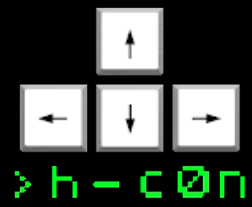
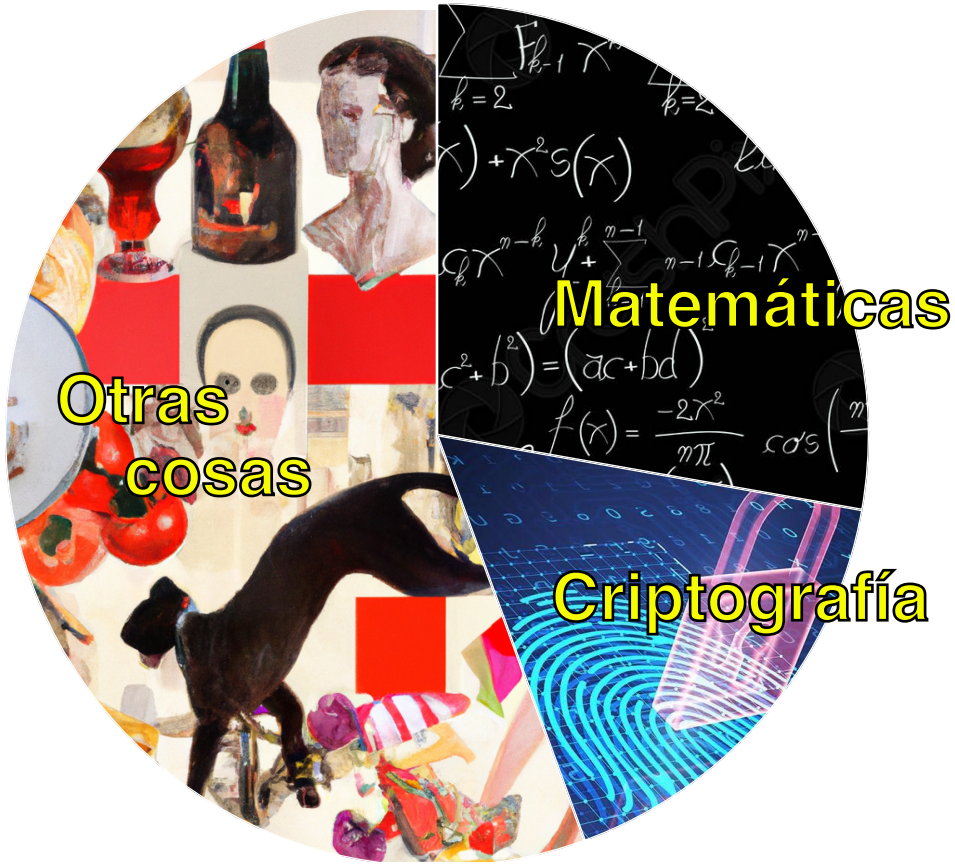
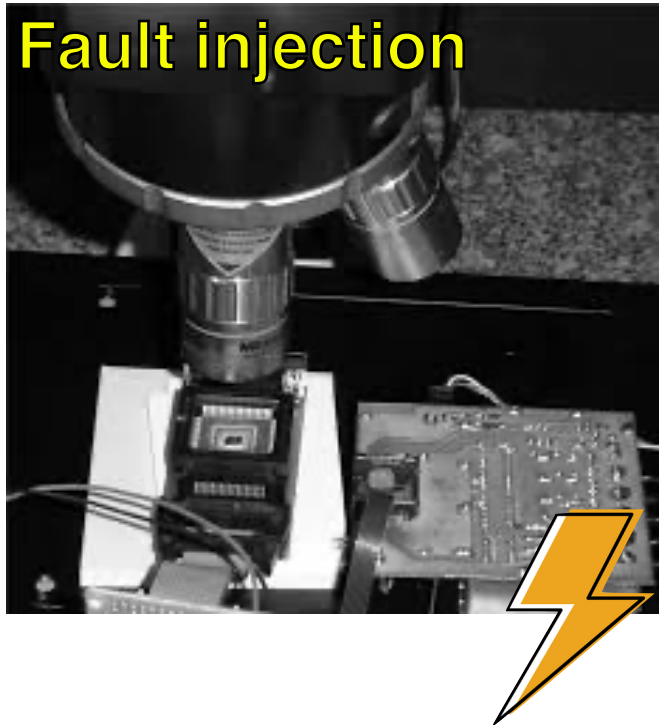


Watermarking sobre imágenes digitales resistente al proceso Print-Scan

Tània Diaz


Otras cosas
Matemáticas
Criptografía


Side-Channel


Fault injection

Esteganografía

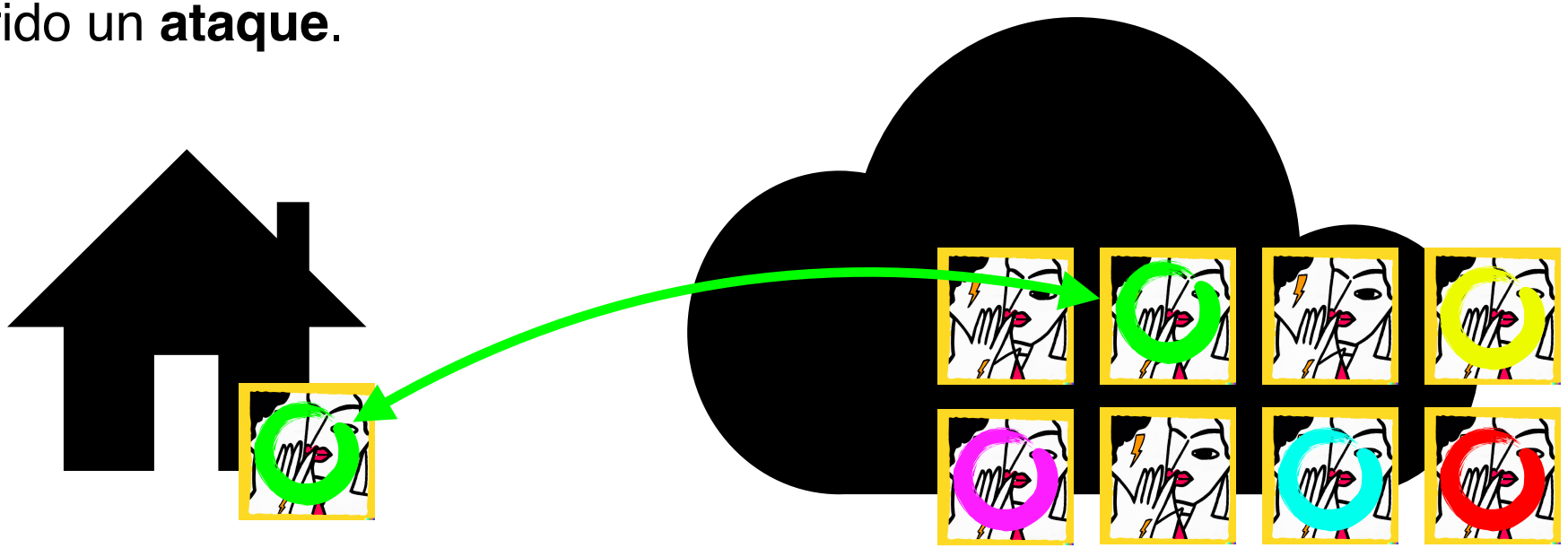
Esteganografía -del griego “*stego*” (esconder o secreto) y “*grapho*” (escribir)- es la ciencia que busca esconder la propia existencia de una comunicación.

Watermarking

Las técnicas de watermarking buscan esconder cierta información dentro de un contenido, asegurando que con la distribución o modificación de ese contenido se puedan atribuir los derechos sobre el producto en concreto a posteriori.

Implementar un algoritmo de incrustación de marcas que permita:

- Incrustar marcas de agua **invisibles** en una imagen digital.
- Detectar si una imagen ha sido marcada con una marca concreta incluso si esta ha sufrido un **ataque**.



Invisible

Consideraremos invisible una marca de agua cuando la diferencia entre a imagen original y la marca de agua sea **imperceptible** a la sensibilidad humana. Usaremos la medida ***PSNR*** para calcular la similitud píxel a píxel.

Ataque

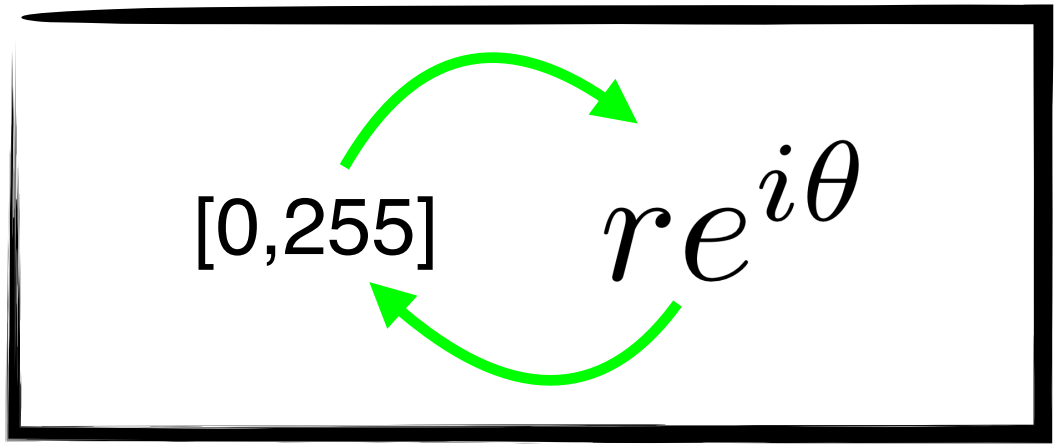
Entenderemos como un ataque a la marca de agua **cualquier deformación** que pueda transformar la imagen, y, por tanto, la marca.

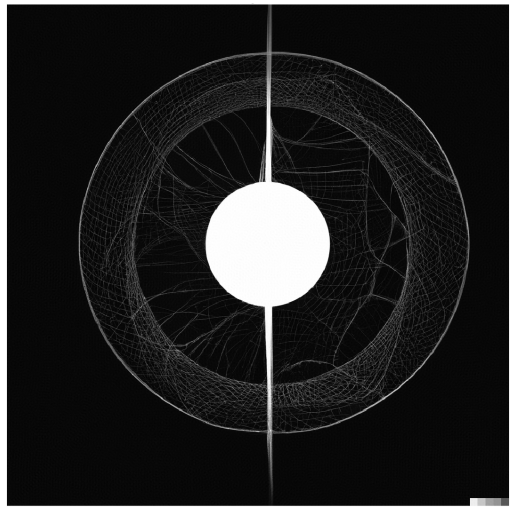
Resistencia

Una marca es resistente a un ataque si después del ataque la **tasa de detección** aparece por encima de un cierto umbral establecido.

Dado $z = (z(0), z(1), ..., z(N-1)) \in \ell^2(\mathbb{Z}_N)$. Para $k = 0, 1, \ldots, N-1$, definimos

$$\hat{z}(k) = \sum_{j=0}^{N-1} z(j) e^{\frac{-2\pi i j k}{N}}$$



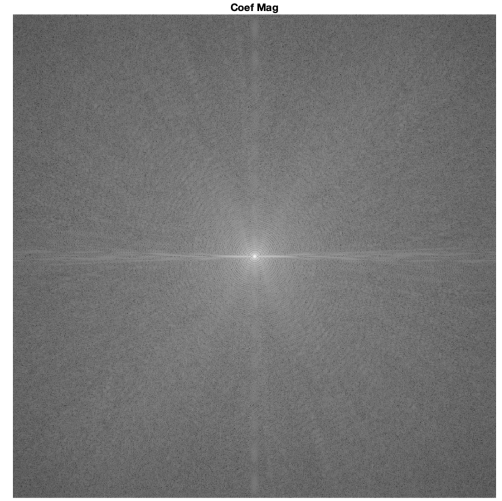


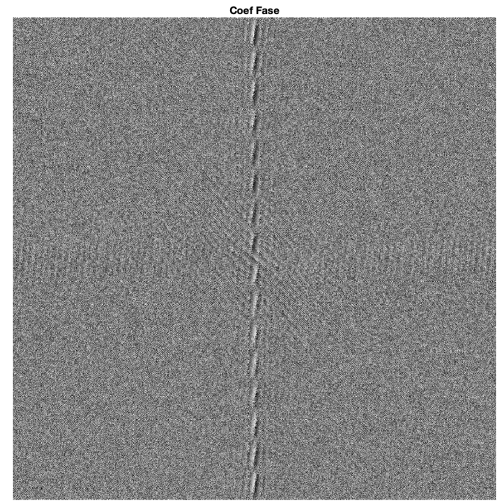
[0,255]

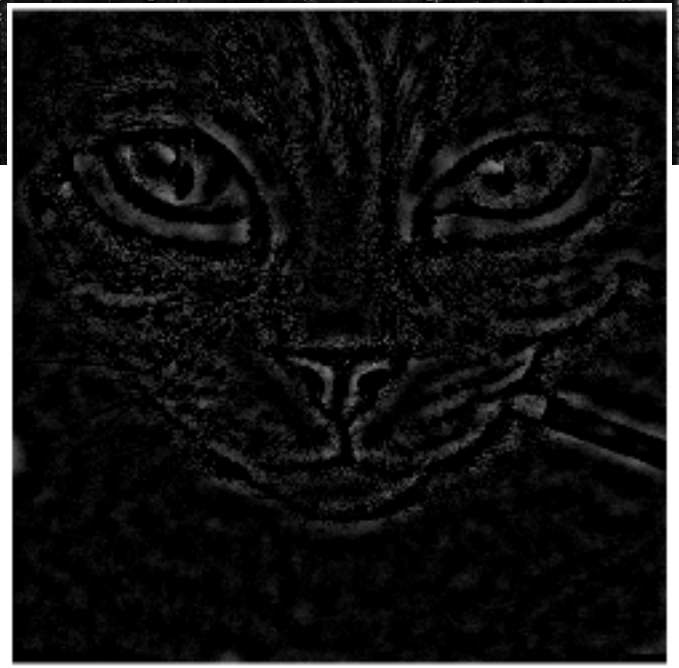
$re^{i\theta}$

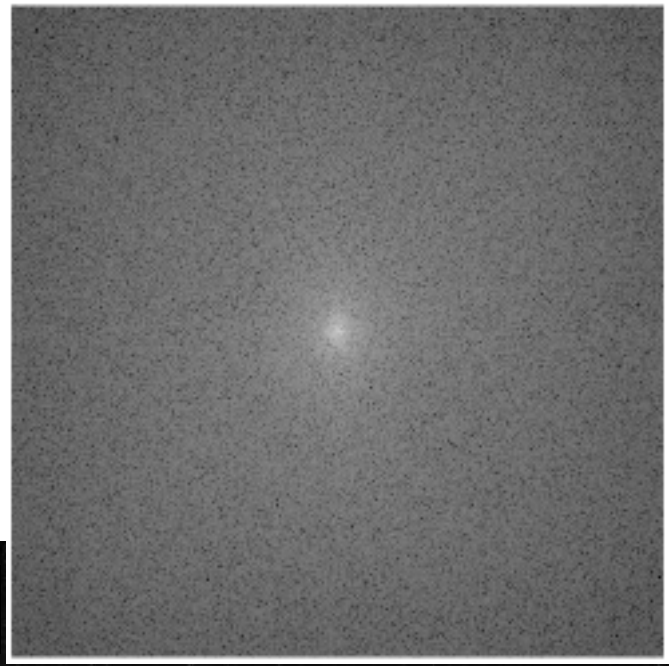
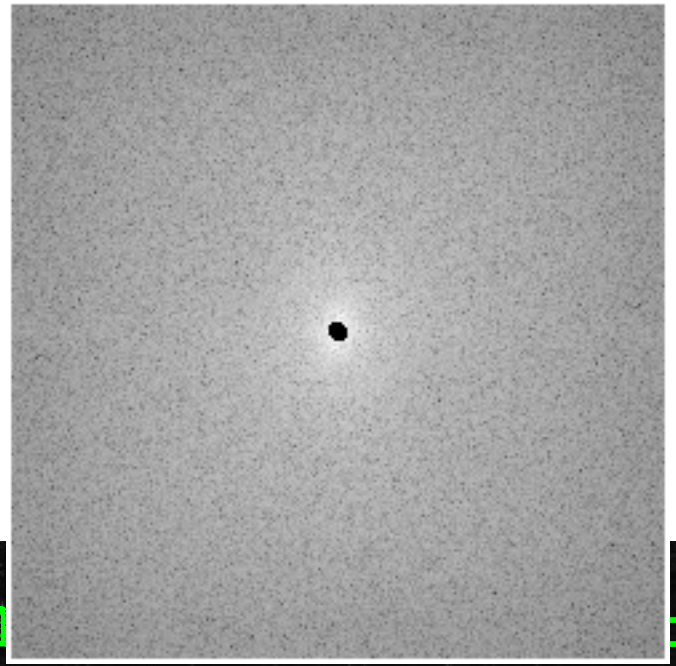
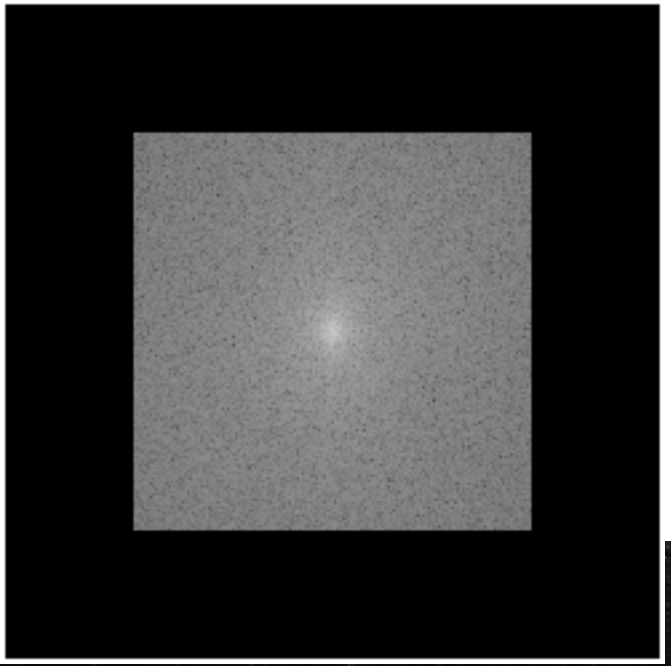
Coeficiente de magnitud

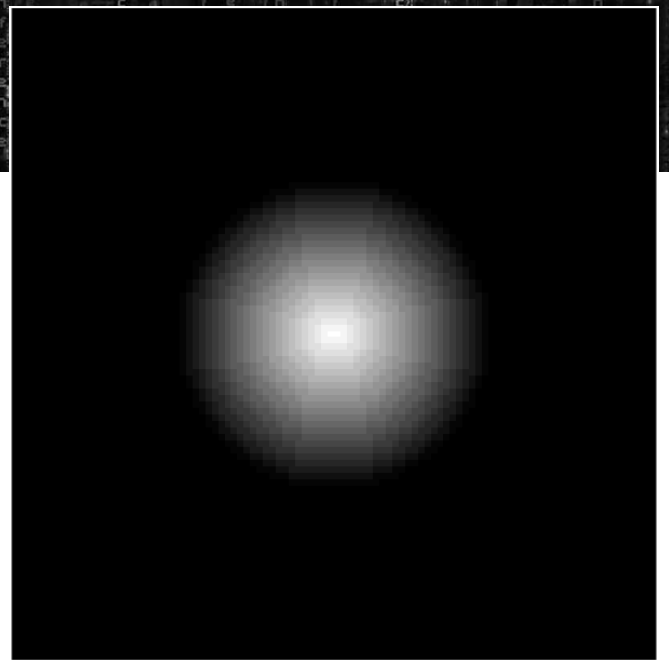
Coeficiente de fase

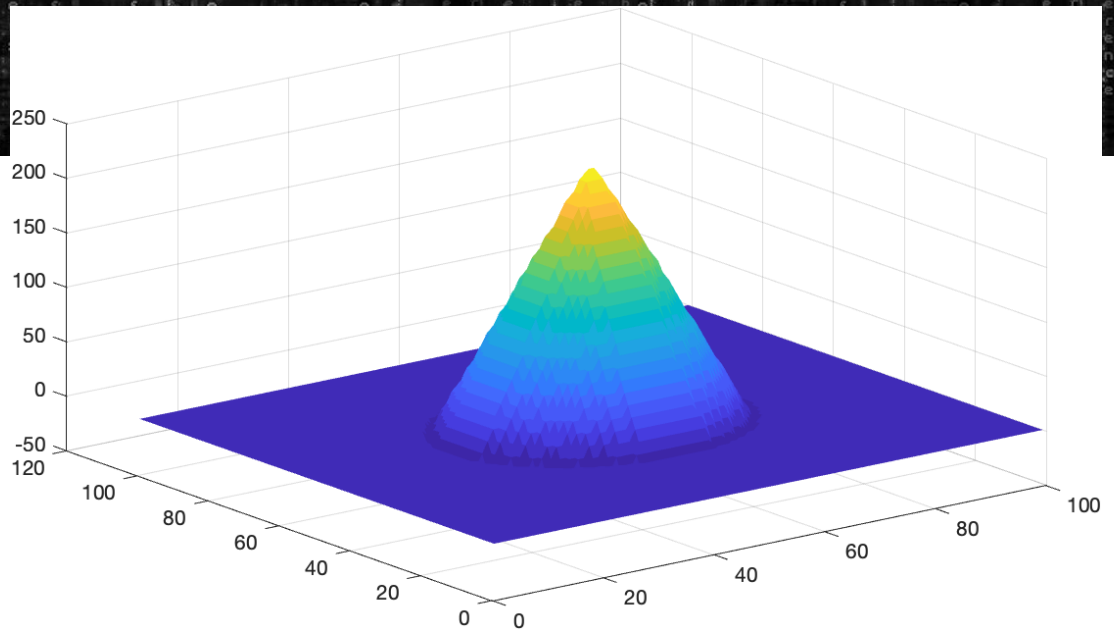


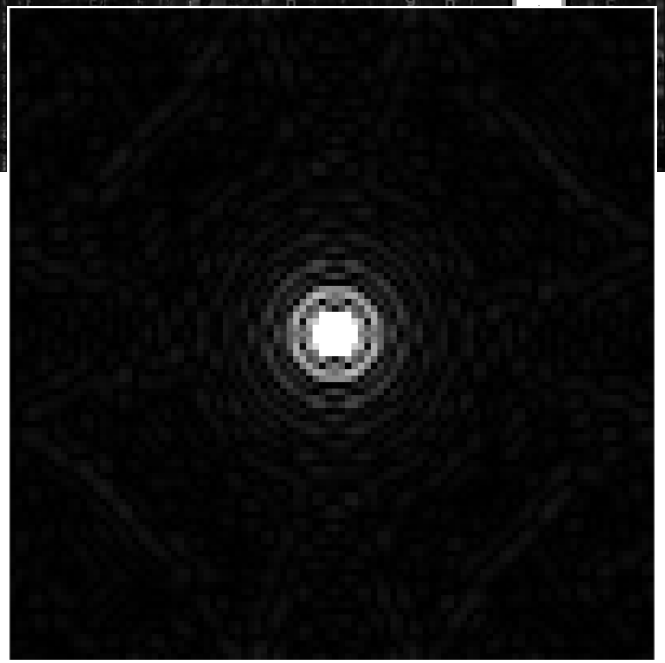


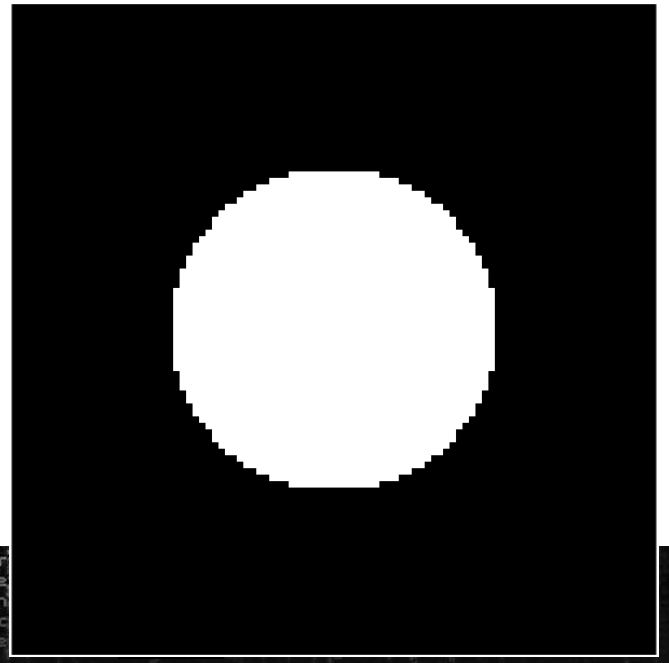



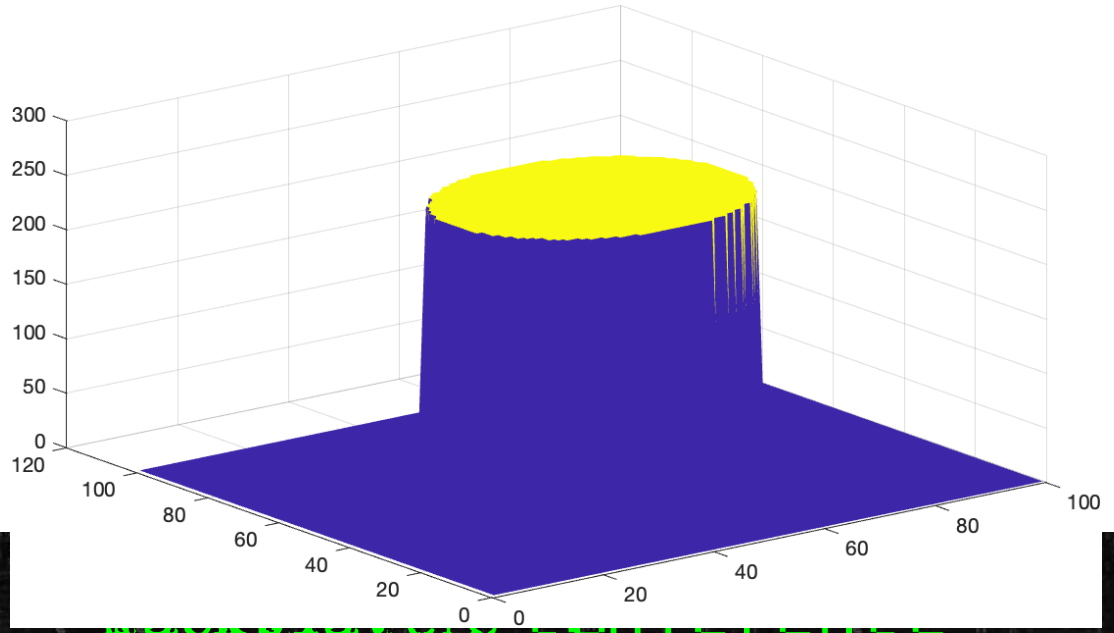




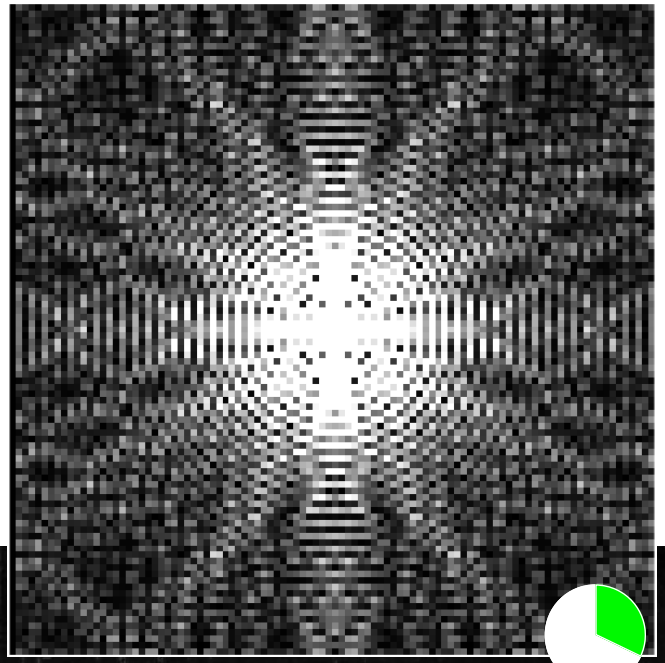












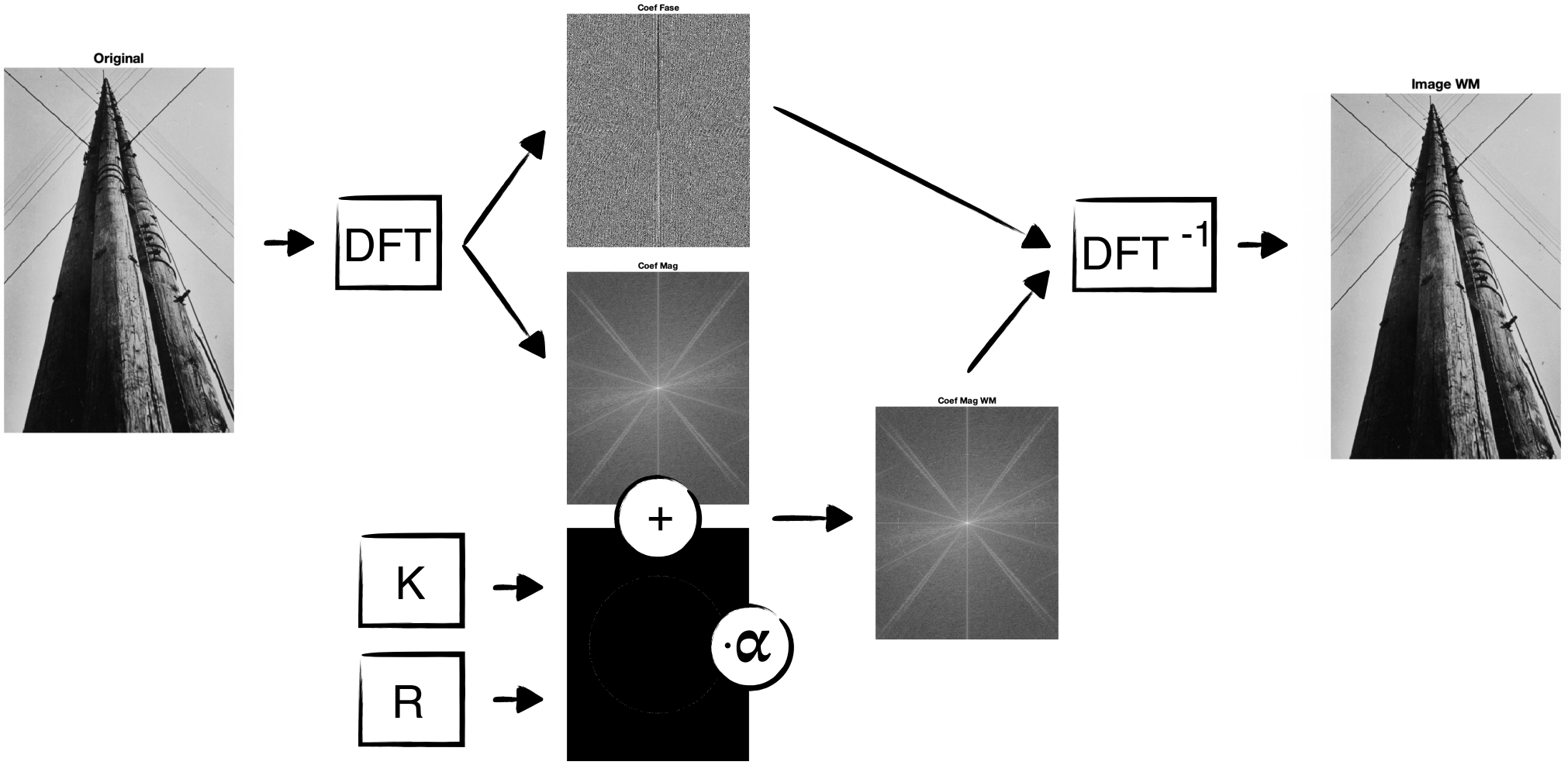
Propiedades de la DFT

DFT → Transformada discreta de Fourier
PS → Print-Scan

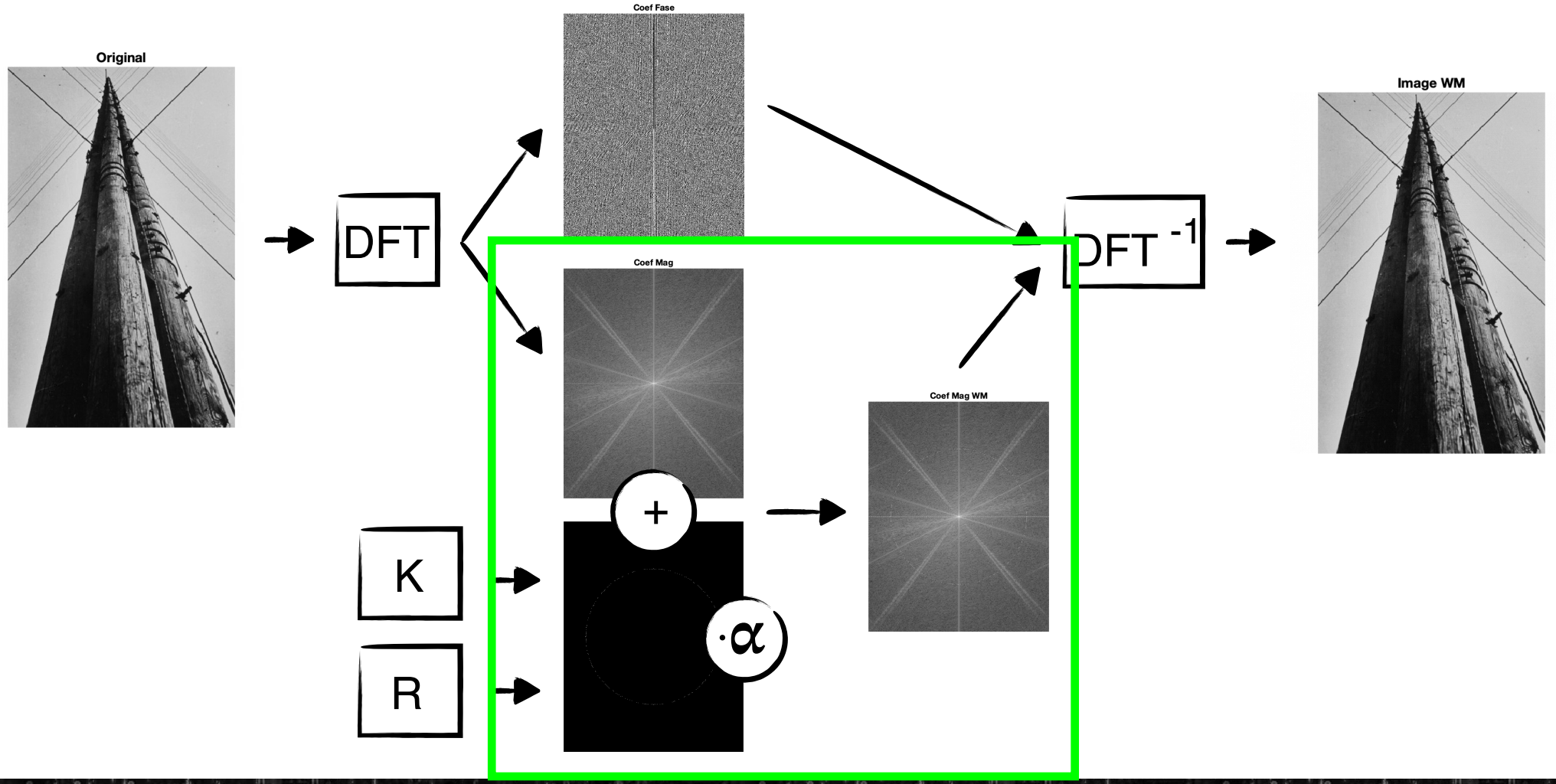
Propiedades durante el proceso PS

- Los coeficientes de baja y mediana frecuencia se conservan mejor.
- Aumentar ligeramente la magnitud de los coeficientes de baja frecuencia no es significativamente perceptible.
- La mayoria de relaciones entre los coeficientes de la DFT se conservan.

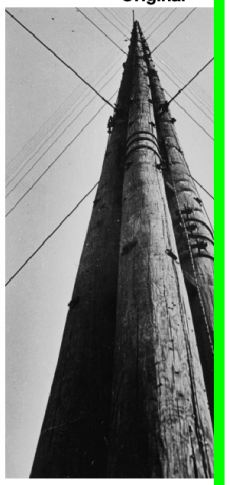
Algoritmo de incrustación



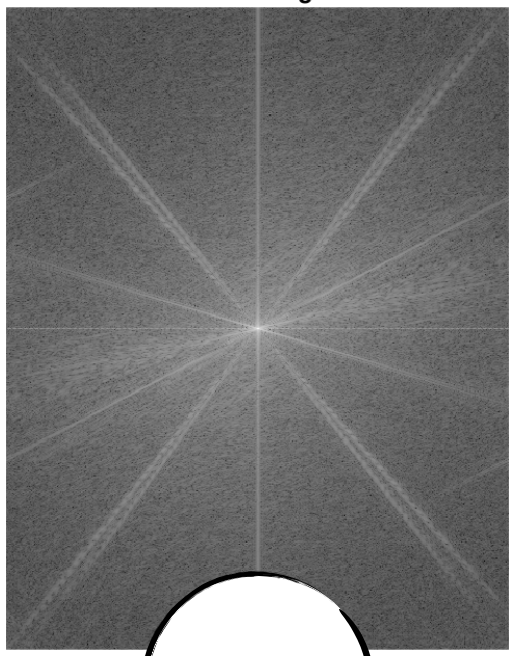
Algoritmo de incrustación



Original



Coef Mag



+

K

R

·α

Coef Mag WM

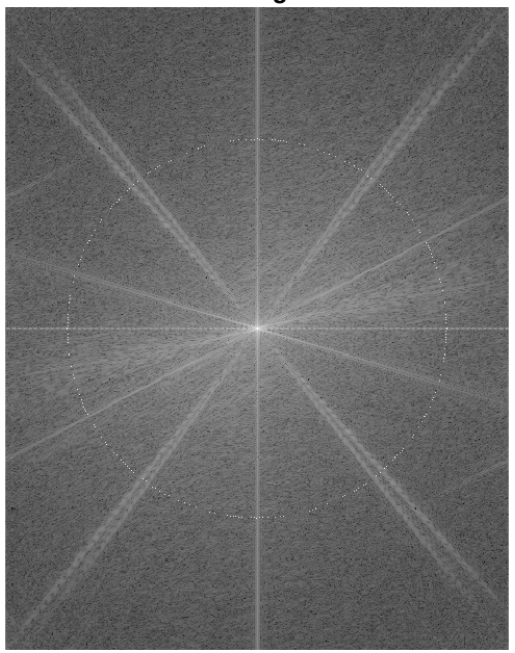


Image WM

Vector binario de dimensión l o secreto

Matriz coeficientes de magnitud de la imagen

$$W_{xy} = k_j \cdot \left(\frac{1}{9} \sum_{s=-1}^{1} \sum_{t=-1}^{1} M_{x+s,y+t} \right)$$

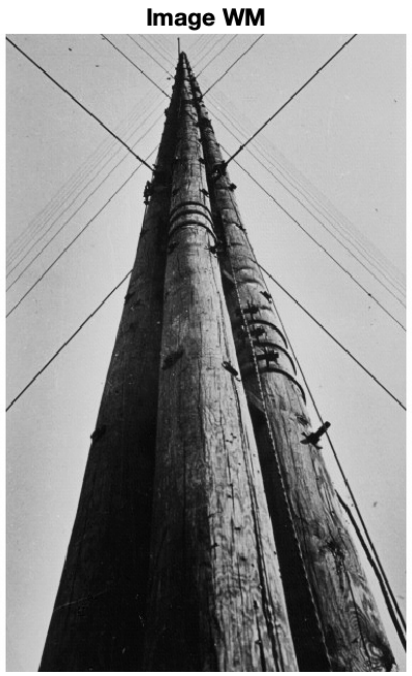
Matriz marca de agua

$$x = \left(\frac{m}{2} + 1\right) + \lceil r \cdot \cos\left(\frac{j \cdot \pi}{l}\right) \rceil$$

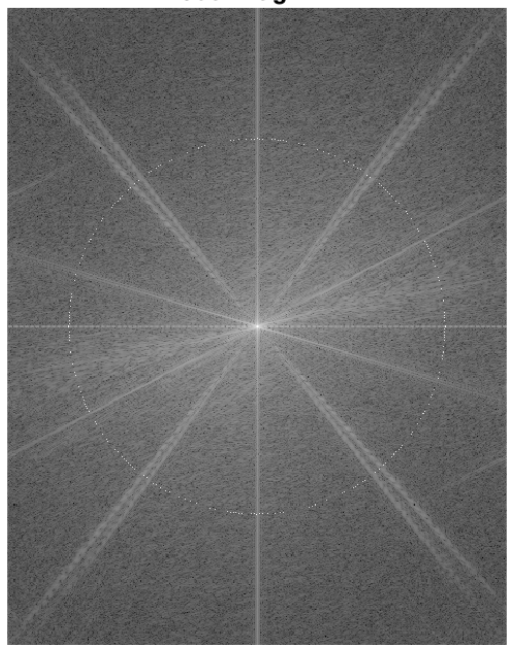
Función parte entera

$$y = \left(\frac{n}{2} + 1\right) + \lceil r \cdot \sin\left(\frac{j \cdot \pi}{l}\right) \rceil$$

Radio de implementación



DFT



Extracción de vectores

K

Covarianza cruzada

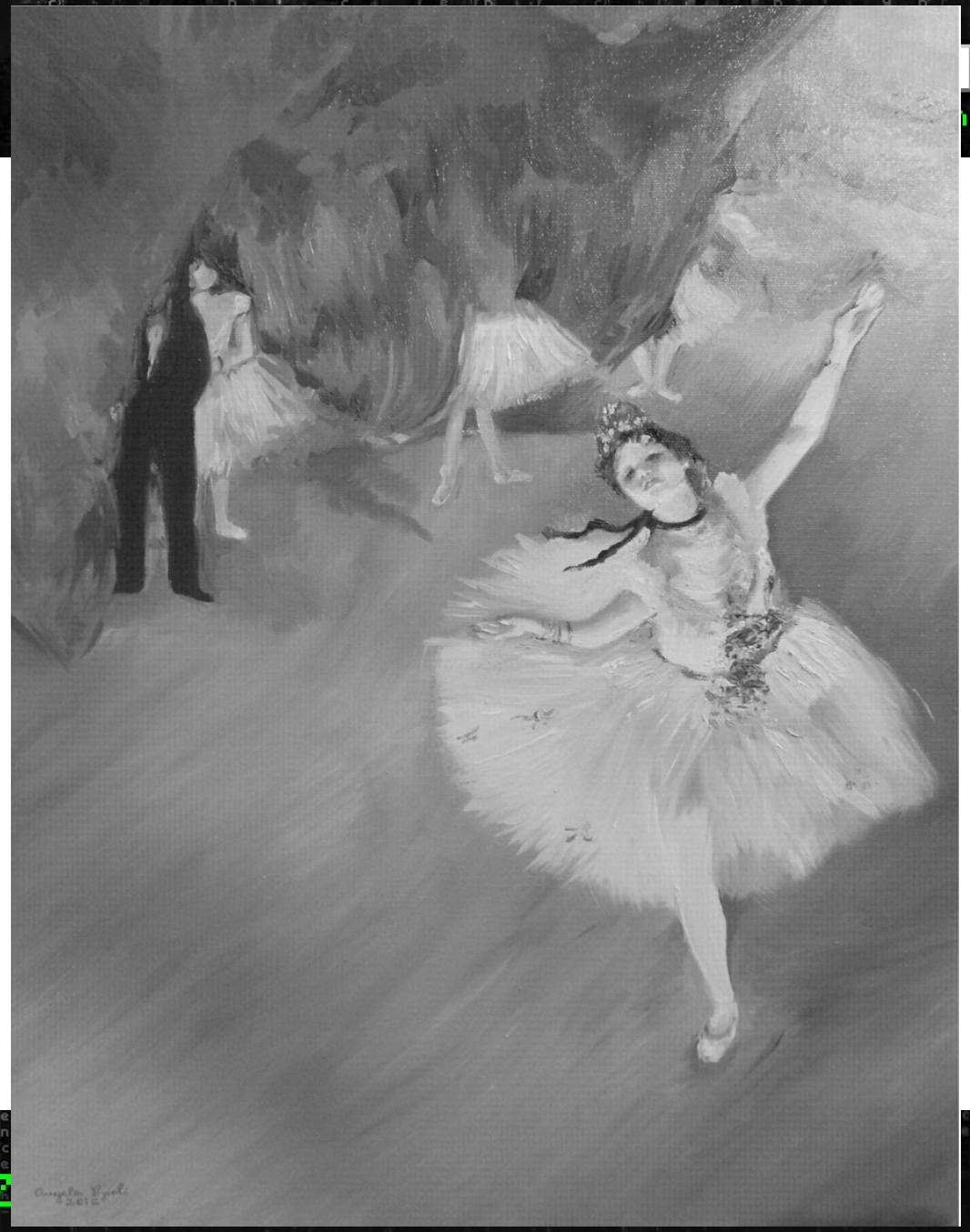
> t

+

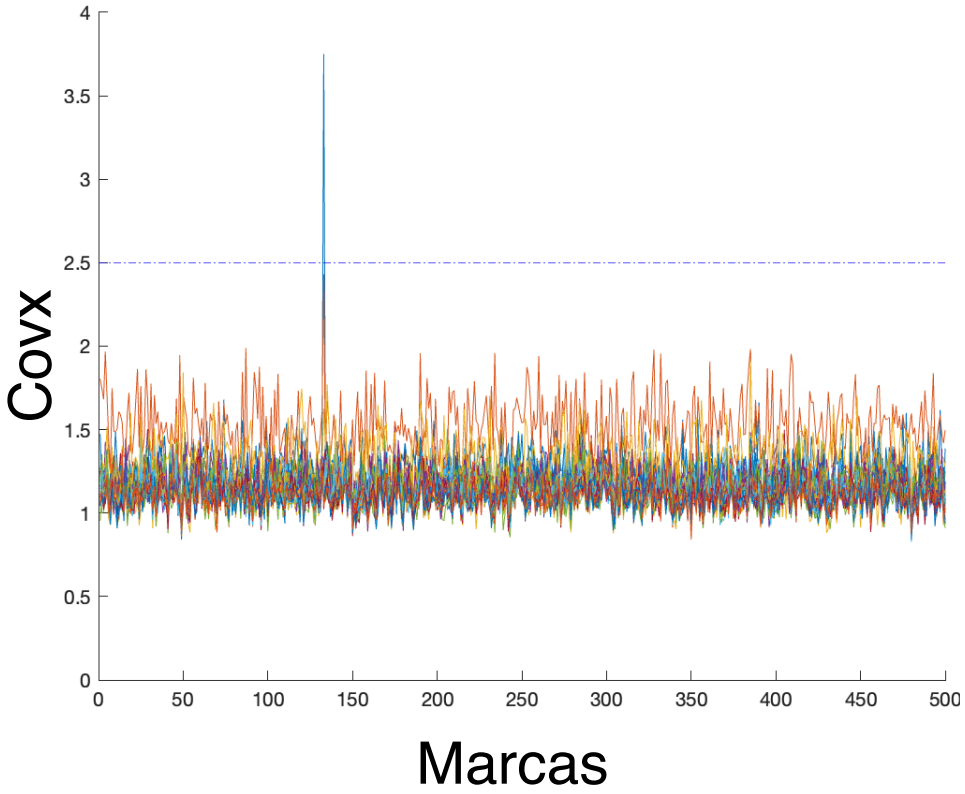
-

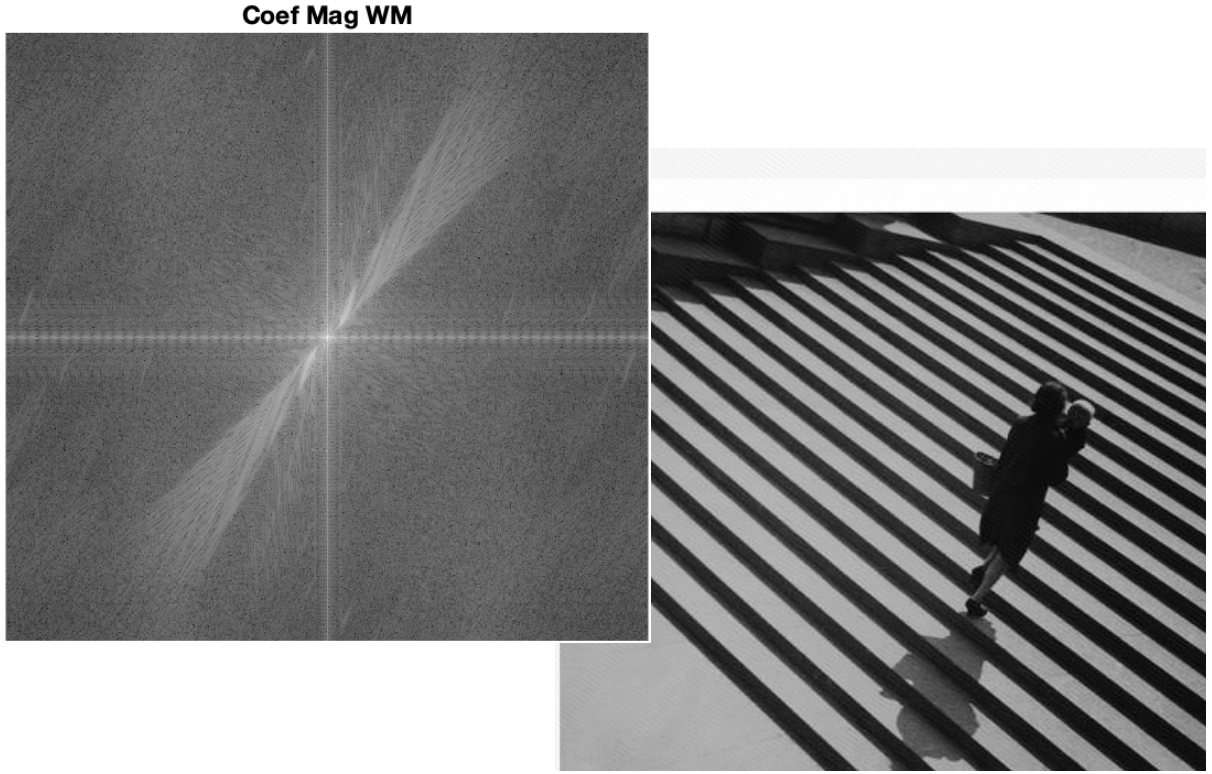
H-CON HACKPLAYERS CONFERENCE FIVE

resultados



1,0,1,0,0,0,0,1,0,1,1,1,0,1,1,0,0,1,0,0,1,1,0,1,0,0,0,1,0,1,0,0,0,1,1,0,1,1,0,1,1,0,0,1,0,1,0,1,1,1,1,1,1,1,1,0,1,0,0,1,0,0,0,0,0,1,0,0,0,1,0,0,0,1,1,0,1,0,1,1,0,0,0,0,0,1,0,1,1,1,1,1,1,1,0,0,1,1,0,0,0,1,1,1
,0,1,1,1,0,1,1,0,1,0,1,0,1,0,0,1,1,0,0,0,1,1,1,1,0,0,1,0,0,1,1,0,1,0,0,1,0,1,0,0,1,1,0,0,1,0,0,1,1,1,0,1,1,1,0,0,0,1,1,0,1,0,0,1,0,1,0,1,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,1,1,1,0,0,1,1,0,0,0,1,0,0





$\alpha = 5$

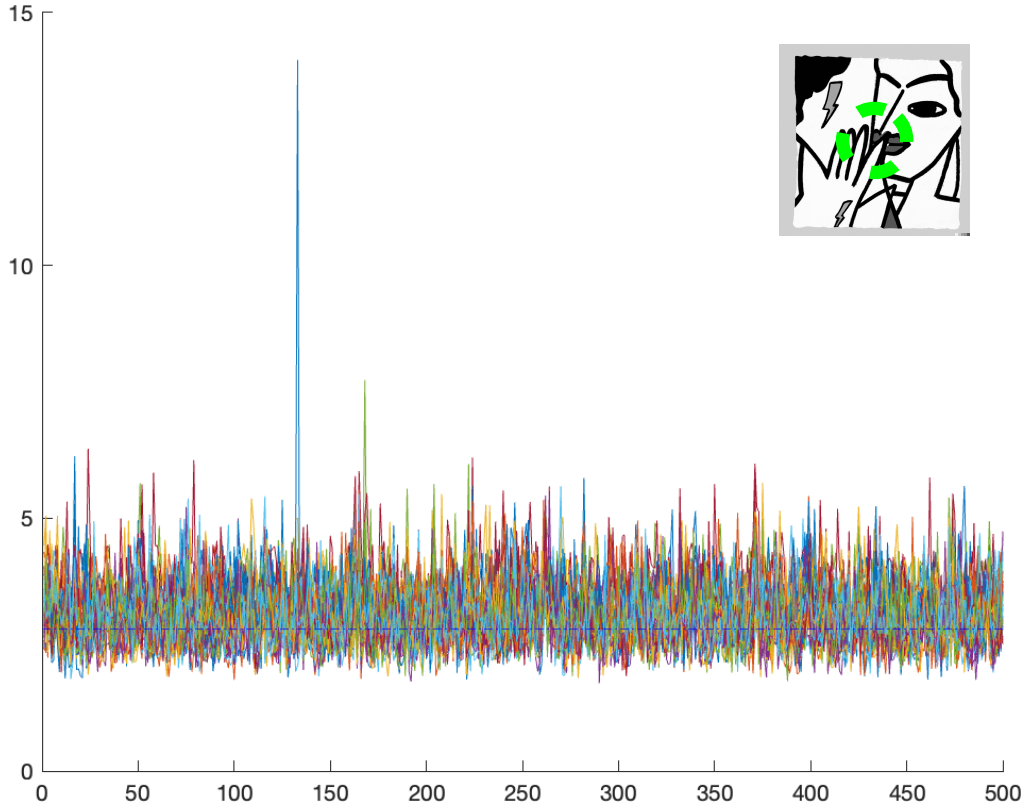
R = 5

$\alpha = 5$

R = 175

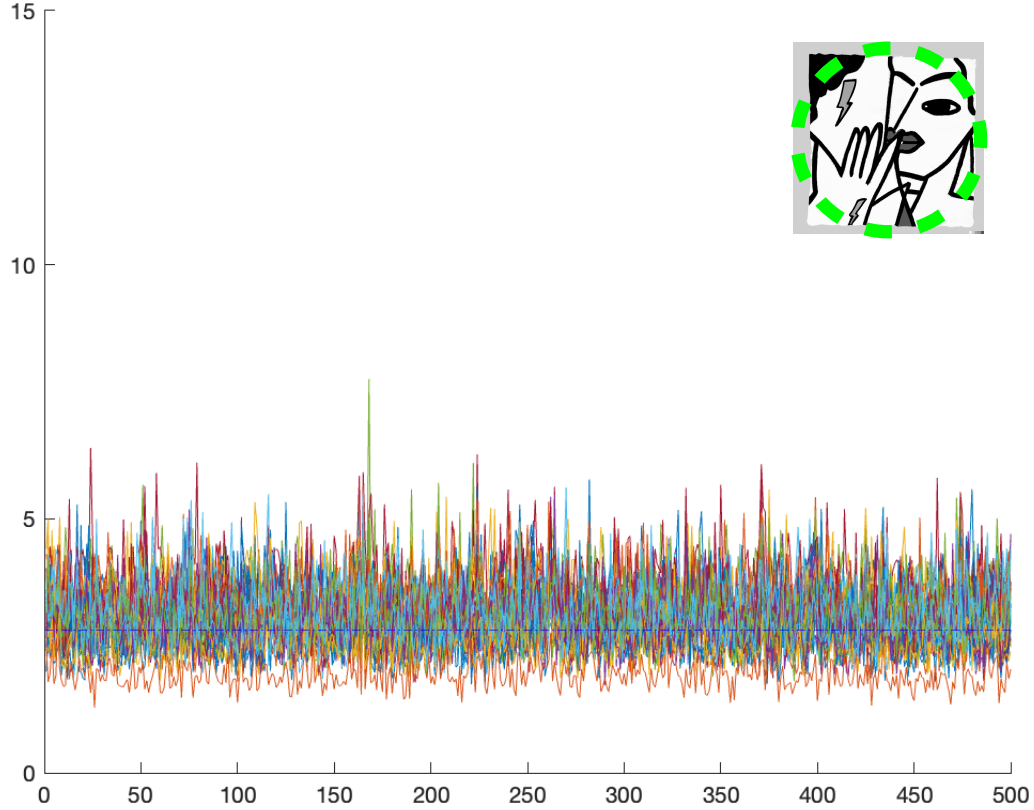
$\alpha = 5$

R = 500



$\alpha = 5$

R = 175



$\alpha = 5$

R = 500

$\alpha = 1$

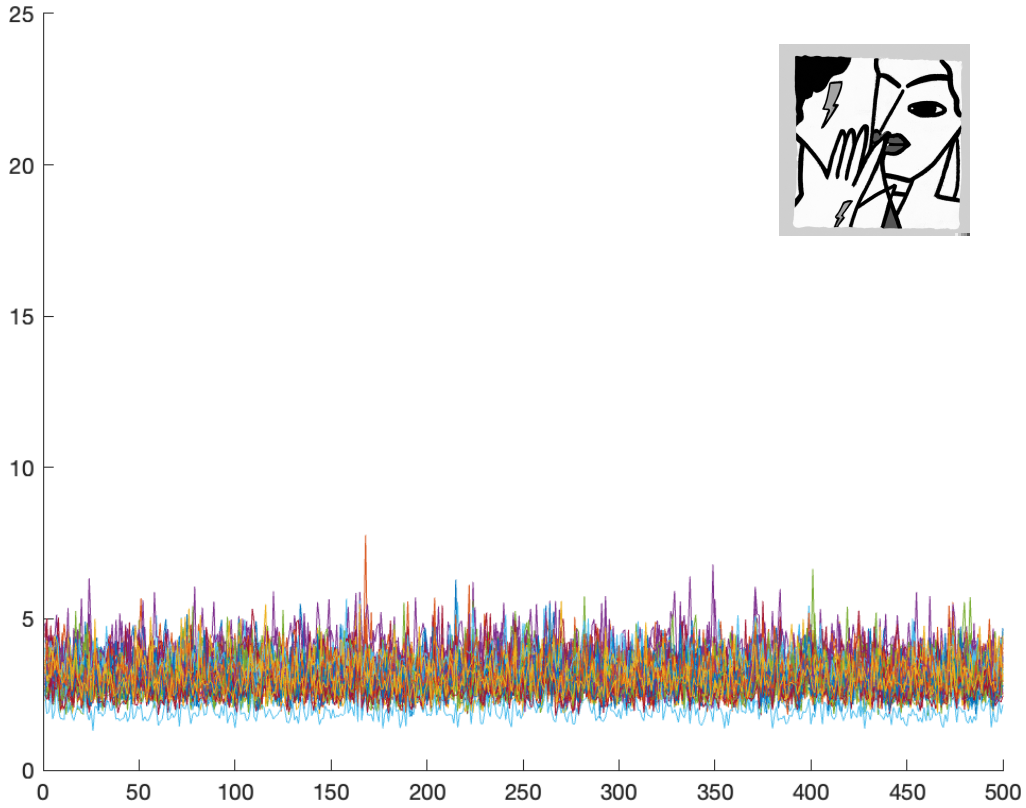
R = 175

$\alpha = 10$

R = 175

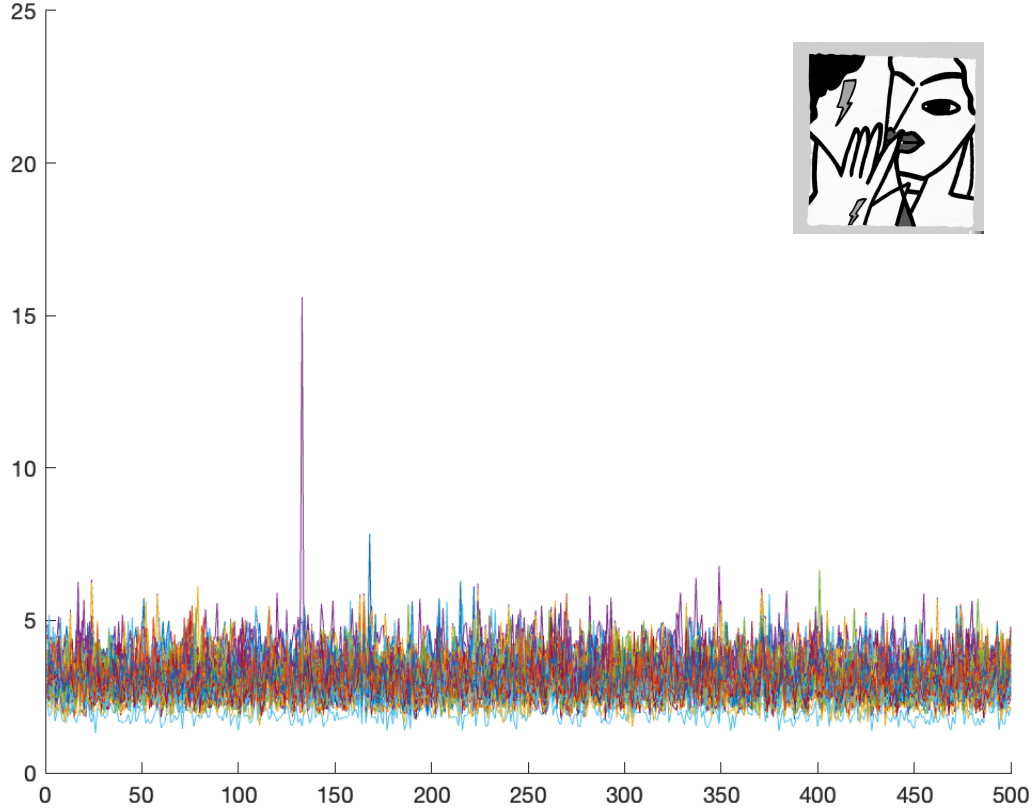
$\alpha = 500$

R = 175



$\alpha = 1$

R = 175



$\alpha = 10$

R = 175

Imagen original

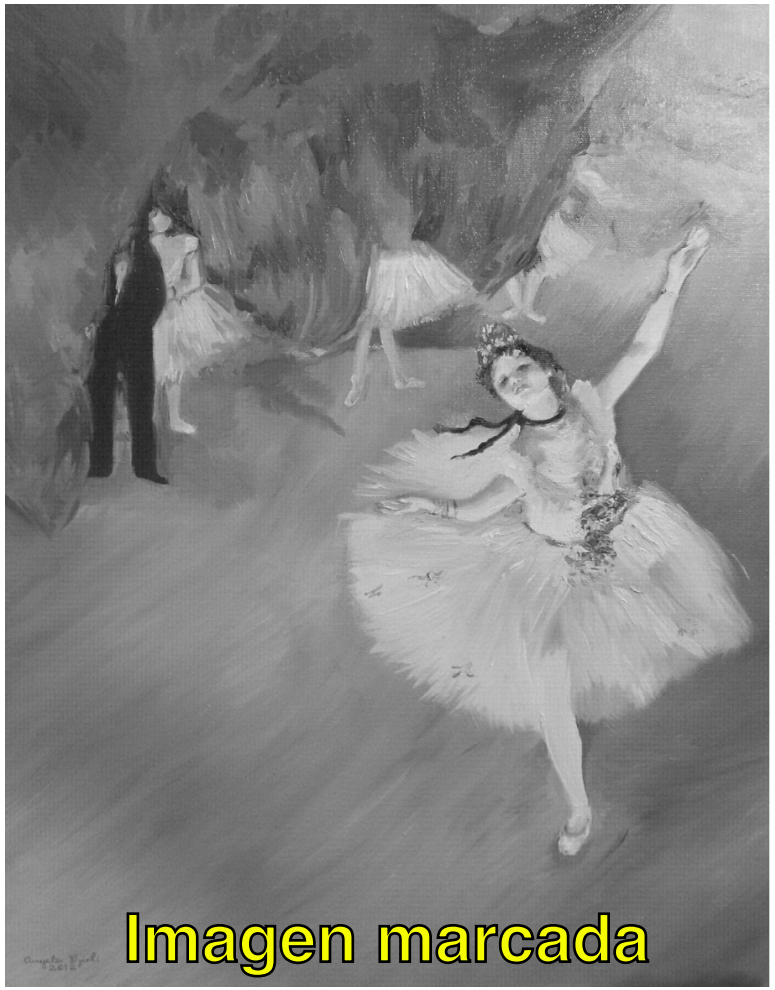


Imagen marcada

Imagen marcada PS

Digital

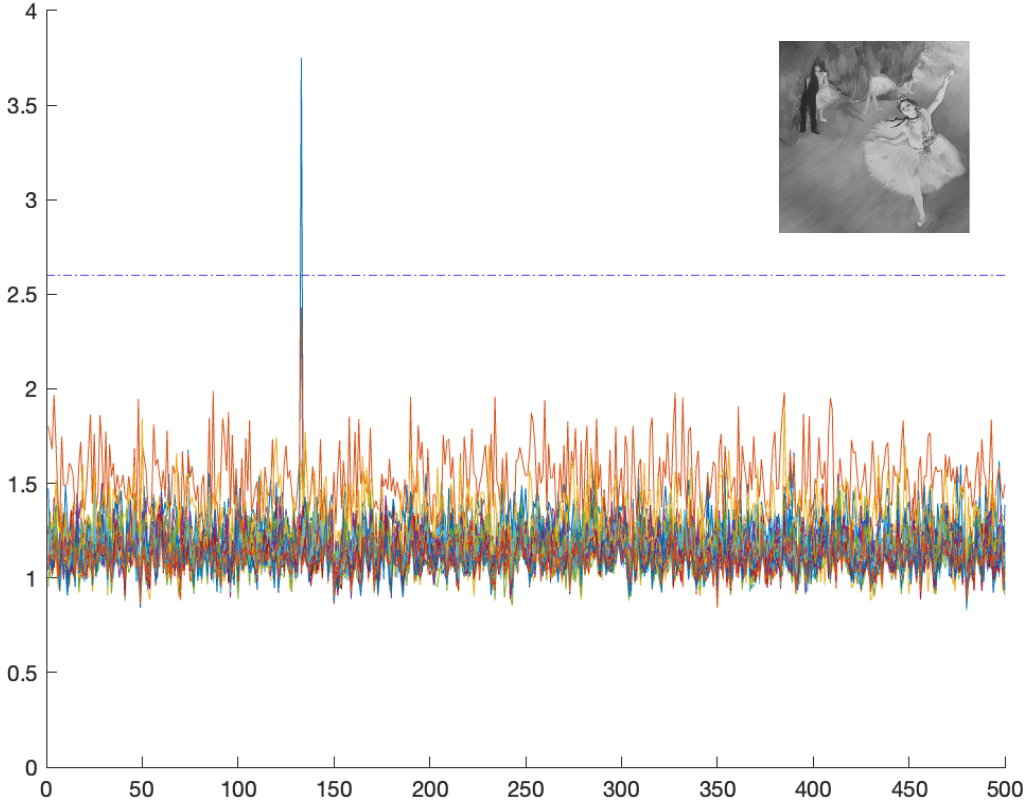


Imagen marcada

Papel satinado 100g (folio)

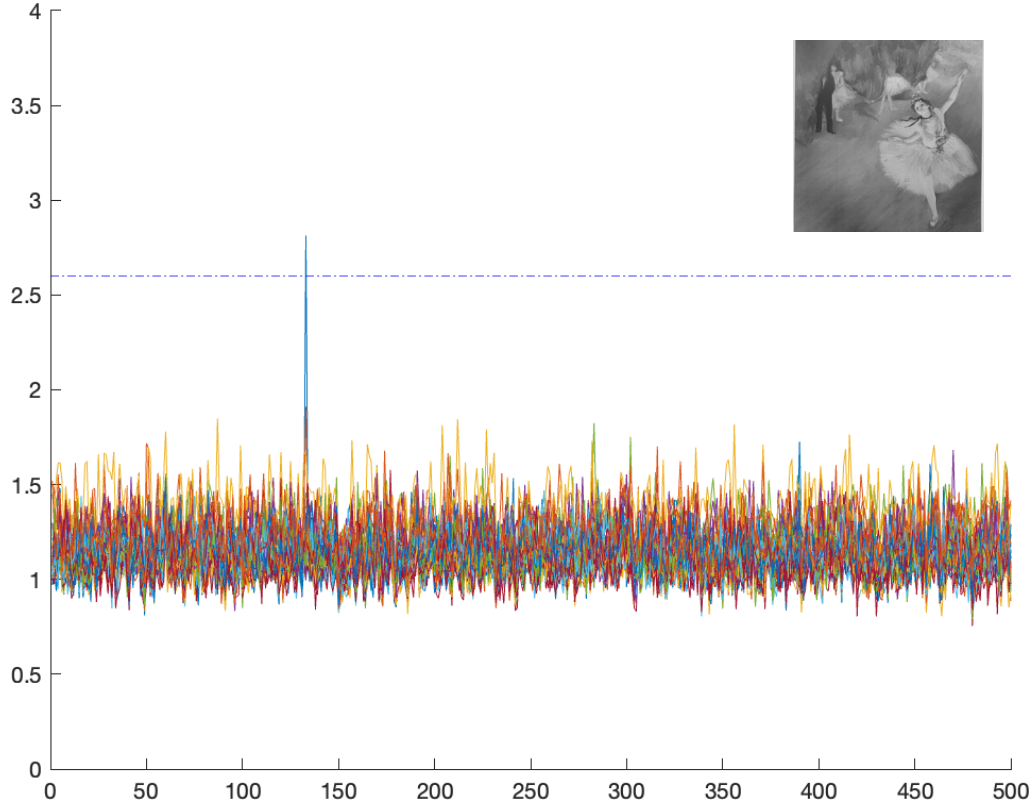


Imagen marcada PS

Digital

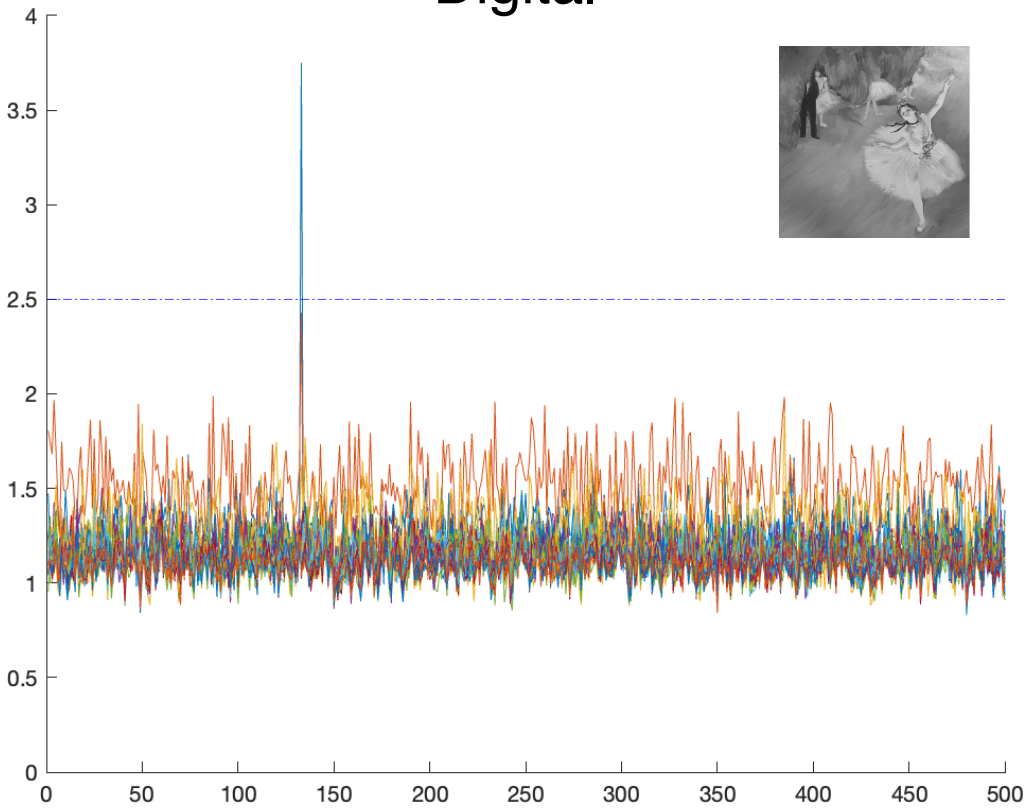


Imagen marcada

Papel estucado mate (cartulina)

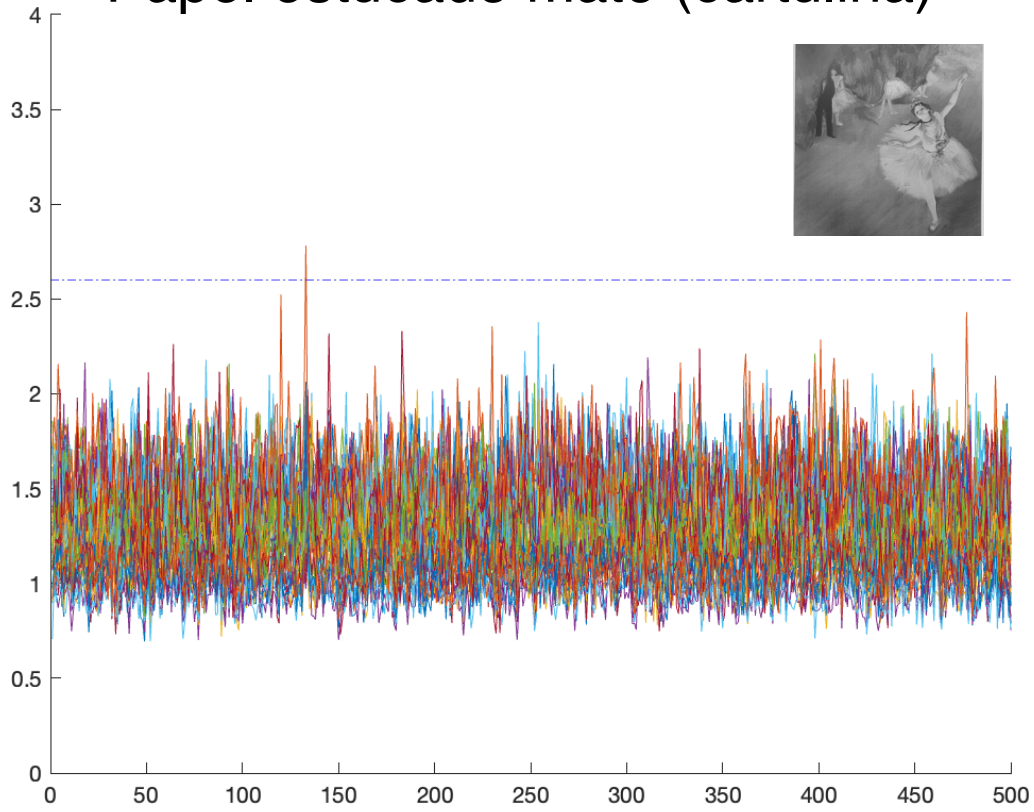


Imagen marcada PS

CONCLUSIONES

Thnks <3

in taniadiazcancer

Hackplayers c0nference

```
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
[64857.521348] sd 0:0:0:0: [sda] Synchronizing SCSI cache
[64857.522838] Restarting system.
_
```

www.h-c0n.com