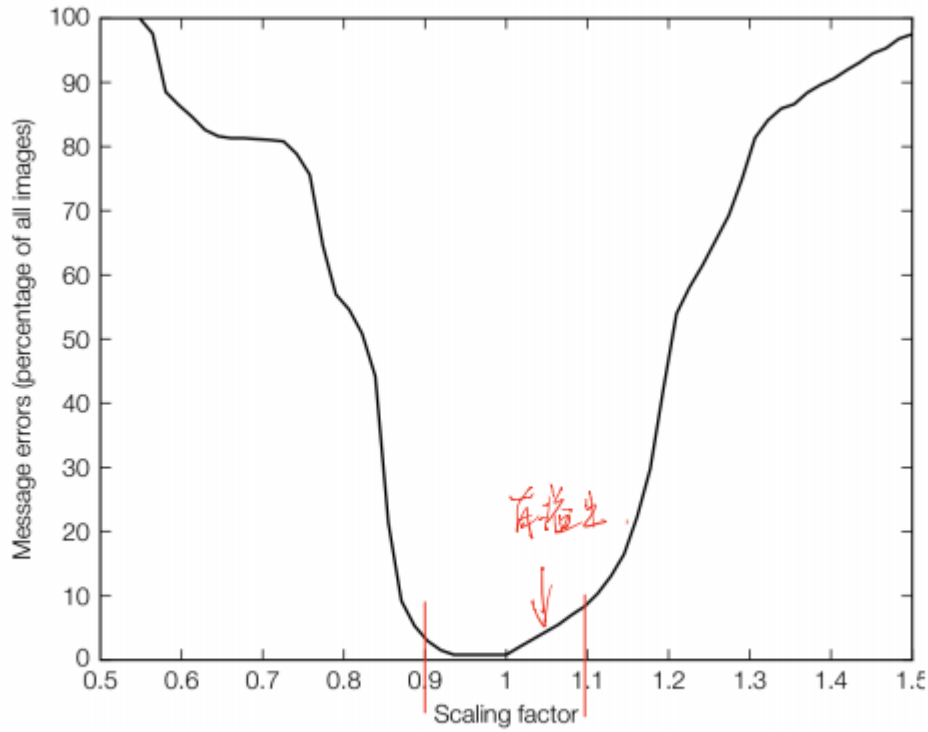


同样，信道传输过程的值会取round，上面得到的（7.36,4.48）会被重新round成（7，4）后仍旧是7，并没有变成8。解决方案：高维度空间下这种影响会比较小。

CHAPTER 9 Robust Watermarking

QIM难以抵抗亮度伸缩等变化

下图，左右不对称的原因是大于1的时候会溢出：



Valumetric scaling on the E_LATTICE/D_LATTICE system.

解决措施：固定长度的情况下改变夹角

考点 2**-Dimensional Case**

2-Dimensional Case

- Choosing two bases $\mathbf{X}_1, \mathbf{X}_2$. 考试不告诉很多Bases
- Get coordinates x_1, x_2.
- Evaluate the length and angle:

$$r = \sqrt{x_1^2 + x_2^2}, \quad \theta = \arctan(x_1/x_2).$$

- Angle QIM:

$$\theta^Q = Q_{m,\Delta}(\theta) = \left\lfloor \frac{\theta + m\Delta}{2\Delta} \right\rfloor 2\Delta + m\Delta.$$

↑ 相邻 code 间距

- Restore:

$$x_1' = r\cos(\theta^Q), \quad x_2' = r\sin(\theta^Q).$$

CHAPTER 10 Watermark Security

主要讲了给定原图和加水印的图的情况下，如何构造一个图来做到对称，无法分清原图是哪一张。

目标：

Ownership 真假判断

	$\mathbf{c_o}$	$\mathbf{c_d}$	$\mathbf{c_f}$
$\mathbf{w_r}$	-0.016	0.973	0.971
$\mathbf{w_f}$	0.968	0.970	0.005

- $\mathbf{w_f}$: large z_{lc} for $\mathbf{c_o}$ and $\mathbf{c_d} = \mathbf{c_o} + \mathbf{w_r}$

$$\mathbf{c_o} \cdot \mathbf{w_f}, \quad (\mathbf{c_o} + \mathbf{w_r}) \cdot \mathbf{w_f}.$$

- $\mathbf{c_f}$: small z_{lc} to $\mathbf{w_f}$

$$\mathbf{c_f} \cdot \mathbf{w_f} \approx 0.$$

A Naive Solution

- $\mathbf{w_f}$ has high correlation with $\mathbf{c_d}$ (or $\mathbf{c_o}$): $\mathbf{w_f} \cdot \mathbf{c_d} = 1$.
- $\mathbf{c_f} = \mathbf{c_d} - \mathbf{w_f} / \|\mathbf{w_f}\|^2$.

但是这种情况下的Cf几乎等于0，fidelity很差

A Better Solution

Using the Fourier transformation F:

- Project to Fourier bases:

$$\mathbf{c_d^1} = F\mathbf{c_d}.$$

- Scaling $\mathbf{c_d^1}$ by a random diagonal matrix D into a random vector:

$$\mathbf{c_d^2} = D\mathbf{c_d^1}.$$

- Reconstruct it back:

$$\mathbf{w_f} = F^T\mathbf{c_d^2} = F^T D F \mathbf{c_d}.$$

$$
\begin{aligned}
\mathbf{w_f} \cdot \mathbf{c_o} &= (F^T DF)(\mathbf{c_d}) \cdot \mathbf{c_o} \\
&= \mathbf{c_o}^T (F^T DF)\mathbf{c_d} \\
&= (D^{1/2} F \mathbf{c_o})^T (D^{1/2} F(\mathbf{c_o} + \mathbf{w_r}) \\
&= \mathbf{c'_o} \cdot \mathbf{c'_o} + \mathbf{c'_o} \cdot \mathbf{w'_r} \\
&\approx \mathbf{c'_o} \cdot \mathbf{c'_o}.
\end{aligned}
$$

这样得到的水印添加Wf具有一定原图性质，所以需要添加噪声

解决办法是直接往加了原水印的图中添加噪声：

Add noise before applying Fourier transformation.

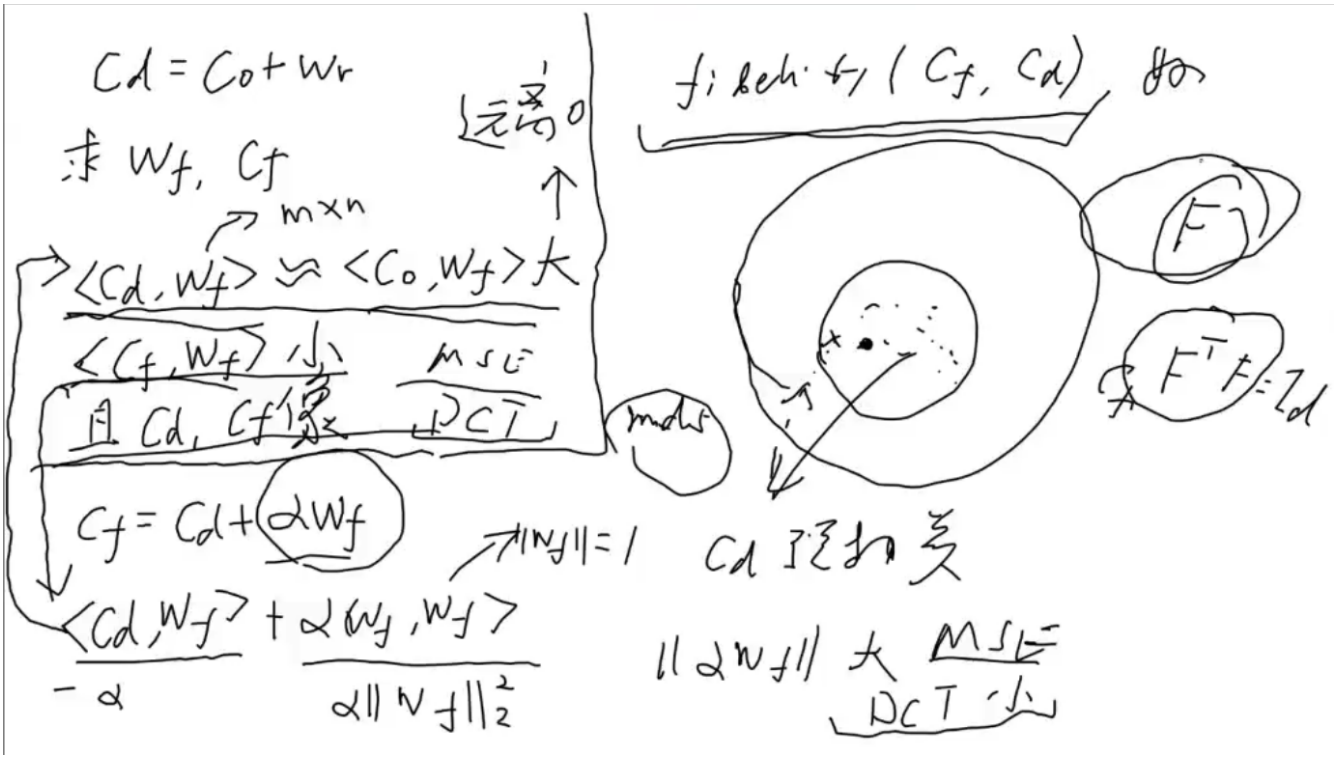
$$
\mathbf{w_f} = (F^T DF)(\mathbf{c_d} + \mathbf{n}).
$$

Check:

$$
\begin{aligned}
\mathbf{w_f} \cdot \mathbf{c_o} &= (F^T DF)(\mathbf{c_d} + \mathbf{n}) \cdot \mathbf{c_o} \\
&= (D^{1/2} F \mathbf{c_o})^T (D^{1/2} F(\mathbf{c_d} + \mathbf{n})) \\
&\approx \mathbf{c'_o} \cdot \mathbf{c'_o} + \mathbf{c'_o} \cdot \mathbf{n'} \\
&\approx \mathbf{c'_o} \cdot \mathbf{c'_o}
\end{aligned}
$$

应对上述方法，可以在水印和原图中构建一种关联，比如MD5

下图是一种分析，在寻求与Cd和Cf极大线性相关的同时，寻求Cf和Wf线性相关最小，这两个要求是互相有关联的，可以使<Cd，Wf>的值达到-α



补充mse和DCT

- mse判断两张图的相似性：

- Approximate by mean squared error (MSE)

$$D_{\text{mse}}(\mathbf{c}_1, \mathbf{c}_2) = \frac{1}{N}\|\mathbf{c}_1 - \mathbf{c}_2\|^2.$$

$$D_{\text{snr}}(\mathbf{c}_1, \mathbf{c}_2) = \frac{\|\mathbf{c}_1 - \mathbf{c}_2\|^2}{\|\mathbf{c}_1\|^2}.$$

- DCT

  分割，首先将图像分割成8x8或16x16的小块； DCT变换，对每个小块进行DCT变换； 舍弃高频系数（AC系数），保留低频信息（DC系数）。高频系数一般保存的是图像的边界、纹理信息，低频信息主要是保存的图像中平坦区域信息。

二维DCT变换就是将二维图像从空间域转换到频率域。形象的说，就是计算出图像由哪些二维余弦波构成

$$F = AfA^T$$

$$A(i,j) = c(i)cos[\frac{(j+0.5)\pi}{N}i]$$

其中F就是变换得到的系数，f是图像的像素值，A是转换矩阵，其中i为二维波的水平方向频率，j为二维波的垂直方向频率，取值范围都是0-(N-1)，N是图像块的大小，

$$c(i) = \begin{cases} \sqrt{\frac{1}{N}}, & i = 0 \\ \sqrt{\frac{2}{N}}, & i \neq 0 \end{cases}$$

1）求出转换矩阵A；
2）利用转换矩阵A，转换到频域，即由图像 f 得到系数矩阵F。

CHAPTER 11 Content Authentication

主要讲如何看出work被改动了，以及添加水印后复原

将图像分割为两半（一块计算MD5一块添加MD5）用SHA和MD5的方法难以抵抗图像distortion

Erasable Watermarks

普通的水印添加会溢出。

解决方案1：溢出后直接反向（eg. 256->-1）。缺点是，影响fidelity，同时是一种informed 方式，需要side information

解决方法2：

这里利用了人眼感知，取相邻的像素点，用插值添加水印

Giving two neighboring pixels

$x_1, x_2 \in \{0, \cdots, 255\}.$

- Transform

$x_1+(x_1-x_2)$ $x_2+(x_2-x_1)$

$$(y_1, y_2) = T(x_1, x_2) = (2x_1 - x_2, 2x_2 - x_1)$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \left(\mathrm{Id} + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Example:

$$T(59, 54) \Rightarrow (64, 49).$$

How to embed?

- Modulo 3: $y_1 - y_2 = 3(x_1 - x_2)$. 差被大三倍.
- embed 1: $y_1 + = 1$.
- embed 0: $y_1 - = 1$.

How to detect?

- $y_1 - y_2 \mod 3$.
  - 0: no message.
  - 1: 1.
  - 2: 0.

After extracting the message and restore y_1:

$$\begin{aligned}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &= T^{-1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \frac{1}{6} \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} (4y_1 + 2y_2)/6 \\ (2y_1 + 4y_2)/6 \end{pmatrix}\end{aligned}$$

要先提出message
否则会变成小数

更多symbol的情况下：

For $2n$ symbols $(-n, \cdots, -2, -1, 1, 2, \cdots, n)$:

$$
\begin{aligned}
(y_1, y_2) &= T_n(x_1, x_2) \\
&= ((n+1)x_1 - nx_2, (n+1)x_2 - nx_1)
\end{aligned}
$$

$$
\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \left(\mathrm{Id} + n \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.
$$

Modifying y_1 by at most n.

核心思想 这里放大三倍的原因是，能够做逆变换，从添加水印的图像中重新提取出原图

同时，如果无法放入信息（也就是三倍差值超出阈值），修改像素差为2n+1的倍数，修改的值作为后续值，放入图像。MD5信息读完后读修正信息。

Embeddable Pixel Pair

如果 $2x_1 - x_2$, $2x_2 - x_1$ 溢出情况

Both values in the pairs $(y_1 - n, y_2)$ and $(y_1 + n, y_2)$ are within the dynamic range $\{0, \cdots, 255\}$.

How to know?

- $y_1 - y_2 \mod (2n+1) = 0$.

中间差 $2n+1$ 表示没有嵌 message

eg. 155 130

153 100. 差3.

How to do?

- Modify x_1 to make $x_1 + c - x_2 \mod (2n+1) = 0$.
- The correct c is part of payload.

(-2) 嵌入 correction.

MD5信息读完后，再读后读出正信息

这个方法的缺陷：图像的大小或图像数量是有限的，映射要求一对一，给一个message，一边是Co一边是Cw，难以同时hold（两个同样大小有限集难以映射到一个大小中）

CHAPTER 12 Steganography

主要讲水印添加技术

根据cover work分类：

- Preexisting, and will not be modified:

  cover lookup. 已有，不改（eg. 不同work代表不同m，缺点：payload低）

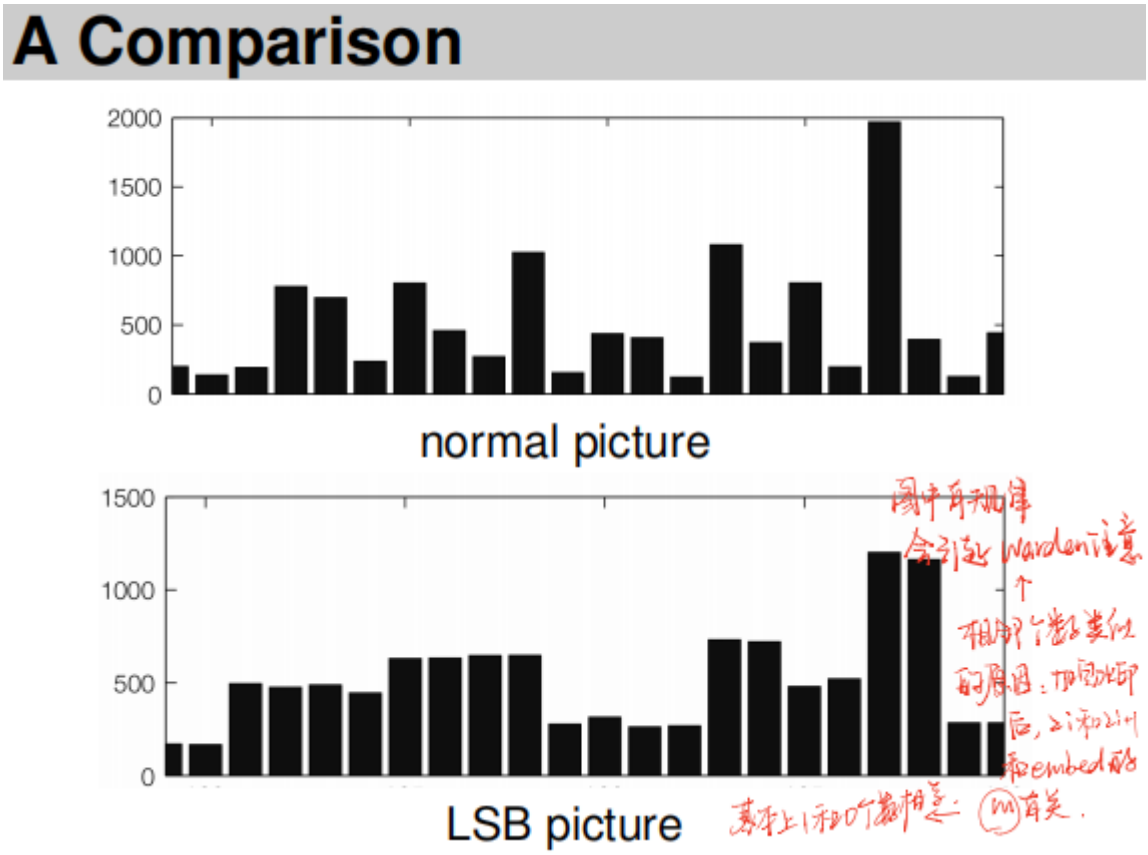
- Generated, and will not be modified:

  cover synthesis. 生成，不改（eg. 一本书中不同单词代表不同m，缺点：表达范围受限，解决方案code book）

- Preexisting and modified:

  cover modification. 已有，改

  - 方法1：LSB，相邻两个像素为一个bin，同一个bin之间交换



  - OutGuess，每个bin内变化的值后续都要矫正回来

OutGuess

- Preserving DCT Statistics
  - first pass: LSB along a pseudo-random walk
  - second pass: correct the coefficients to restore the histogram
- The maximum length that can be embedded
  - Ensuring that one will be able to make corrections
  - determined by the frequencies of the most unbalanced LSB pair.

embed比例不能过高：

For Simple Detection

In a bin consists of a pair of values (U, L). In normal work, $U > L$. Let fraction $q \in [0, 1]$ of the bin is used to embed, how large q could be?

cover	U	L
unchanged	$U \cdot (1-q)$	$L \cdot (1-q)$
changed	$(U+L) \cdot \frac{q}{2}$	$(U+L) \cdot \frac{q}{2}$
sum	$U - (U-L) \cdot \frac{q}{2}$	$L + (U-L) \cdot \frac{q}{2}$

- Embedding: U decreases by $(U-L) \cdot \frac{q}{2}$.
- Restoring: at most $L \cdot (1-q)$ can be turned to U.
- To make sure of recovering U:

$$(U-L) \cdot \frac{q}{2} < L \cdot (1-q) \Rightarrow \frac{q}{2}(U+L) < L \Rightarrow q < \frac{2L}{U+L}.$$

- Model-Based Steganography，（这一种方法和上一种方法可以看作trellis code和汉明码之间的区别，这种方法将数据位和校验位放在一起，而上一种分离）用概率来表示编码的组成

Generalized Cauchy model with probability density function (pdf)

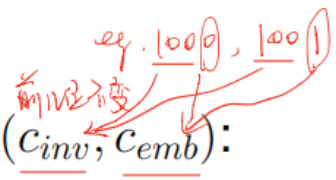
- Generalized Cauchy distribution (GCD):

$$P(x) = \frac{p-1}{2s}\left|\frac{|x|}{s}+1\right|^{-p}.$$

- $p > 1, s > 0$ are the two parameters.

Two-Class Pattern Classification

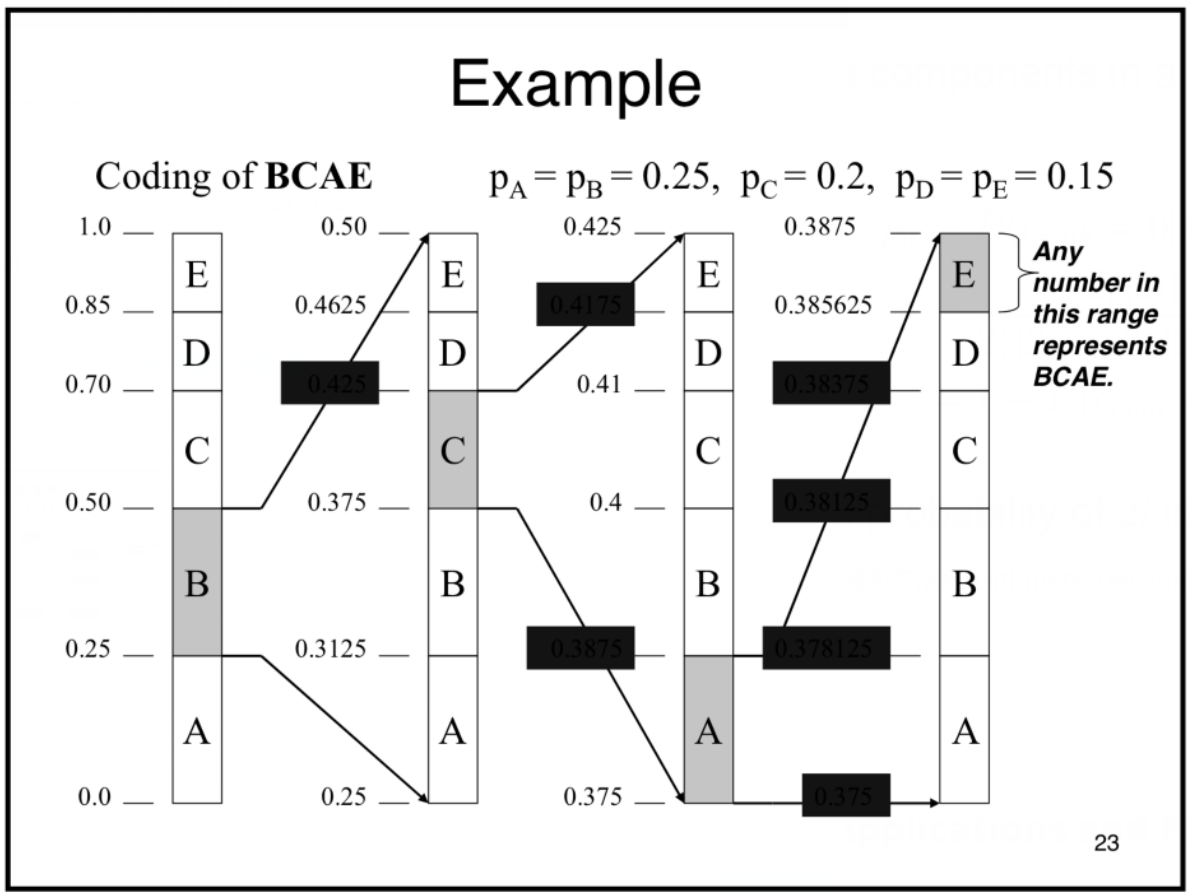
Two components in a cover work (c_{inv}, c_{emb}):



$$\begin{aligned} p_0 &= P(c_{emb} = 0 | c_{inv} = MSB_7(2i)) \\ &= \frac{T_c[2i]}{T_c[2i] + T_c[2i+1]} \\ &= 1 - P(c_{emb} = 1 | c_{inv} = MSB_7(2i)). \end{aligned}$$

The probability of $2i$ in the bin $(2i, 2i+1)$.

后续解压用到的方法是Arithmetic Decompress：



Reverse Compression

- In embedding:

  uniformly distributed bitstream

  Decompress $\Rightarrow$

  GCD distributed bitstream

- In detection:

  GCD distributed bitstream

  Compress $\Rightarrow$

  uniformly distributed bitstream

Embedding Effificiency

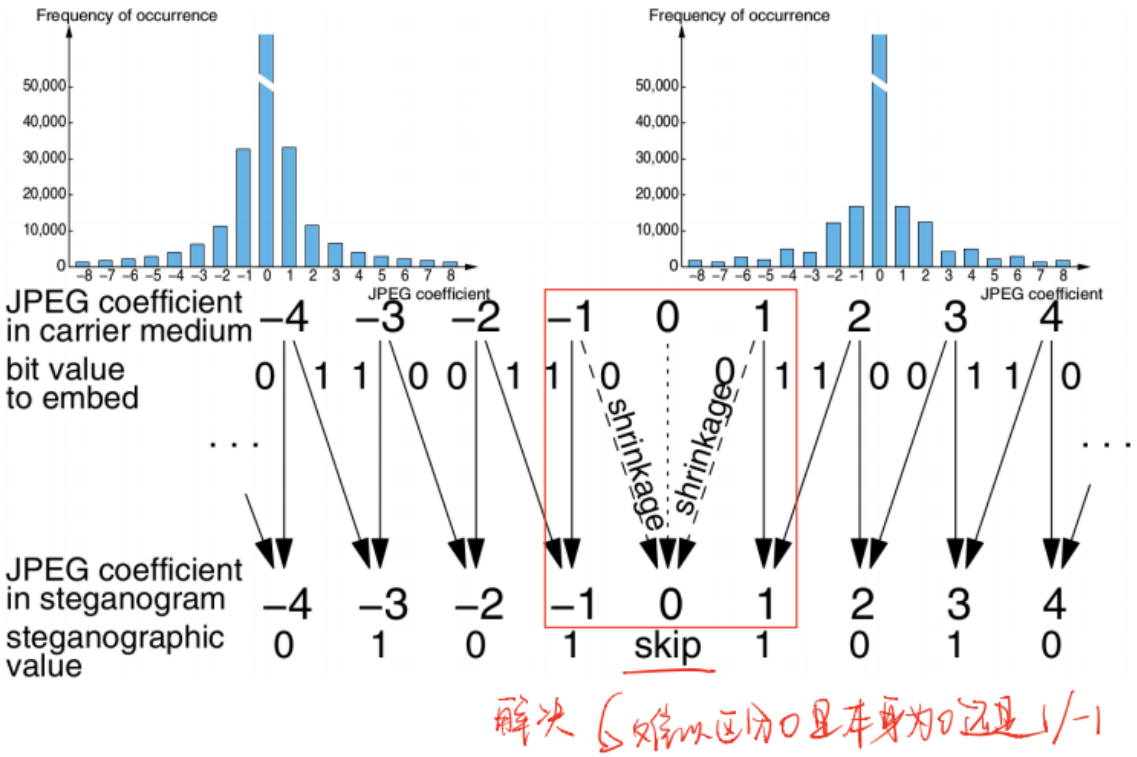
LSB的效率：

$$\frac{1}{0.5}$$

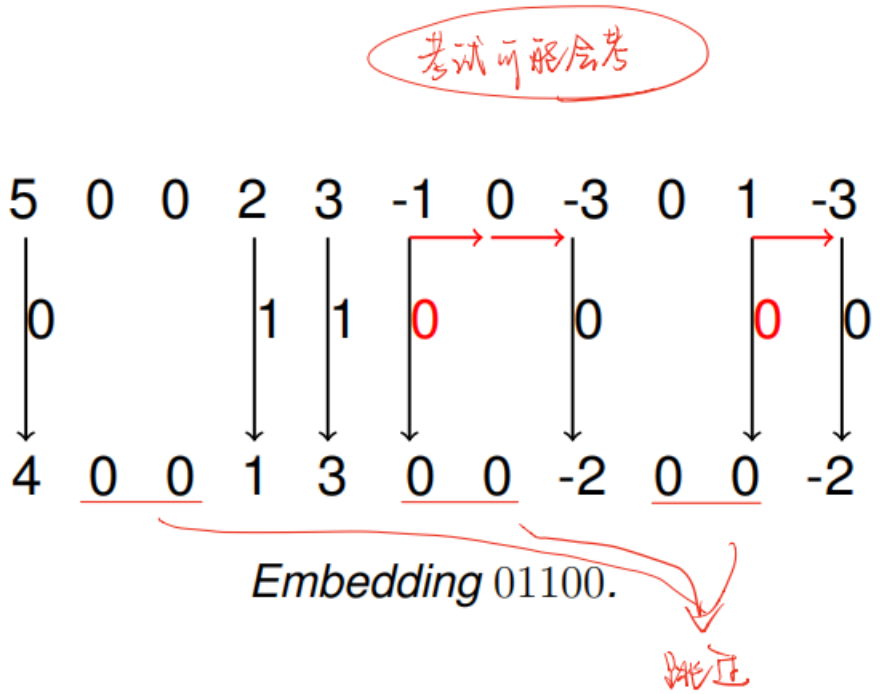
概率分布均匀的情况下，需要的改动就多，ee就小

- Jsteg：相邻两个之间改动，缺点是造成bin内变得平均
- F3

F3



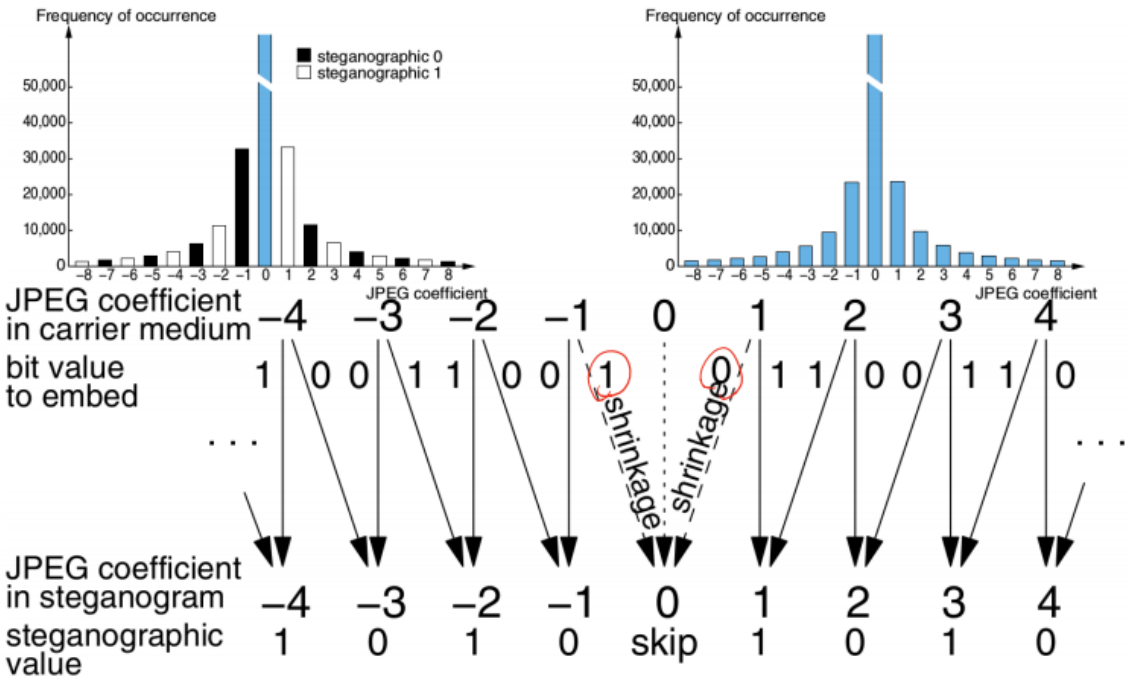
F3 Algorithm



但是F3造成0变多

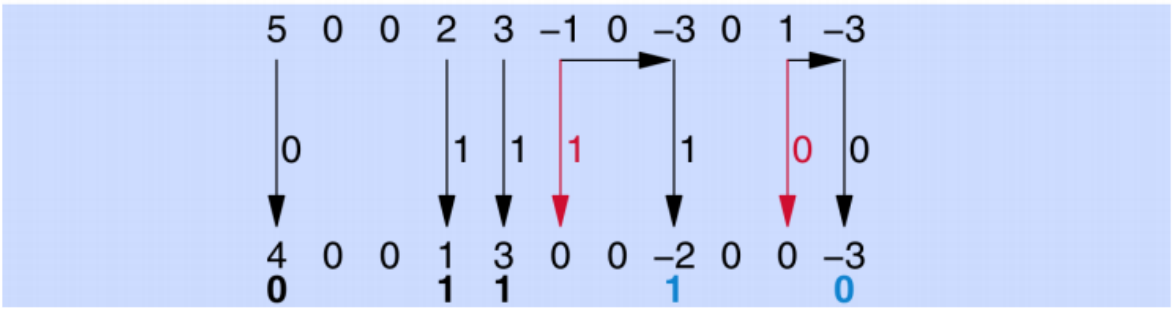
- F4

F4



F4 Algorithm

- Steganographic interpretation
  - Positive coefficients: LSB
  - Negative coefficients: inverted LSB
- Skip 0, adjust coefficients to message bit
  - Decrement positive coefficients
  - Increment negative coefficients
  - Repeat if shrinkage occurs



Matrix Encoding F5算法

Matrix Encoding

Embedding b_1, b_2 to x_1, x_2, x_3 with at most 1 change.

$$b_1 = LSB(x_1) \text{ XOR } LSB(x_2)$$
$$b_2 = LSB(x_2) \text{ XOR } LSB(x_3)$$

- Four equal probability cases.
- Change x_i accordingly.

$$b_1 = LSB(x_1) \text{ XOR } LSB(x_2)$$
$$b_2 = LSB(x_2) \text{ XOR } LSB(x_3)$$

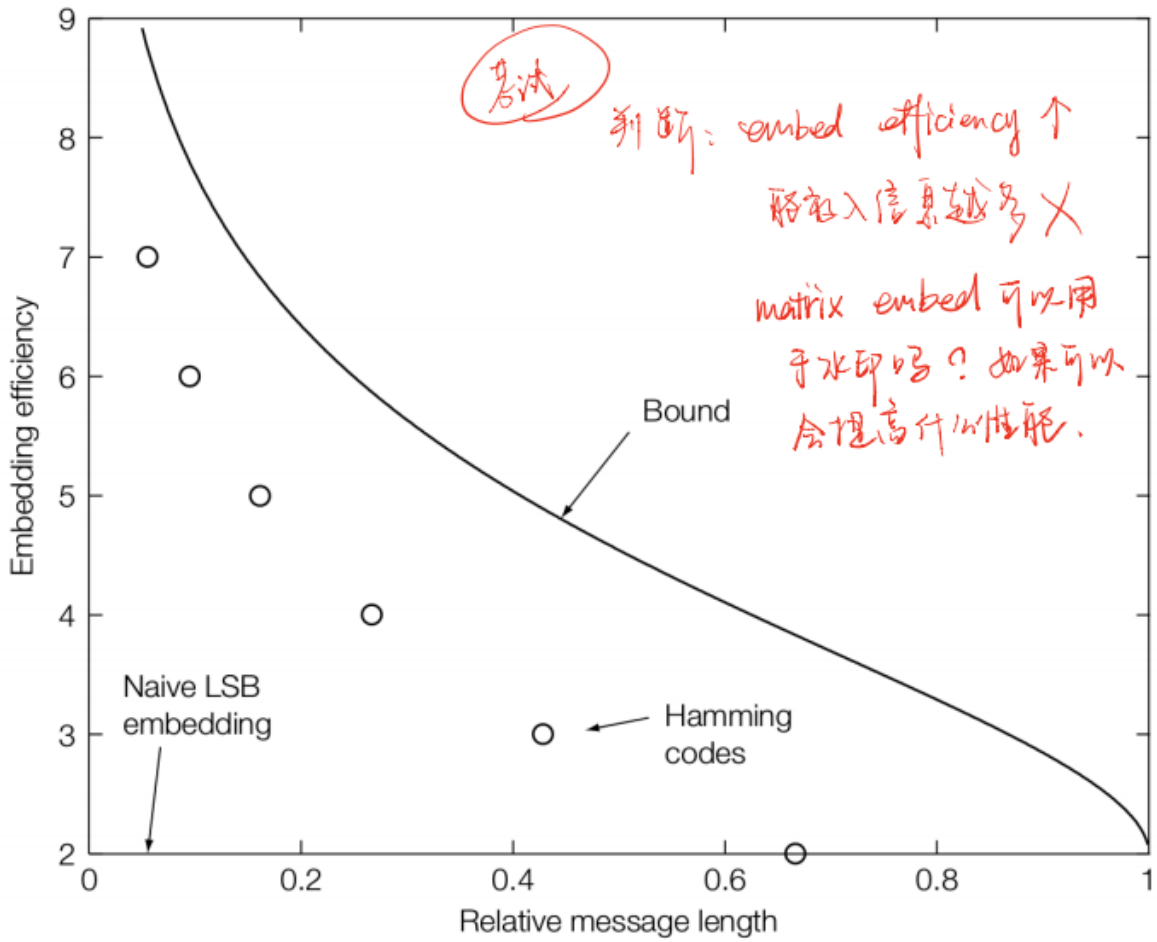
0,0	1,0	0,1	1,1
/	$\bar{x}_1$	$\bar{x}_3$	$\bar{x}_2$

Efficiency:

$$2/(3/4) = 8/3 > 2.$$

前面数学推导不会考

Illustration



Matrix Embedding 算法

考点

In $\mathbf{x}$, we only change part of it.

- Dry part: $\mathbf{x}[j], j \in \mathcal{J} \subset \{1, \cdots, n\}$.
  - Can be changed.
- Wet part: $\mathbf{x}[j], j \notin \mathcal{J}$.
  - Cannot be changed, i.e. fixed.

Thus the change $\mathbf{v} = \mathbf{y} - \mathbf{x}$ has the property:

$$\mathbf{v}[j] = 0, j \notin \mathcal{J}.$$

P代表排列，重组v，能改的部分放到一起，不能改的置0

考试 不会解方程，记到 H 即停 or 简单数据.

$$\mathbf{Dv} = \mathbf{m} - \mathbf{Dx} = \mathbf{z}$$

$$(\mathbf{DP^{-1}})(\mathbf{Pv}) = \mathbf{z}$$

$$(\mathbf{H} \quad \mathbf{K}) \begin{pmatrix} \mathbf{u} \\ 0 \end{pmatrix} = \mathbf{z}$$

$$\mathbf{H}_{m \times |\mathcal{J}|} \mathbf{u} = \mathbf{z}.$$

Choosing the solution with the minimal number of changes.

Perturbed Quantization

chemes known today.

$$J = \{j | j \in \{1, \cdots, n\},$$
$$\mathbf{u}[j] \in [L + 0.5 - \epsilon, L + 0.5 + \epsilon], L \in \mathbb{Z}\}.$$

CHAPTER 13 Steganalysis

一些简单的概念性的知识（感觉不会考）

False alarm ==== False positive

False detection ==== False negative

Targeted Steganalysis 针对某种算法寻找技术 （eg. LSB 直方图）

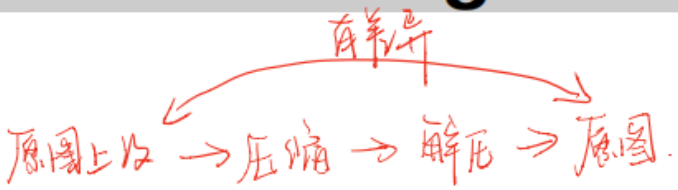
Blind Steganalysis 机器学习数据集

Stego Key 和work大小有关

Forensic Steganalysis 窃听

Cover Work Choosing 图需要大（能放足够多信息）； 但不能过大（会被检测出原图）

Cover Work Choosing



Spatial domain LSB on a decompressed JPEG.

- Spatial vs DCT: many to one.
- Re-compress it into JPEG.
- Decompress it back: the original cover work.
- Shorter message is more easy to detected!

一些检测隐写术的技术

Sample Pairs Analysis

Giving a sequence of values $s_1, s_2, \cdots, s_n$.

- All adjacent pairs
  $\mathcal{P} = \{(u, v) = (s_i, s_{i+1}), 1 \leq i \leq n\}$.

  $$(s_1, s_2), (s_2, s_3), \cdots, (s_{n-1}, s_n).$$

- Partition of $\mathcal{P}$:

	$v\%2 = 0$	$v\%2 = 1$
$u = v$	$\mathcal{Z}$	$\mathcal{Z}$
$u < v$	$\mathcal{X}$	$\mathcal{Y}$
$u > v$	$\mathcal{Y}$	$\mathcal{X}$

Continue partitioning $\mathcal{Y}$ into $\mathcal{W}, \mathcal{V}$.

- $\mathcal{W}$: A small subset of $\mathcal{Y}$.

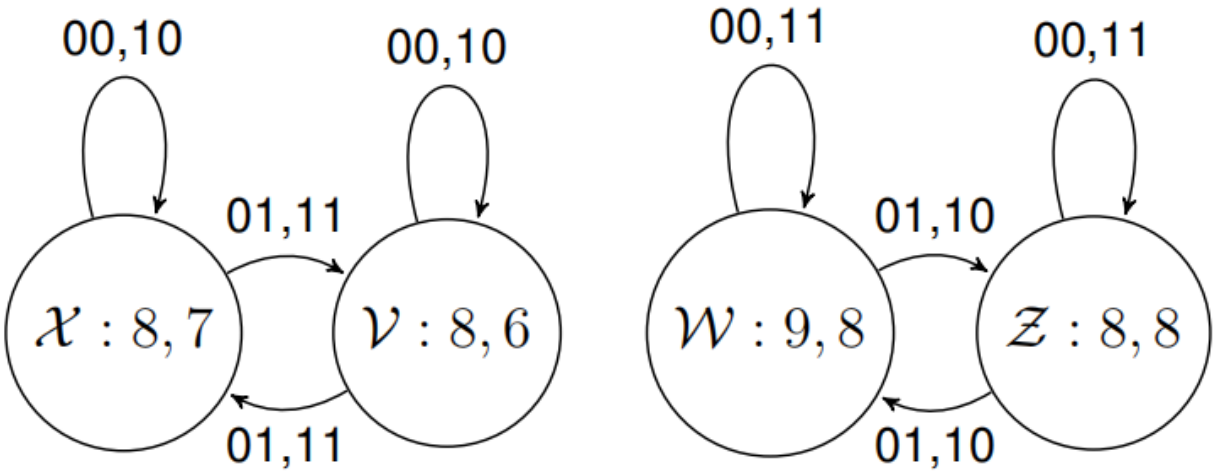
  $$\{(u = 2k, v = 2k+1) \vee (u = 2k+1, v = 2k), k \in \mathbb{Z}\}.$$

  or

  $$|u - v| = 1.$$

- $\mathcal{V} = \mathcal{Y} - \mathcal{W}$.

The bin of LSB: $\mathcal{W} + \mathcal{Z}$.



$$\begin{aligned}\rho(00,\mathcal{P}) &= \left(1-\tfrac{q}{2}\right)^2\\ \rho(01,\mathcal{P}) &= \tfrac{q}{2}\left(1-\tfrac{q}{2}\right)\\ \rho(10,\mathcal{P}) &= \tfrac{q}{2}\left(1-\tfrac{q}{2}\right)\\ \rho(11,\mathcal{P}) &= \left(\tfrac{q}{2}\right)^2\end{aligned} \Rightarrow \begin{cases} 00,10: & \rho_{00}+\rho_{10} = 1-q/2\\ 01,11: & \rho_{01}+\rho_{11} = q/2\\ 00,11: & \rho_{00}+\rho_{11} = 1-q+q^2/2\\ 01,10: & \rho_{01}+\rho_{10} = q(1-q/2)\end{cases}$$

注意：

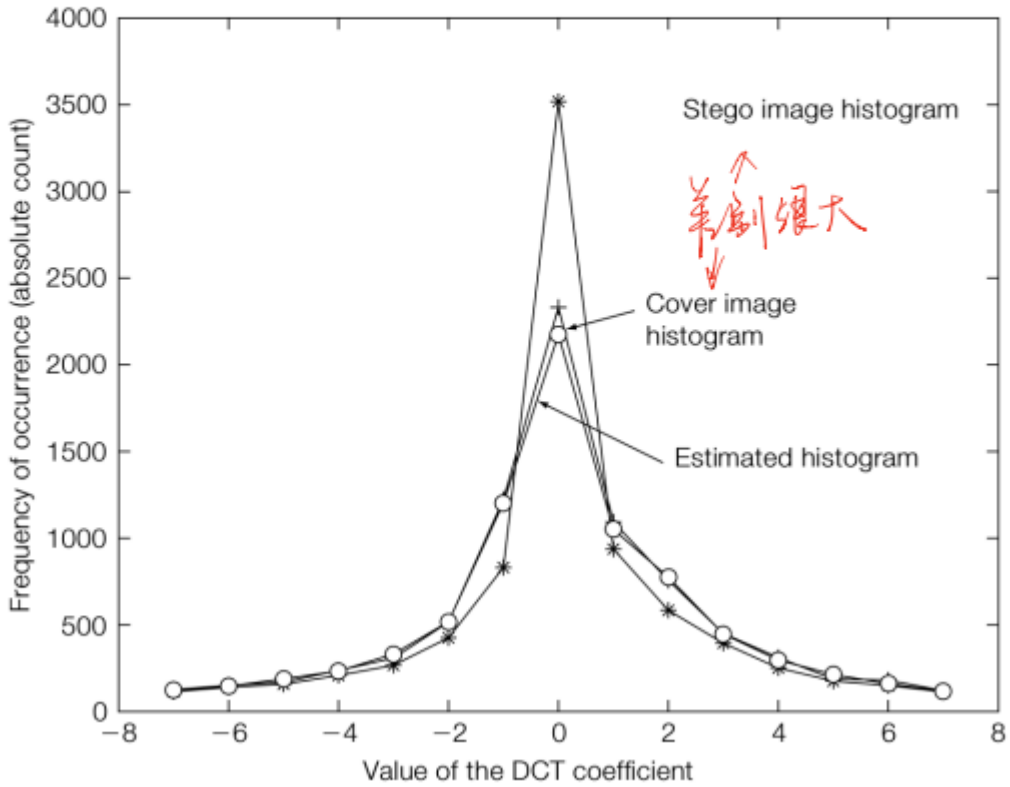
- If $\gamma = 0$, $|\mathcal{X}| = |\mathcal{X}'| = |\mathcal{Y}| = |\mathcal{Y}'| = |\mathcal{P}|/2$.

$$0q^2 + 0q + 0 = 0.$$

尽量增多W+Z，方法是选取临近的点对

Blind Steganalysis Using Calibration

- Shift 4 pixels and re-compress.



隐写：尽量选择噪声多的work来隐写

检测隐写：也可以通过添加噪声来设置样本，用分类器进行学习分类