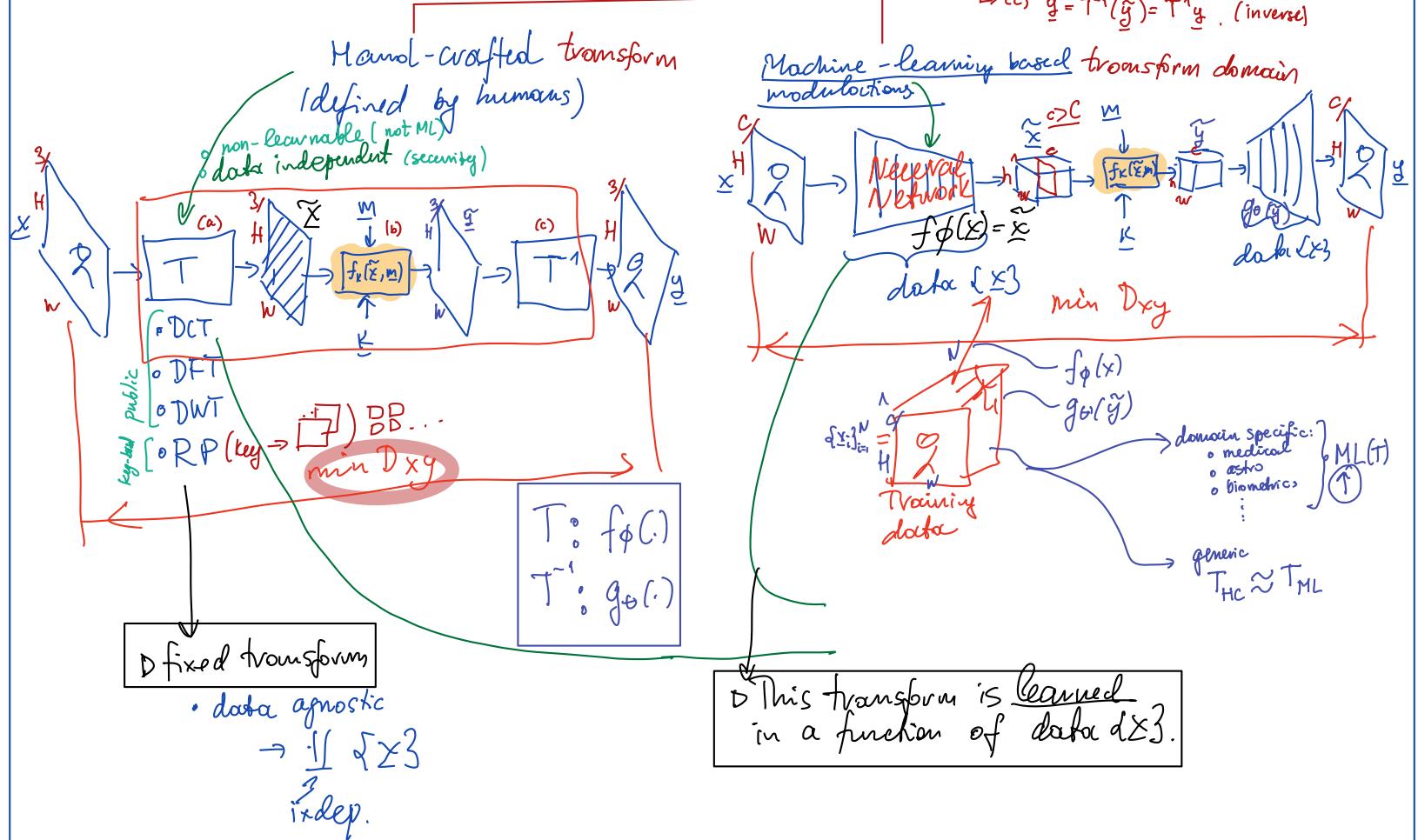


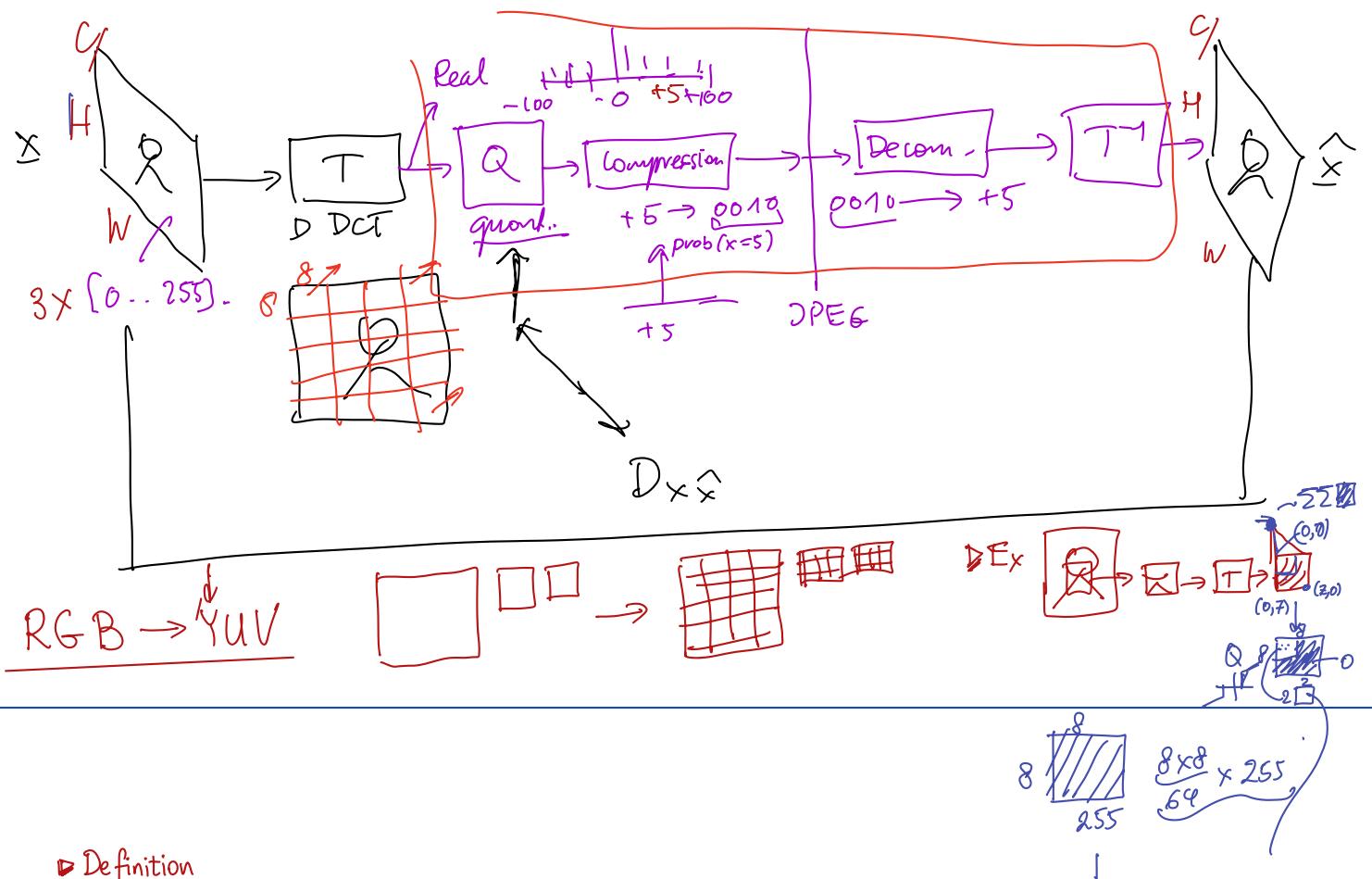
② Types of $f_k(\cdot)$

- (1) Direct domain $y = f_k(x, m)$
- (2) Transform domain: T, T^{-1} , s.t. $TT^{-1} = I$

$$\begin{aligned} &\rightarrow (a) \tilde{x} = T(x) \xrightarrow{\text{mod}} Tx \quad (\text{direct}) \\ &\rightarrow (b) \tilde{y} = f_k(\tilde{x}, m) \\ &\rightarrow (c) \tilde{y} = T^{-1}(\tilde{y}) = T^{-1}\tilde{y}. \quad (\text{inverse}) \end{aligned}$$

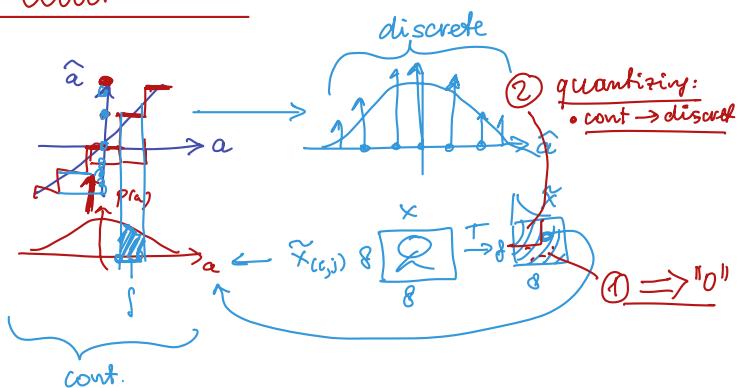


Link to lossy (JPEG) image compression



► Definition

Quantization



$$\triangleright f_K(\tilde{x}, m) = \frac{Q(\tilde{x}, m)}{K} - \text{quantization based embedding.}$$

• Dither quantizer,

$$Q(\tilde{x} + d)$$

$$d \in (k, m)$$

+0+0+0+0+

Recall:

- ▷ direct domain ($T=I$)
- ▷ additive modulation
- ▷ quantization modulation

$$y = \underline{x} + \underline{w}$$

$\underline{m}, \underline{k}$

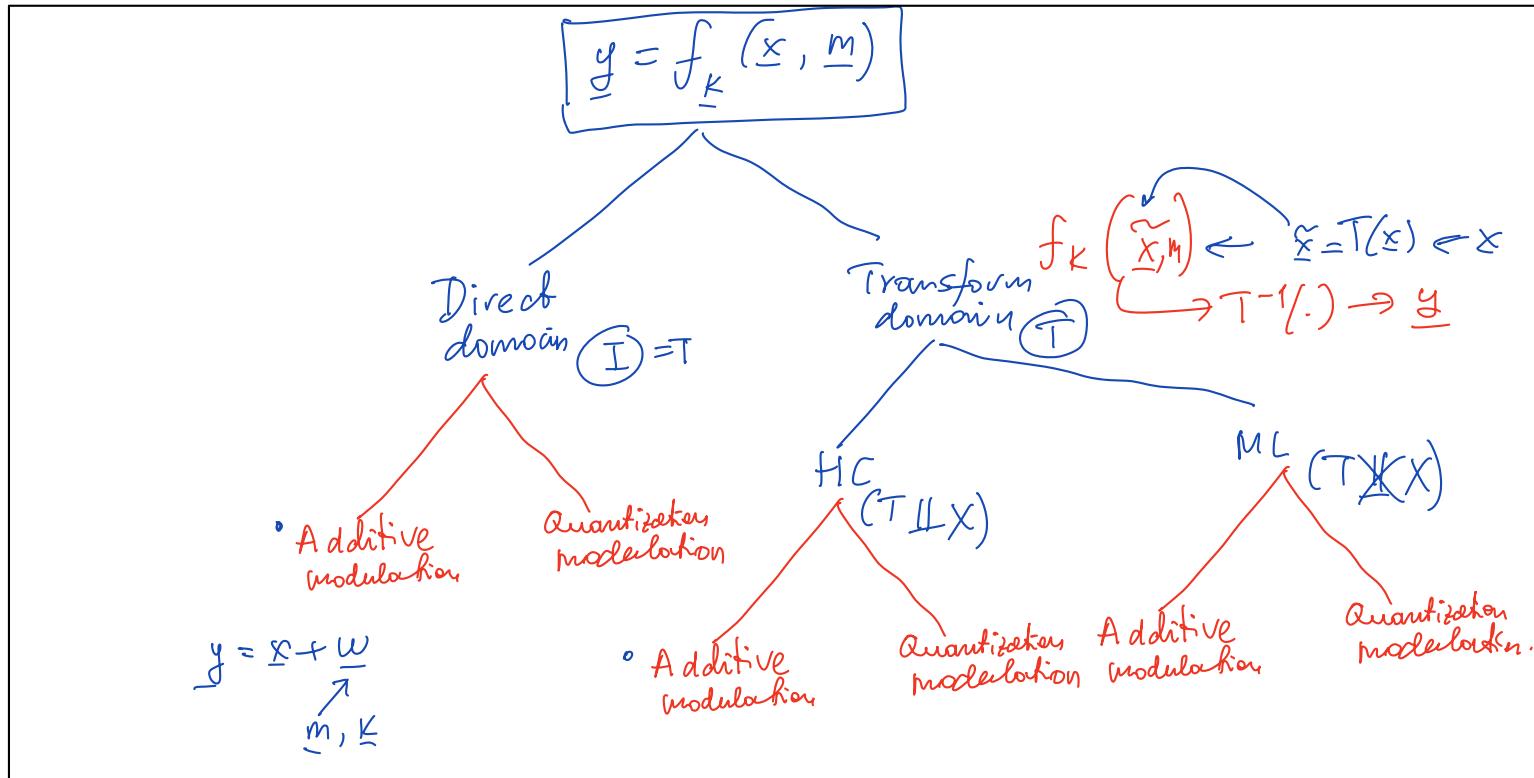
in the direct / image domain.

$$\underline{m} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$\underline{k} \rightarrow (x_1, y_1) \quad 0 \rightarrow -1$$

$$1 \rightarrow +1$$

Table: general classification of DM modulation techniques.

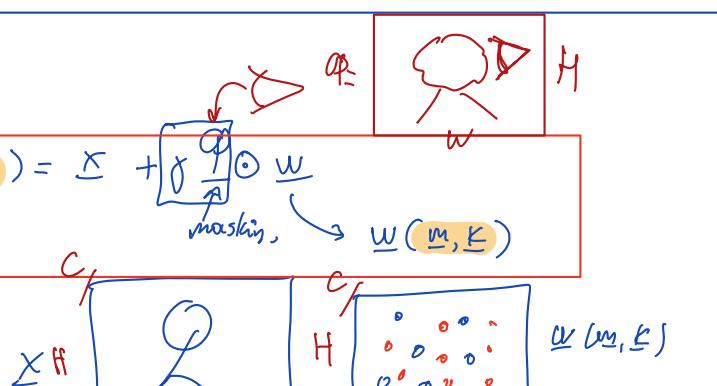


1) Additive modulation

1.1. Direct domain:

$$y = f_{\underline{k}}(\underline{x}, \underline{m}) = \underline{x} + \underline{w}$$

masking, $\underline{w}(\underline{m}, \underline{k})$



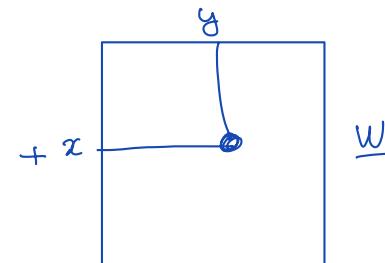
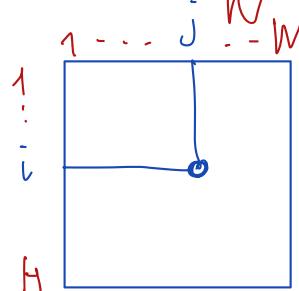
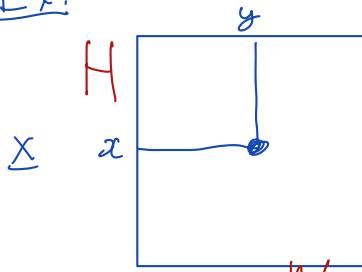
$$y = T^{-1}[T(\underline{x})] = (\underline{x}) + T^{-1}(\tilde{f} \tilde{\varphi} \odot \tilde{w})$$

1.2. Transform domain.

$$y = f_{\underline{k}}(\underline{x}, \underline{m}) = T^{-1}(T(\underline{x}) + \tilde{f} \tilde{\varphi} \odot \tilde{w})$$

$\approx T(a\underline{x} + b\underline{y}) = aT(\underline{x}) + bT(\underline{y})$

D Ex:

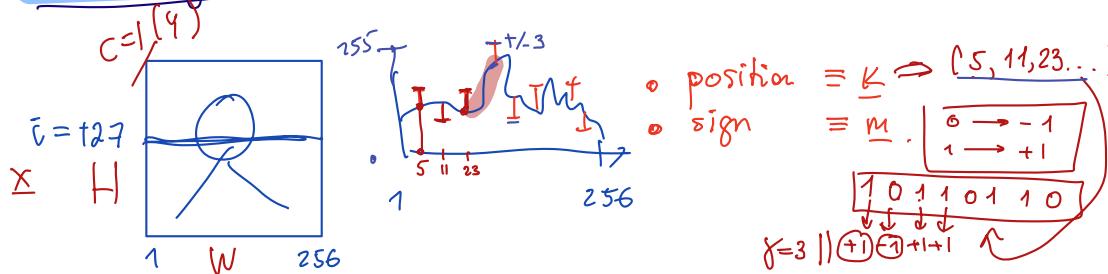


$$y[i,j] = x[i,j] + w[i,j]$$

$$\epsilon[0 \dots 255] \xrightarrow{\downarrow} x \cdot \varphi[i,j] \in [0 \dots 1]$$

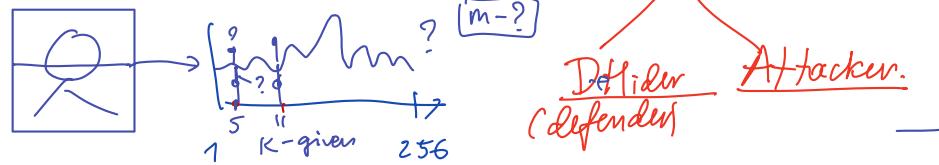
$$\begin{cases} > 1 \\ \pm 3 \\ \leq -1 \end{cases}$$

① Embedding (encoding) $f_K(x, w)$



② Extraction (decoding)

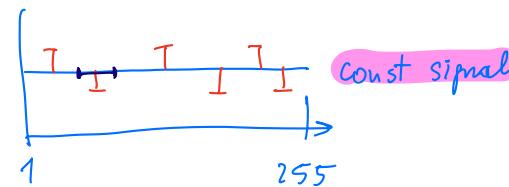
The extraction of WM is NOT a trivial problem.



Why?

Intuition.

Suppose!



$$0 \rightarrow -1$$

$$1 \rightarrow +1$$

$$y = x + g \varphi w$$

$$\hat{w} = g(g)$$



Extraction on the window \rightarrow "local mean".

Local mean

(a)

$$y = x + w$$

$$\hat{x} = \frac{1}{3} \sum_{i=1}^3 x_i$$

$$\hat{w} = y - \hat{x} = (127 - 7) - (127 - \frac{7}{3}) = -7 + \frac{7}{3} = -\frac{14}{3}$$

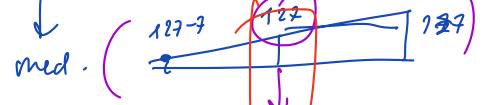
Local media.

(b)

Watermark w faces a strong interference from the side of host image x .

127

$$y_w = [(127, (127-7), 127)]$$

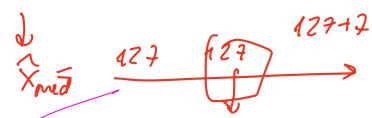


$$\text{local mean } \hat{x}_{\text{med}} = 127$$

$$\hat{w} = y - \hat{x}_{\text{med}} = (127-7) - 127 = -7$$

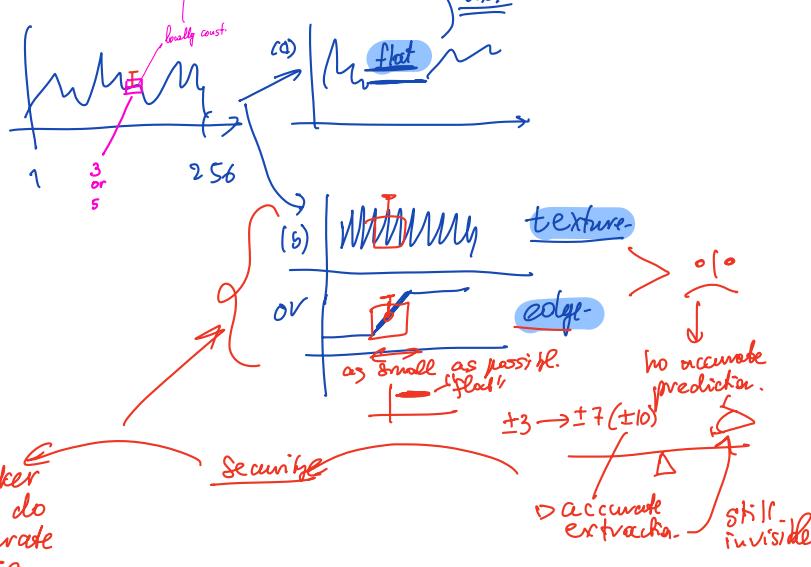
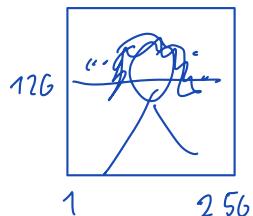
127

$$y_w = (127, (127+7), 127)$$



$$\hat{w} = y - \hat{x}_{\text{med}} = (127+7) - 127 = +7$$

D Real signals



*

D In case of image:

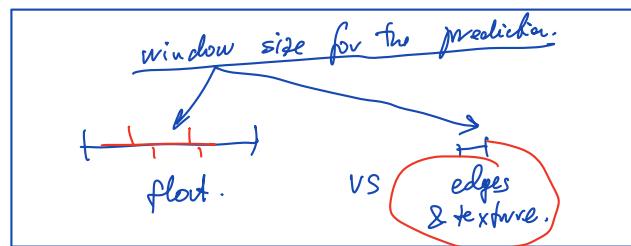
$$g = x + w = x + \epsilon \quad \text{noise.}$$

[jP]: denoiser: $w \equiv \epsilon$ as noise.

(a) $\hat{x} = \text{denoiser}(g)$ Matlab: wiener2($\frac{1}{4}, [33], \frac{\epsilon^2}{5 \times 3}$, auto.)

(b) $\hat{w} = g - \hat{x} = x + \epsilon - \hat{x}$
5.1. if $\hat{x} = x$: $\hat{w} = \epsilon$.

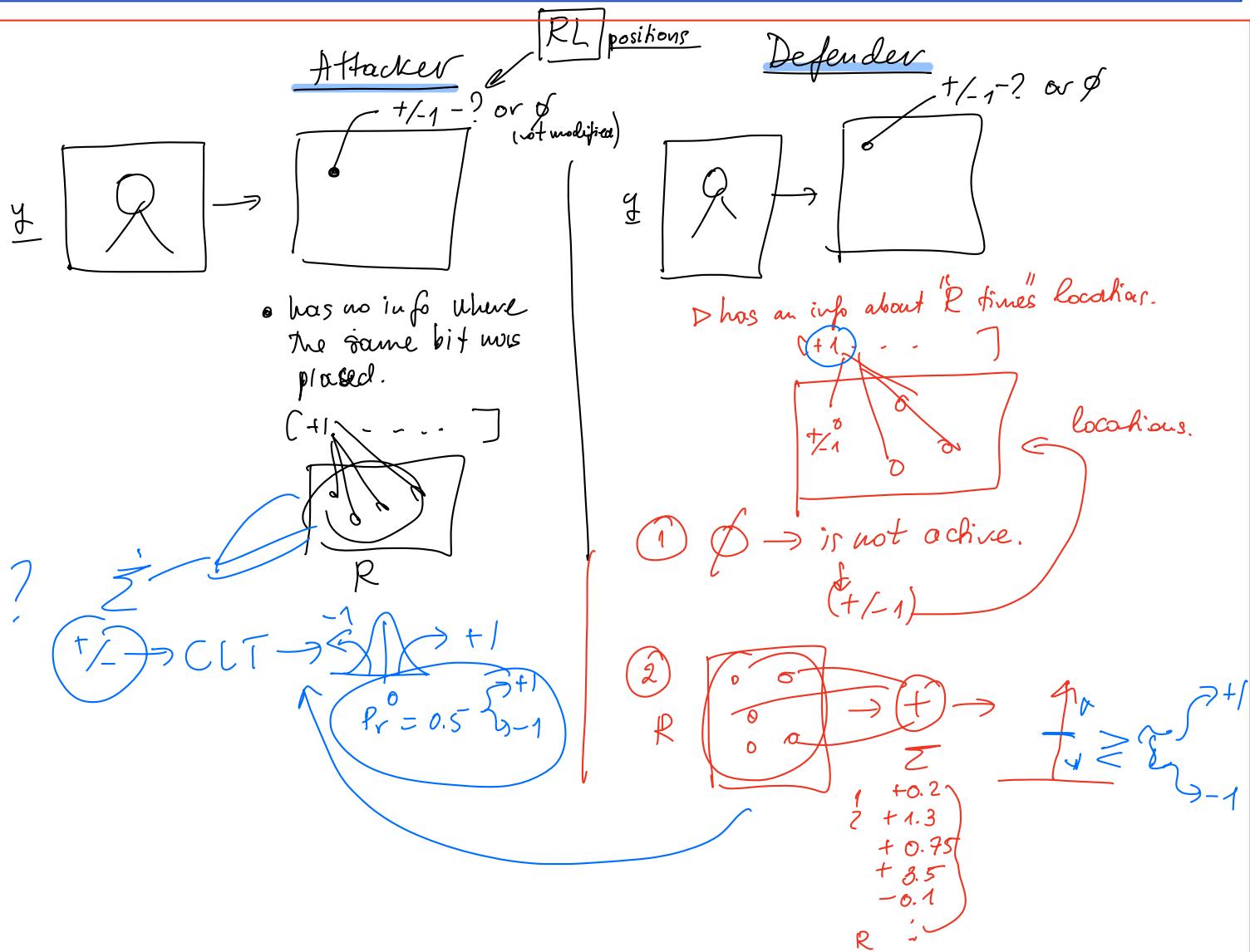
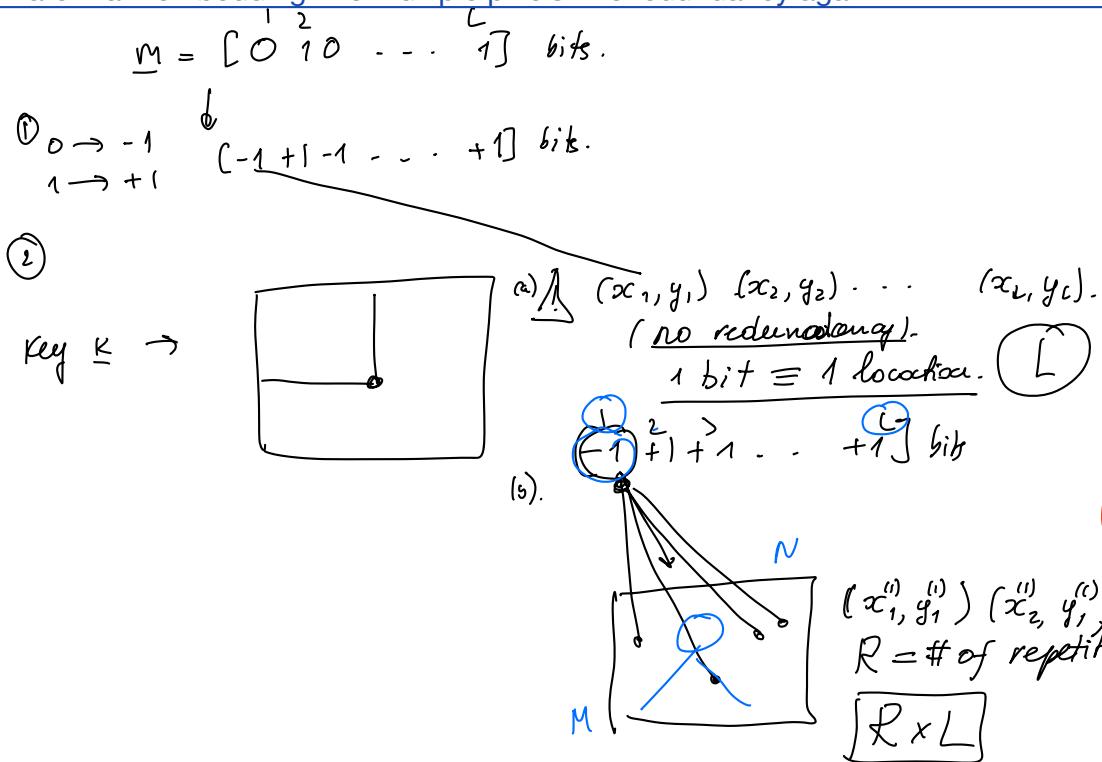
6.2: If $\hat{x} = x + \beta_{\text{est}}$:
 $\hat{w} = g - \hat{x} = g + w - x - \beta_{\text{est}} = w - \beta_{\text{est}}$



repetitive embedding.
one bit (+1)

$$\text{multiple times} \quad (+3.5 +5.7 \rightarrow 13 +25.7) = \sum \frac{1}{4} \uparrow$$

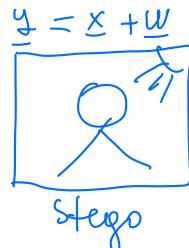
"Distributed" watermark embedding into multiple pixels: the redundancy again



D Robustness to geometrical attacks.

CIP: Theme S

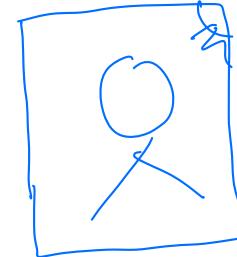
Given



(a) affine
(b) projective

Geometrical attack

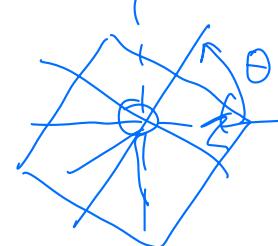
rescale



or

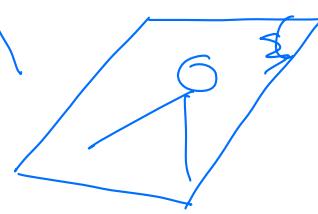


rotation

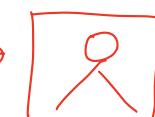
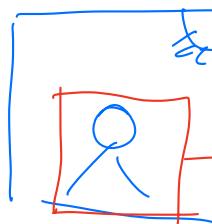


shearing

skipping



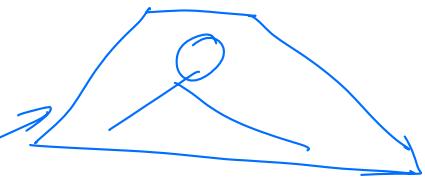
warping



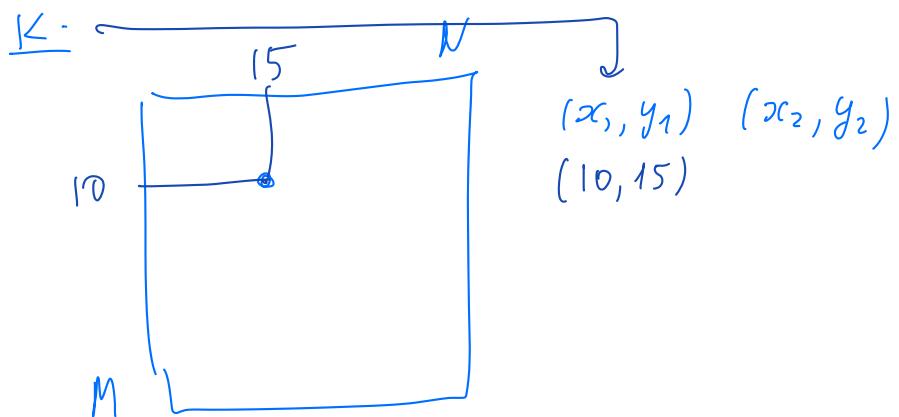
Practical use case:



→ projective



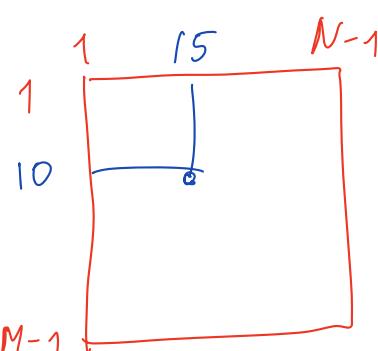
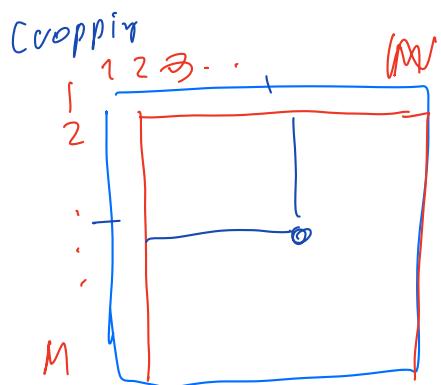
①



②

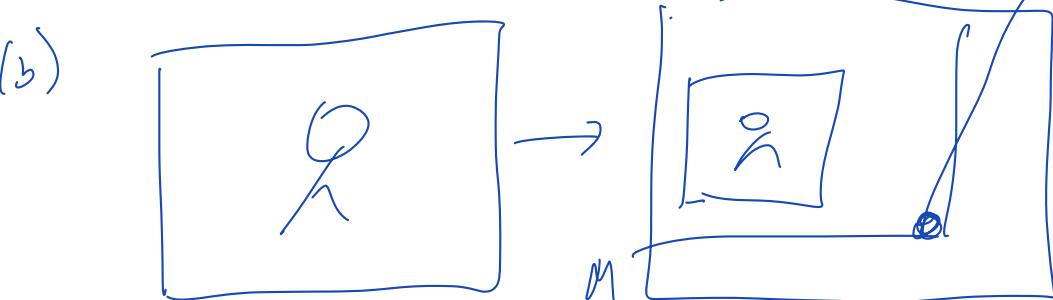
Extraction

(a)

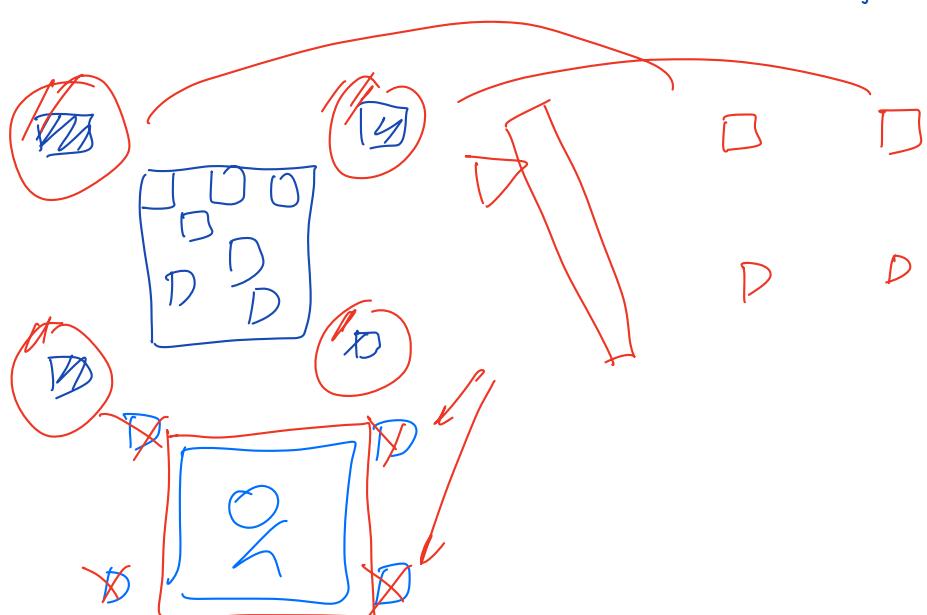


(b)

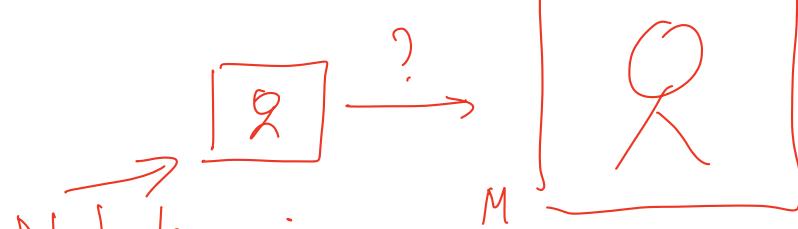
$K \rightarrow (x_1, y_1), (x_2, y_2) = \dots$



QR codes

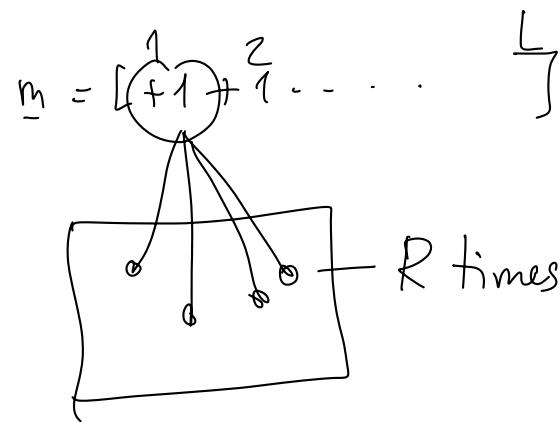


D Solution:



Not knowing what was done with this image??

i) label A



= For redundancy.
(errors of prediction in view of interference with x).

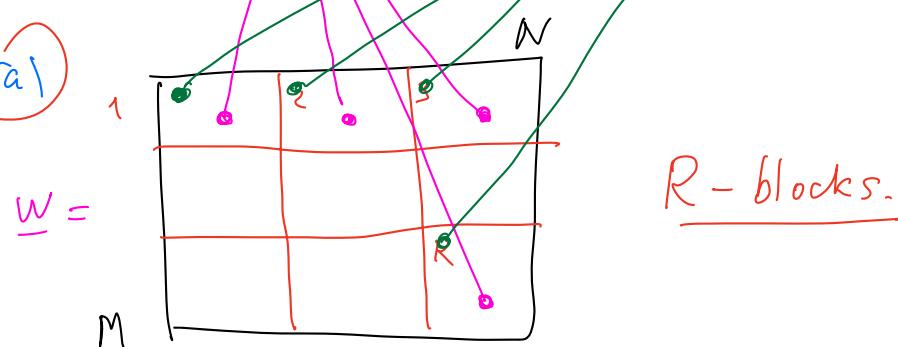
2). Embedding

$$\underline{m} = [f_1 \ f_2 \ \dots \ f_{L-1} \ f_L]$$

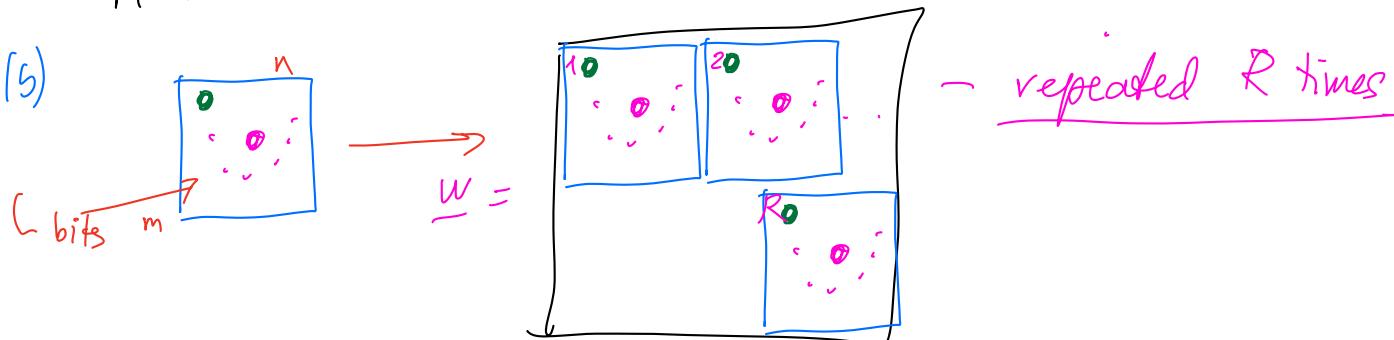
R times.

Covered placement.

(a)



(b)



$$\underline{y} = \underline{x} + \underline{w}$$

Extraction

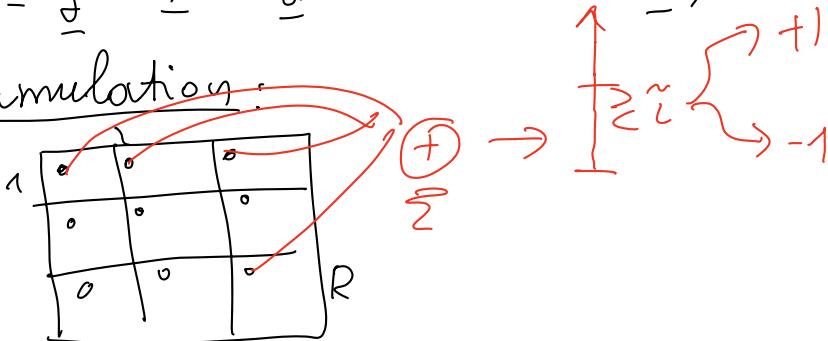
No geom. attacks

$$1) \quad \underline{y} = \underline{x} + \underline{w}$$

2) Prediction of $\hat{\underline{w}}$:

$$\hat{\underline{w}} = \underline{y} - \hat{\underline{x}} = \underline{y} - \text{denoiser}(\underline{y}) \quad | \text{ wiener2(-)}$$

3) Accumulation:

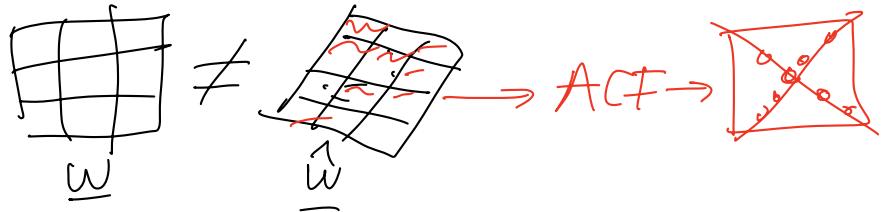


With geom. attacks -

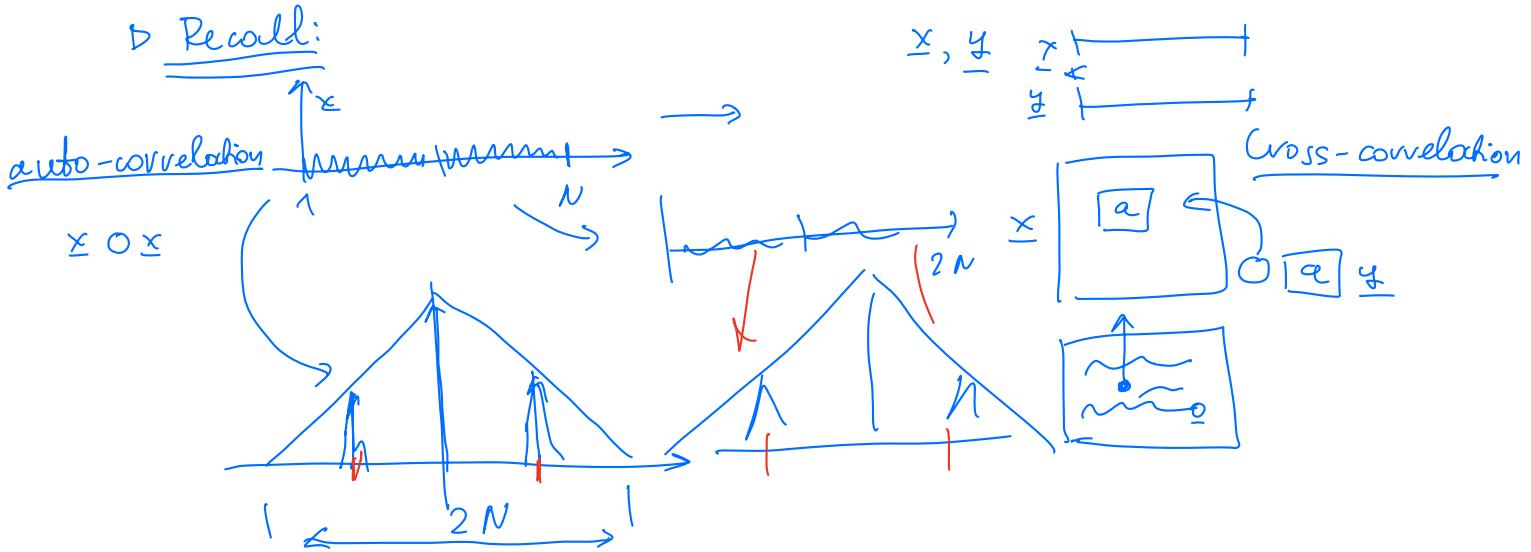
$$1) \quad \underline{y} = G(\underline{x} + \underline{w}) \quad \boxed{2} \rightarrow \boxed{?}$$

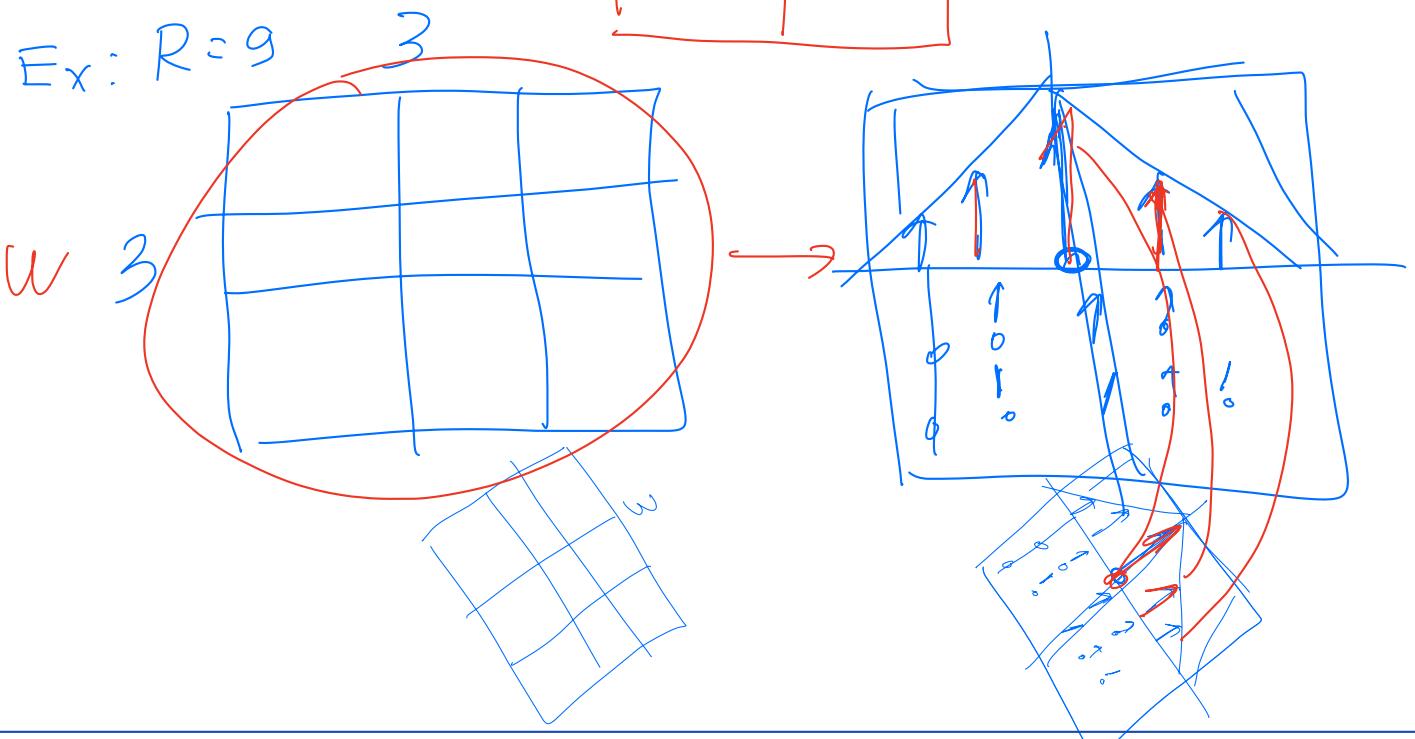
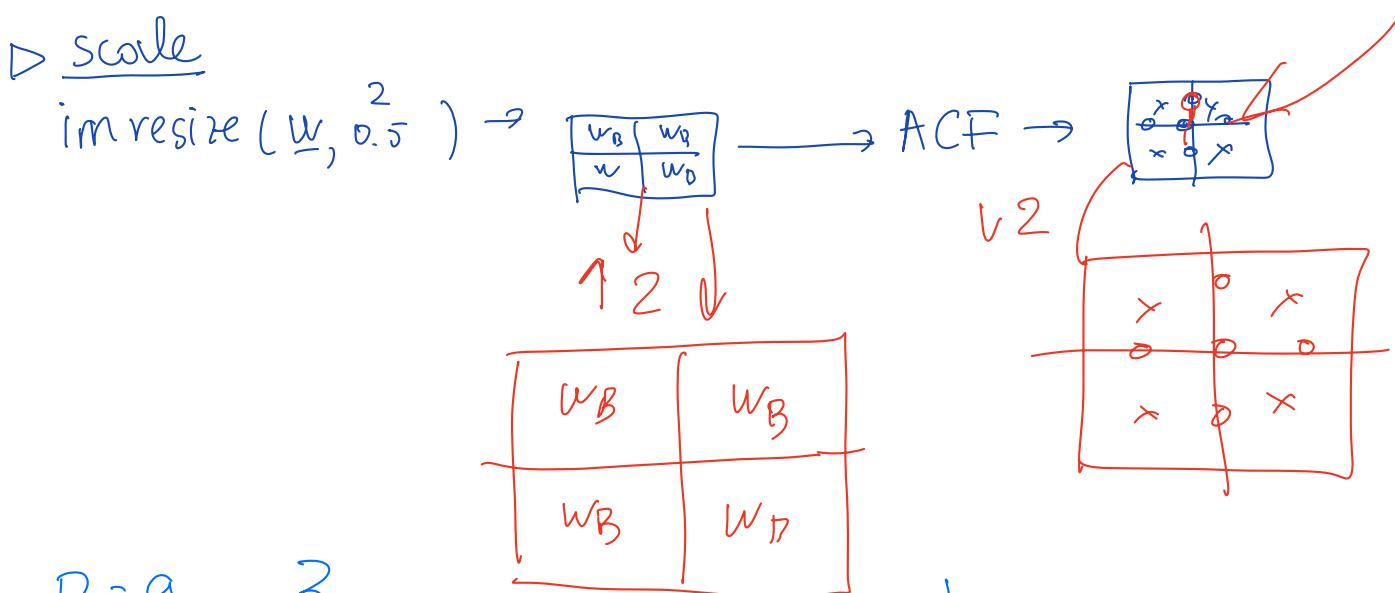
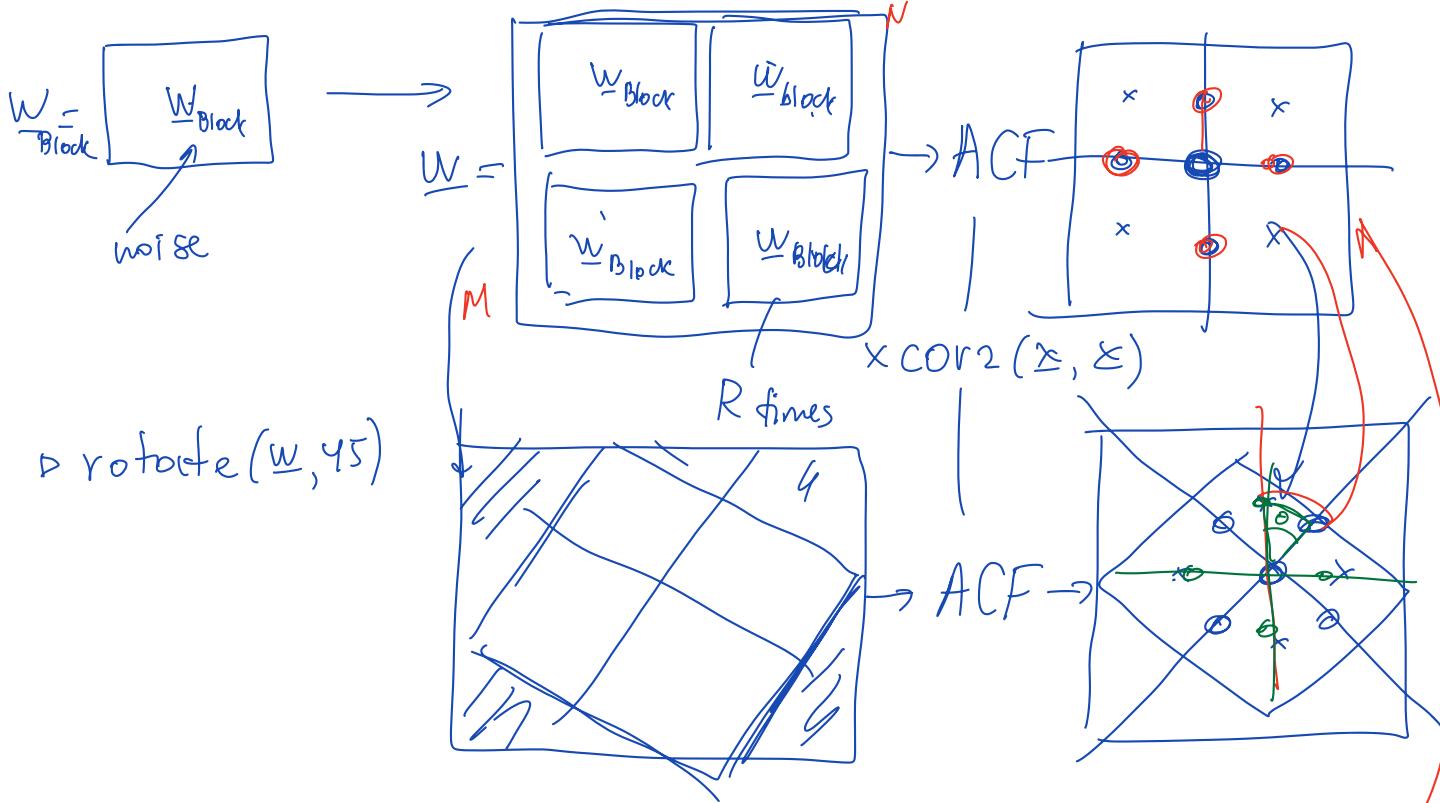
2) Prediction

$$\hat{\underline{w}} = \underline{y} - \hat{\underline{x}} = \underline{y} - \text{denoiser}(\underline{y}) \quad | \text{ wiener2(-)}$$

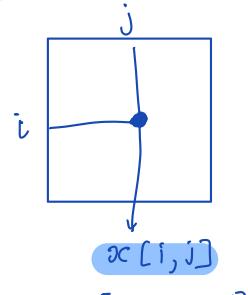


Recall:





2) Quantization modulation



[0 ... 255]

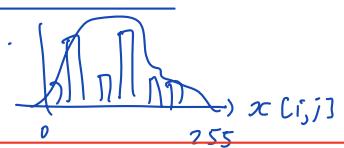
• Direct domain:

▷ additive modulation

$$y(i, j) = \underline{x}(i, j) + w(i, j) \quad (\underline{m}, \underline{k})$$

▷ quantization modulation

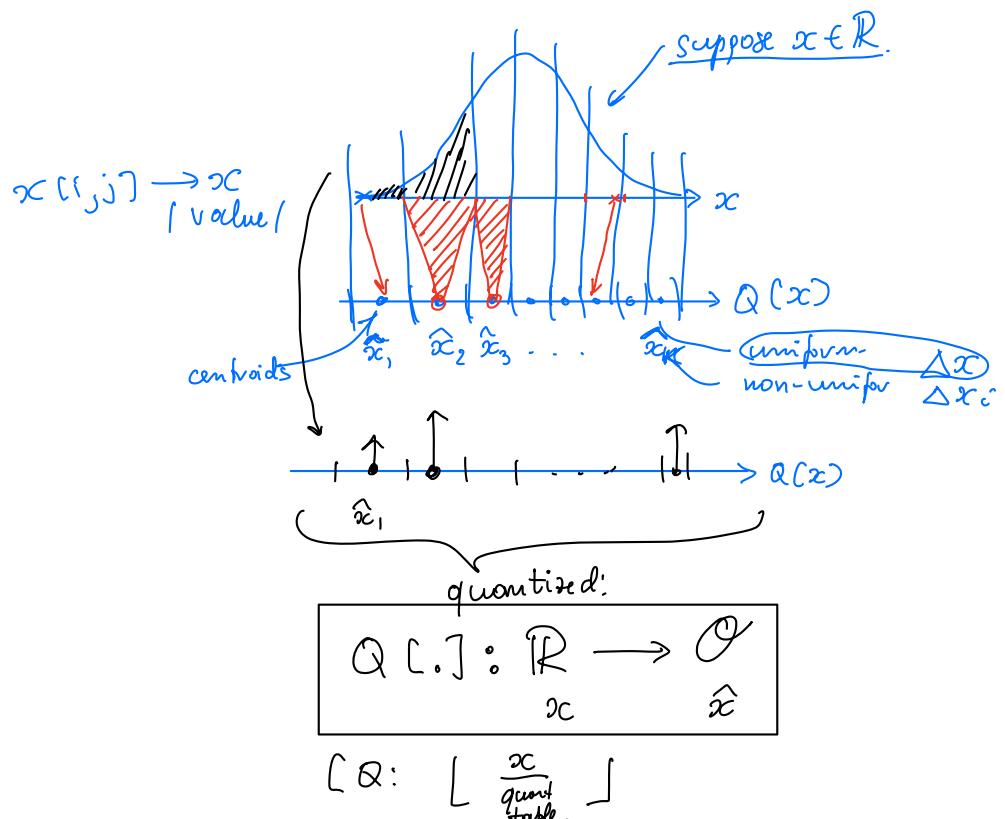
◦ histogram.



$$y(i, j) = \begin{cases} Q_0[x(i, j)], & \text{for } m=0 \\ Q_1[x(i, j)], & \text{for } m=1 \end{cases}$$

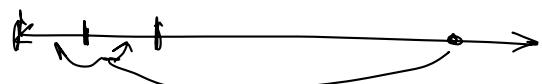
▷ where $Q_0[\cdot]$ for the quantizer
 $Q_1[\cdot]$ for bit 0 or bit 1, respectively

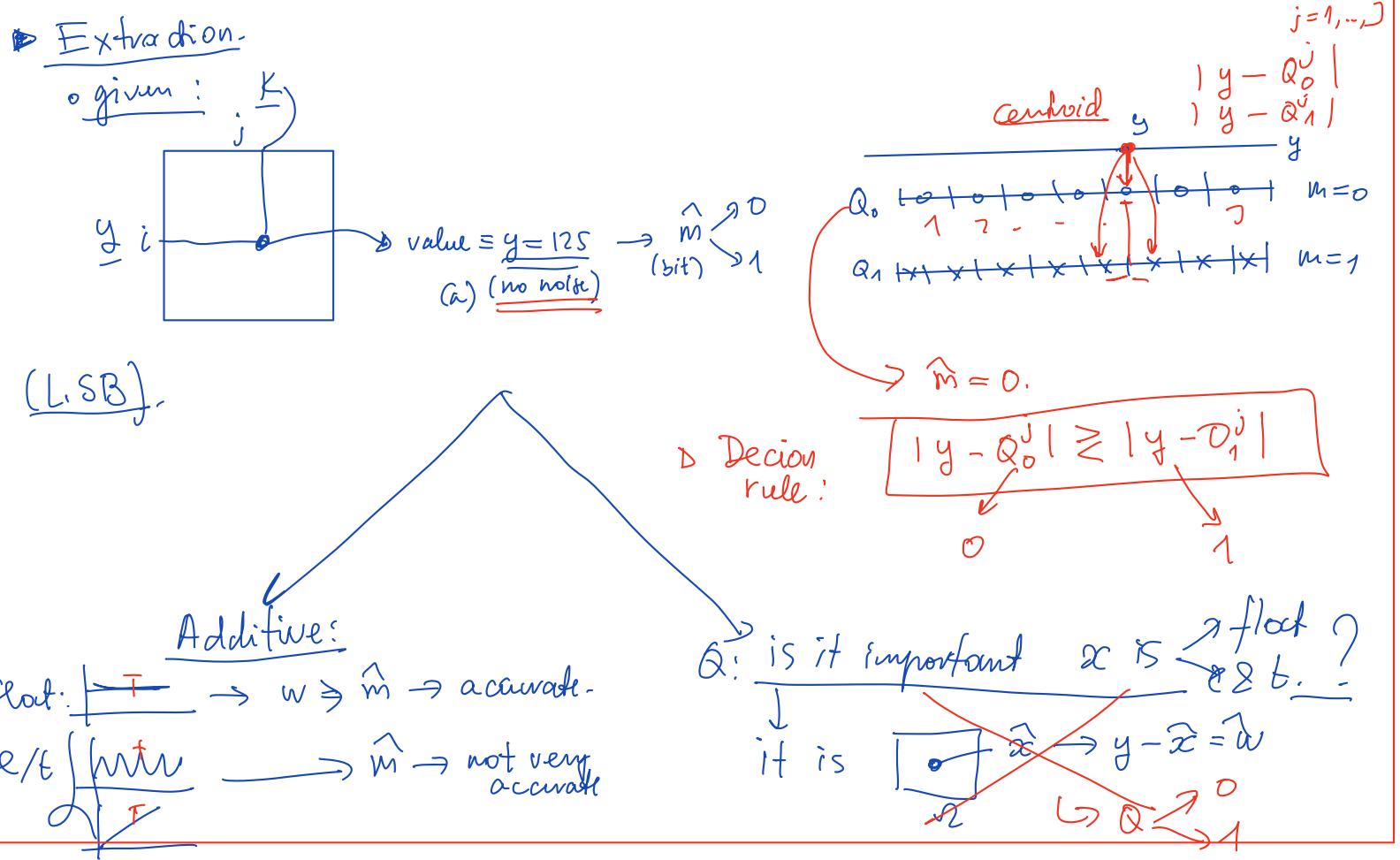
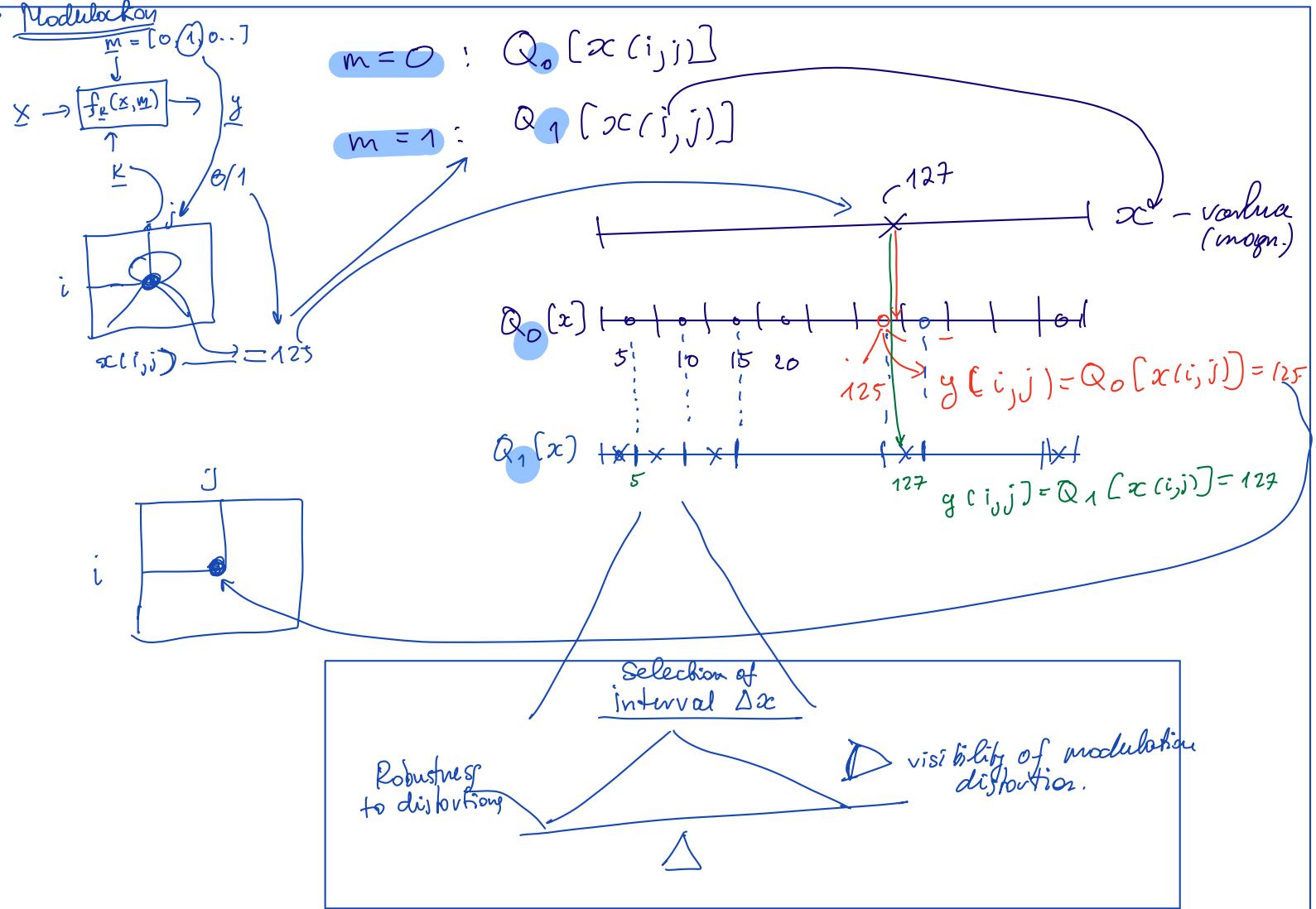
▷ Recall: quantization

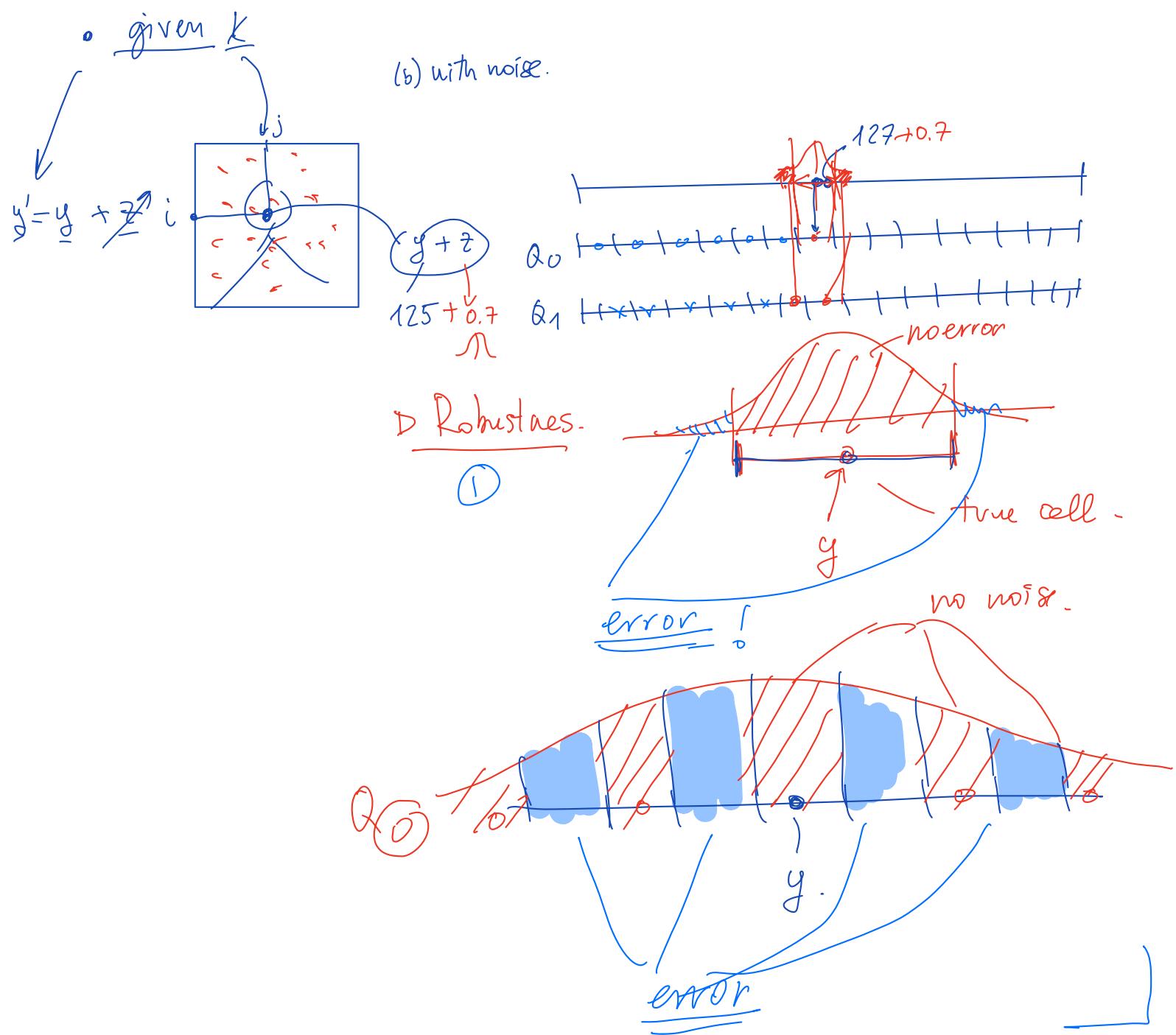


$$Q[\cdot]: \mathbb{R} \rightarrow \mathcal{O}$$

[Q: $\left[\frac{x}{\text{quant table}} \right]$]







D LSB: a part. case of quant. modulation.

① Recall

DH

Direct ✓

A ✓ Q ✓

T

Transform domain.

A Q

$$T^{-1}T = I$$

T_{HC} ↗ ↘
A Q

T_{ML} ↗ ↘
A Q.

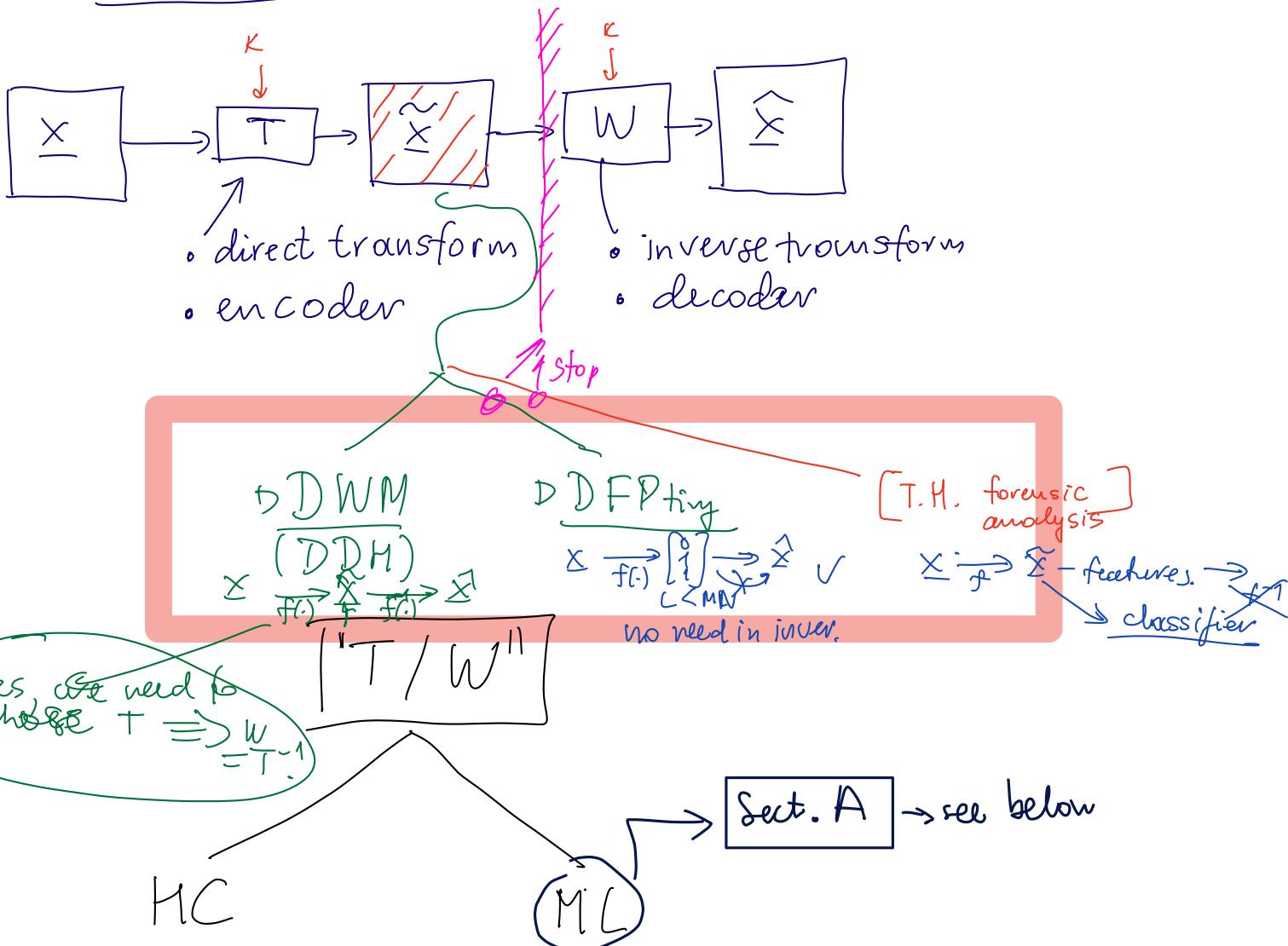
T_{MC}

T_{ML}

T
↑

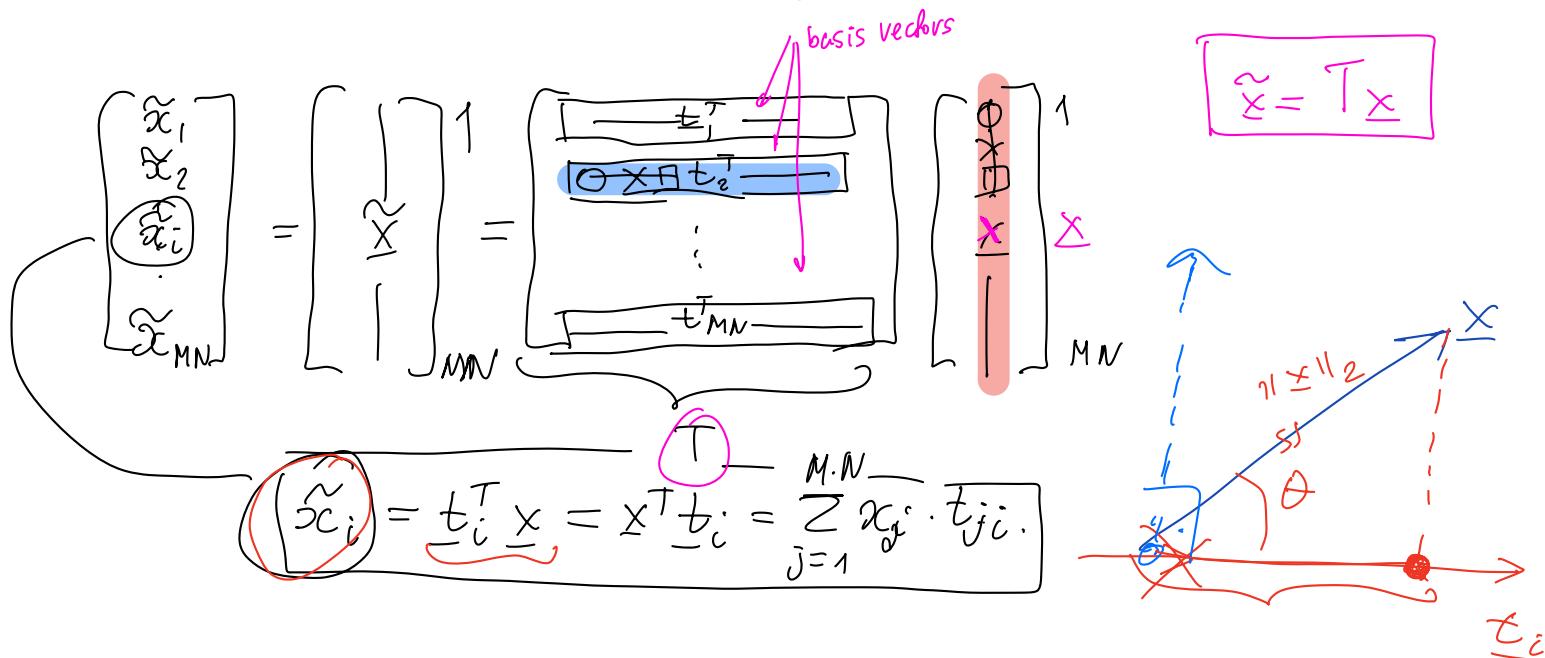
DF Printing

i) Transforms (Defender)



i) HC (hand-crafted = engineered) transform

▷ Recall. $\begin{bmatrix} \underline{x} \end{bmatrix}_M^N \rightarrow \begin{bmatrix} \underline{x}' \end{bmatrix}_1^{MN}$



\triangleright HC Transform: a selection of T (resp. W).

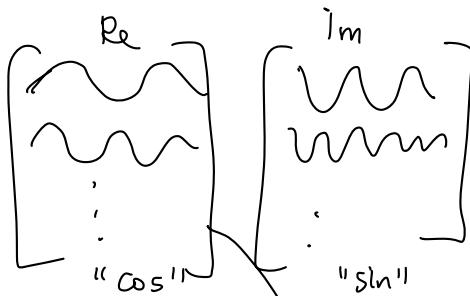
\triangleright "manually" \rightarrow expertise of person.

\triangleright selection is \perp to data X .
(no ML)

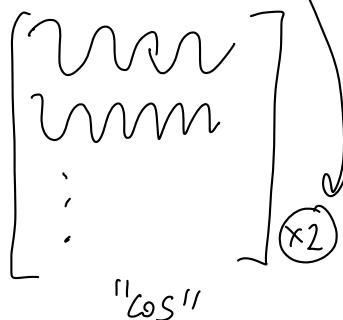
\circ in practice:

T to be:

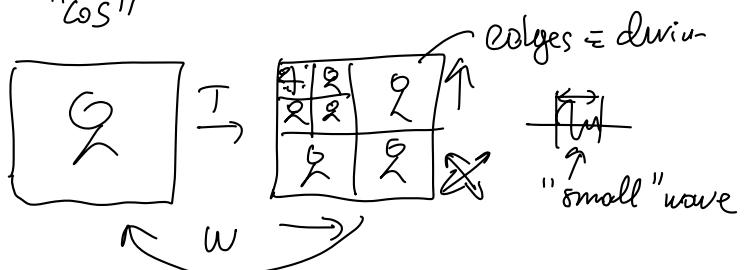
\circ DFT



\circ DCT



\circ DWT
wavelet



\circ Macdonald.

Invertibility

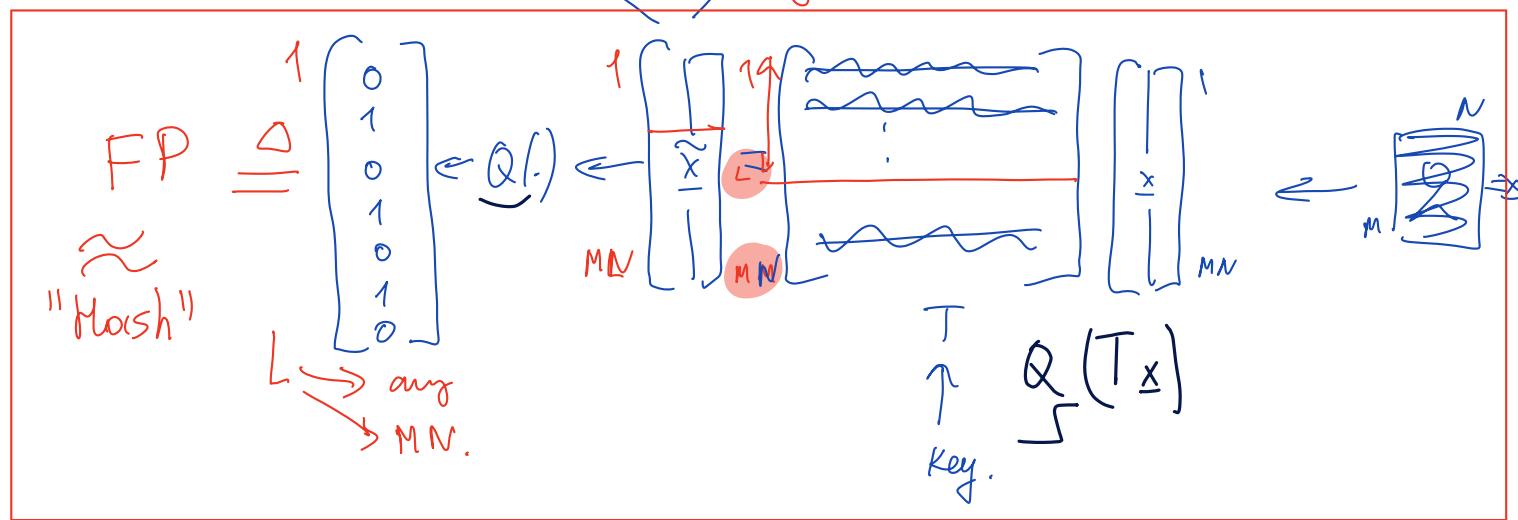
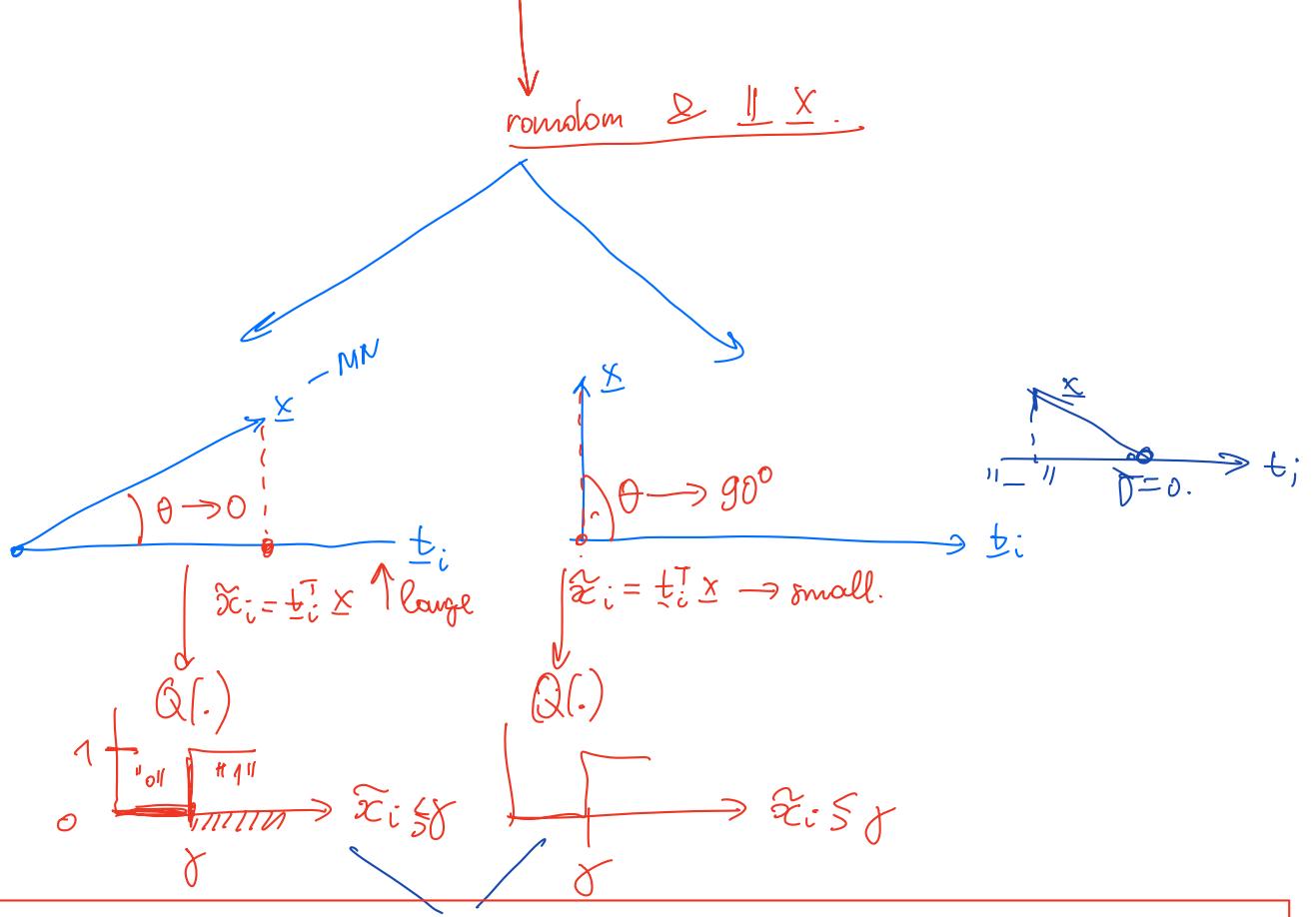
\circ it depends
on the construction
of matrix T . Ex: $T \in \mathbb{R}^{M \times N}$

Random projection

$$\mathcal{N}(0, I_{MN})$$

$$T = \begin{bmatrix} t_1^T \\ t_2^T \\ \vdots \\ t_M^T \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{bmatrix}$$

① $T \perp\!\!\!\perp X$
② $T \leftarrow$ keep
seed(k).
(security).



$$L < M.L \rightarrow T \longrightarrow T^{-1} - ?$$

SVD: $T = U \Sigma V^{-1}$

$$\begin{aligned} T^{-1} &= (U \Sigma V^{-1})^{-1} \\ &= V \Sigma^{-1} U^{-1} \end{aligned}$$

①

$L < M.N$ to avoid a perfect invertibility

②

$\tilde{x} \rightarrow Q(\tilde{x}) \rightarrow_0$

Defender (FP)

$\triangleright \underline{\text{Attacker}} : Q(\tilde{x}) \xrightarrow{\quad} \underline{\tilde{x}} \leftrightarrow \underline{x}$.

Invertability

HC (math).

"SVD":

→ approximate solution (exact).

$\tilde{x} = T^{-1}x$ - linear. equations.

$$\varphi(x) \text{ or } \mathcal{L}(x) = \frac{1}{2} \| \tilde{x} - T^{-1}x \|_2^2$$

$$\begin{aligned} \tilde{x} &= \underset{x \in \mathbb{R}^{MN}}{\operatorname{argmin}} \mathcal{L}(x) \\ &= \underset{x}{\operatorname{argmin}} \underbrace{\frac{1}{2} \| \tilde{x} - T^{-1}x \|_2^2}_{l_2} \end{aligned}$$

(15:13)

ML

$$\cdot \{ \underline{x}_i, Q(\tilde{x}_i) \}_{i=1}^N$$

$$\underline{x}_i \leftarrow T \rightarrow \tilde{x}_i \rightarrow Q \rightarrow \underline{y}_i$$

$$\begin{array}{c} 1 \begin{bmatrix} \underline{x} \end{bmatrix} \rightarrow \begin{bmatrix} \underline{x} \end{bmatrix}^T \rightarrow \begin{bmatrix} \underline{y} \end{bmatrix} \\ 2 \begin{bmatrix} \underline{x} \end{bmatrix} \rightarrow \vdots \rightarrow \begin{bmatrix} \vdots \end{bmatrix} \end{array}$$

$$\begin{array}{c} N \begin{bmatrix} \underline{x} \end{bmatrix} \rightarrow \begin{bmatrix} \underline{x} \end{bmatrix}^T \rightarrow \begin{bmatrix} \underline{y} \end{bmatrix} \\ \underline{x} \quad \underline{y} \\ ? \quad \downarrow \rightarrow W_\theta \rightarrow \hat{x} \end{array}$$

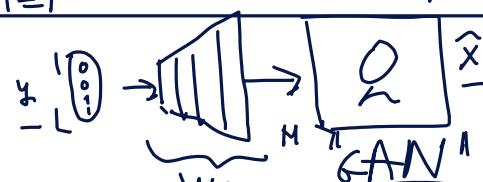
Key-?

$$\triangleright_x \mathcal{L}(x) = 0.$$

$$\tilde{x} = (TT^T)^{-1} T^T \underline{x}$$

$$T^{-1} \rightarrow T^T T^{-1}$$

$$\mathcal{L}(\theta) = \sum_{i=1}^N \| \underline{x}_i - W_\theta(\underline{y}_i) \|_2^2$$



① T not invertable $L \ll MN$.

② $Q(\tilde{x}) \rightarrow \text{loss of inform-}$

→ stoch. (M.A.P.)

$$\hat{\theta} = \underset{\theta}{\operatorname{argmin}} \mathcal{L}(\theta)$$

$$L \sim MN$$

$$\mathcal{L}(x) = \frac{1}{2} \| \tilde{x} - T^{-1}x \|_2^2 + \lambda \mathcal{L}(x)$$

penal

$\mathcal{L}(x)$

$\ell_2: \|x\|_2 \rightarrow \text{ridge}$

$\ell_1: \|x\|_1 \rightarrow \text{lasso}$

$$\triangleright_x \mathcal{L}(x) = 0..$$

$$Q(\tilde{x}) \rightarrow \text{No}$$

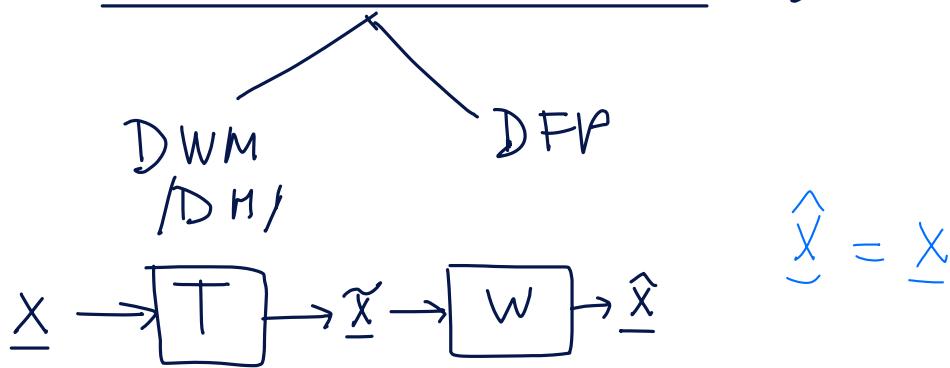
$$\begin{bmatrix} \underline{x} \end{bmatrix} \rightarrow \begin{bmatrix} \underline{x} \end{bmatrix}^T \rightarrow \begin{bmatrix} \underline{y} \end{bmatrix}$$

!

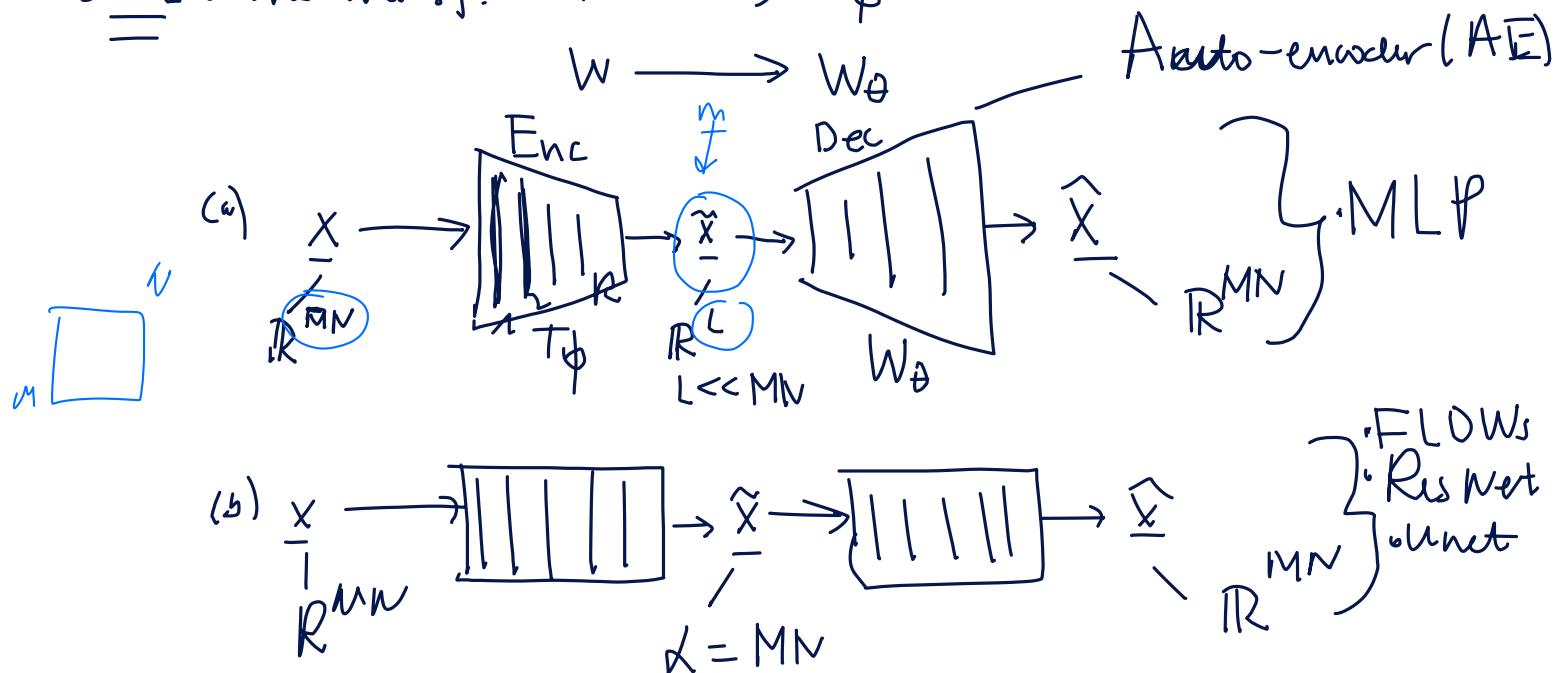
Not feasible.
for the attacker.

Sec A.

T/W based on ML. (Defender)



b) ML: the transf: $T \rightarrow T_\phi$



Ex: Enc:

$$\tilde{X} = T_\phi(X) = G_R(T_1 \dots G_2(T_2 \cdot f_1(\underbrace{T_1 X + b_1}_{\phi}) + b_2) + \dots + b_R)$$

$\phi = \{T_1, T_2, \dots, T_k, b_1, \dots, b_R\}$

Dec:

$$\hat{X} = W_\theta(\tilde{X}) = G_R(W_R - \dots - G_1(W_1 \cdot \tilde{X} + a_1) - \dots - a_R)$$

\triangleright Training

$$\mathcal{L}(\phi, \theta) = \sum_{i=1}^N \| \hat{x}_i - W_\theta T_\phi(x_i) \|_2^2$$

$\hat{x}_i = \sum_{i=1}^N \| x_i - W_\theta T_\phi(x_i) \|_2^2$

$x \sim \hat{x}$

1) $\nabla_{\phi, \theta} \mathcal{L} = 0$

2) (FGD) : $(\hat{\phi}, \hat{\theta}) = (\phi, \theta)^K - \beta \nabla_{\phi, \theta} \mathcal{L}(\phi, \theta)$

Remarks:

① # in $\phi, \theta \rightarrow N \uparrow$

