

Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

- watermark inserat în datele gazdă prin cuantizarea acestora
- în domeniul spațial sau orice domeniu transformat
- fie watermark-ul $w \in \{w_1, w_2, \dots, w_n\}$
- fie X un eșantion al datelor gazdă:
 - luminanța, crominanța unui pixel (domeniul spațial)
 - coeficientul unei transformate a imaginii (domeniul transformat)

Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

- se alege un set de n cuantizori $Q_i, i = 1, 2, \dots, n$
- n = numărul de valori posibile ale watermark-ului

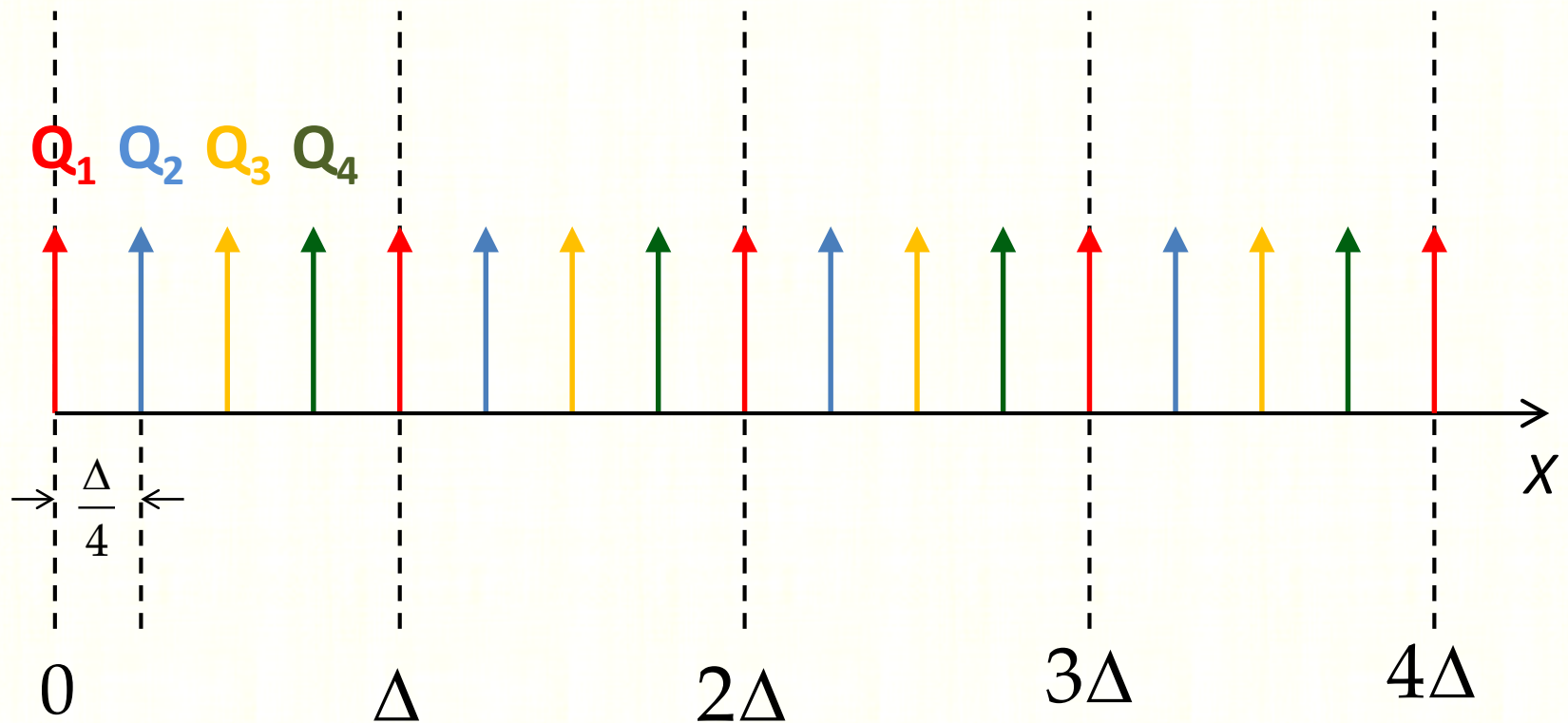
Inserare watermark

- pentru a insera watermark-ul w_i în eșantionul X
- X se cuantizează utilizând cuantizorul Q_i

Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

- Exemplu pentru $n=4$:



Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

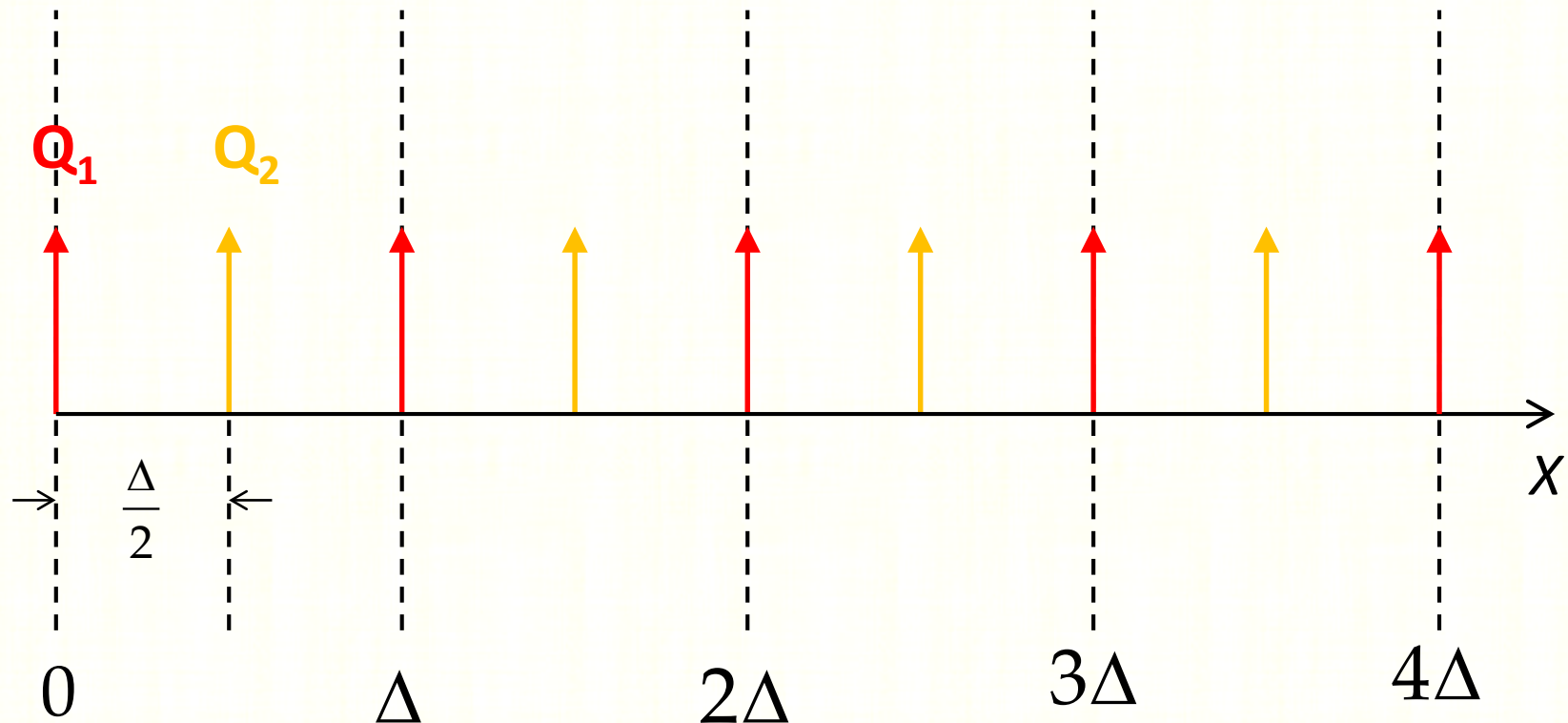
Extragere watermark

- pentru a extrage watermark-ul w' din eșantionul X_w
- se verifică față de ce cuantizor Q_i valoarea X_w se află cel mai aproape
- rezultă că $w' = w_i$
- indicele watermark-ului = indicele cuantizorului

Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

- de regulă $w \in \{0,1\}$ sau $w \in \{-1,1\}$ deci $n=2$
- 2 cuantizori $Q_1, Q_2 \rightarrow$ cuant. la un nr. par sau impar de $\frac{\Delta}{2}$



Tehnici de watermarking bazate pe cuantizare

Modulația indicelui de cuantizare (QIM)

Realizare practică pentru $n=2$

- Inserare:

$$X_w = \left\lfloor \frac{X}{\Delta} \right\rfloor \cdot \Delta + \frac{\Delta}{2} \cdot w \cdot \text{semin}(X - \left\lfloor \frac{X}{\Delta} \right\rfloor \cdot \Delta)$$

$$\text{semin}(x) = \begin{cases} -1, & \text{daca } x \leq 0 \\ 1, & \text{daca } x > 0 \end{cases}$$

- Extragere:

$$w' = \text{mod } 2 \left(\text{round} \left(\frac{X_w}{\frac{\Delta}{2}} \right) \right)$$

Îmbunătățirea calității imaginilor cu watermark

- exploatarea efectelor de mascare ale sistemului vizual uman (SVU)
 - mascare de contrast
 - sensibilitate spațială
 - mascare de luminanță
 - mascare temporală
 - fenomene de focalizare a ochiului uman
- analiză prin teste perceptuale
- toate acestea cresc complexitatea algoritmului

Îmbunătățirea calității imaginilor cu watermark

Exemplu

- ochiul uman mai puțin sensibil la zgomot în zone cu textură decât în zone uniforme ale unei imagini
- compresia păstrează intacte zonele cu textură și marginile
 - watermark-ul ar trebui inserat în zone perceptual importante ale imaginii
 - un atacator nu poate îndepărta ușor watermark-ul fără a cauza o distorsiune importantă

Îmbunătățirea calității imaginilor cu watermark

- principiul de **mascare de contrast** al SVU
 - scăderea vizibilității unui semnal în prezența altui semnal mai puternic
 - efect mai puternic dacă ambele componente sunt de aceeași fr.
 - **Ex:** ponderarea energiei watermark-ului în funcție de valoarea coeficientului din domeniul frecvență

Îmbunătățirea calității imaginilor cu watermark

- sensibilitatea spațială a SVU
 - fenomenul de diferențiere mai ușoară a modificărilor din regiuni de **contrast scăzut**, în comparație cu schimbările din regiunile de **contrast mare**
 - **Ex:** determinarea puterii și regiunii de inserare a watermark-ului în funcție de energia totală a coeficienților AC din acel bloc

Îmbunătățirea calității imaginilor cu watermark

- principiul de mascare de luminanță al SVU
 - ochiul uman este mai puțin sensibil la contrast în **zone luminoase**, în comparație cu zonele de luminanță mică
 - watermark-ul este ponderat cu o mască vizuală, având la bază acest lucru
 - **Ex:** putere mai mare a watermark-ului în zone de intensitate mare

Îmbunătățirea calității imaginilor cu watermark

- praguri de contrast, pentru determinarea locației și puterii watermark-ului
- pragul de contrast = nivelul minim de contrast pentru ca o grilă sinusoidală să fie vizibilă
- creșterea pragurilor de contrast pentru caracteristicile de mascare ale SVU

Exemplu de prag de contrast:

- Diferență Abia Perceptibilă (JND - *Just Noticeable Difference*)
 - valoarea maximă cu care poate fi schimbat un anumit pixel (sau coeficient în frecvență) pentru ca această schimbare să nu fie vizibilă

Îmbunătățirea calității imaginilor cu watermark

Exemplu: Modelul JND al lui Watson

- se aplică asupra coeficienților DCT
- înglobează mascarea de contrast și mascarea de luminanță
- utilizează o JND originală t_{ij} , numită mască, presupusă identică pentru fiecare bloc

1.40	1.01	1.16	1.66	2.40	3.43	4.79	6.56
1.01	1.45	1.32	1.52	2.00	2.71	3.67	4.93
1.16	1.32	2.24	2.59	2.98	3.64	4.60	5.88
1.66	1.52	2.59	3.77	4.55	5.30	6.28	7.60
2.40	2.00	2.98	4.55	6.15	7.46	8.71	10.17
3.43	2.71	3.64	5.30	7.46	9.62	11.58	13.51
4.79	3.67	4.60	6.28	8.71	11.58	14.50	17.29
6.56	4.93	5.88	7.60	10.17	13.51	17.29	21.15

Îmbunătățirea calității imaginilor cu watermark

Exemplu: Modelul JND al lui Watson

- mascarea de luminanță:

$$t_{ij,k} = t_{ij} \left(\frac{c_{00,k}}{\bar{c}_{00}} \right)^{a_T}$$

- $t_{ij,k}$ masca nouă pentru blocul k
- $c_{00,k}$ coeficientul DC al blocului k
- $\bar{c}_{00}$ luminanța medie a imaginii
- $a_T = 0.648$

Îmbunătățirea calității imaginilor cu watermark

Exemplu: Modelul JND al lui Watson

- mascarea de contrast:

$$m_{ij,k} = \max\left(t_{ij,k}, |c_{ij,k}|^{w_{ij}} t_{ij,k}^{1-w_{ij}}\right)$$

- $m_{ij,k}$ masca nouă pentru blocul k
- $c_{ij,k}$ coeficientul AC de la poziția (i,j) al blocului k
- o valoare empirică pentru w_{ij} este de regulă $w_{ij} = 0,7$

Tehnici de watermarking pentru video

Clasificare	Avantaje	Dezavantaje
Adaptare imagine - video	Beneficiază de toate rezultatele pentru imagini	Pot necesita un efort mare de calcul
Integrarea dimensiunii temporale	Algoritmi video care de obicei permit o mai mare robustețe	Pot necesita un efort mare de calcul
Exploatarea standardului de compresie	Algoritmi simplii, ce permit procesarea în timp real	Watermark-ul este legat doar de respectivul standard de compresie

Atacuri asupra sistemelor de watermarking

- robustețea watermark-ului digital evaluată prin integritatea watermark-ului după distorsiuni/atacuri
- acestea pot altera fără voie sau voit watermark-ul inserat
- BER (Bit Error Rate)

$$BER = \frac{\sum_{j=1}^P |w_{out}(j) - w_{in}(j)|}{P}$$

Distorsiuni și atacuri specifice imaginilor

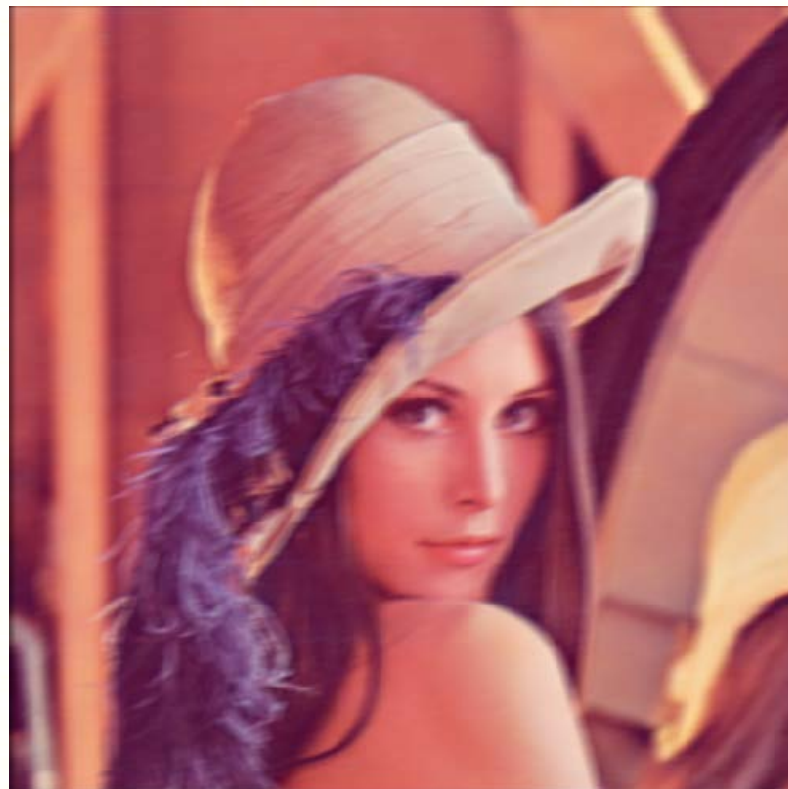
Distorsiuni fotometrice	➤ Iluminare/întunecare a imaginilor ➤ Estompare a contururilor (blurring) ➤ Accentuare a contururilor (sharpening) ➤ Corecție de gama ➤ Filtrare mediană ➤ Adăugare de zgomot (alb gaussian, „saltandpepper”) ➤ Cuantizare ➤ Printare/scanare
Distorsiuni geometrice	➤ schimbarea rezoluției spațiale (scalare) ➤ Rotație ➤ Decupare a unei forme din imagine
Distorsiuni în domeniul comprimat	➤ Compresie JPEG ➤ Compresie JPEG 2000

Distorsiuni și atacuri specifice imaginilor

Estomparea contururilor (blurring)



imaginea originală



blurring pe 10x10 pixeli

```
h = fspecial('average',[10 10]);  
I2=imfilter(I1,h)
```

Distorsiuni și atacuri specifice imaginilor

Accentuarea contururilor (sharpening)



imaginea originală



sharpening folosind un
filtru laplacian

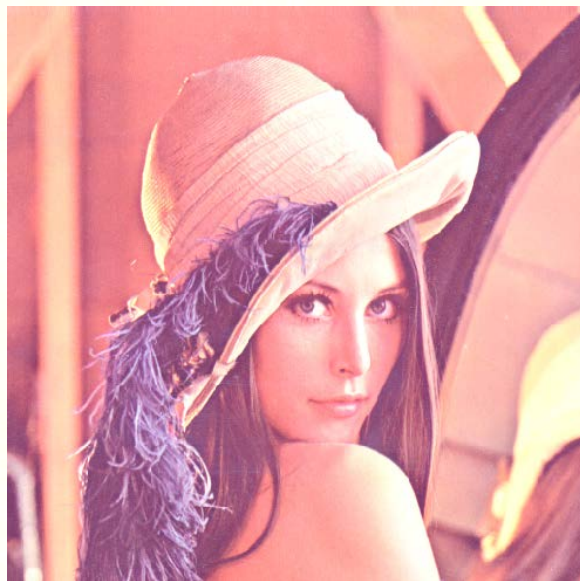
```
h = fspecial('laplacian');  
I2=I1+imfilter(I1,h)
```

Distorsiuni și atacuri specifice imaginilor

Creșterea/scăderea luminozității

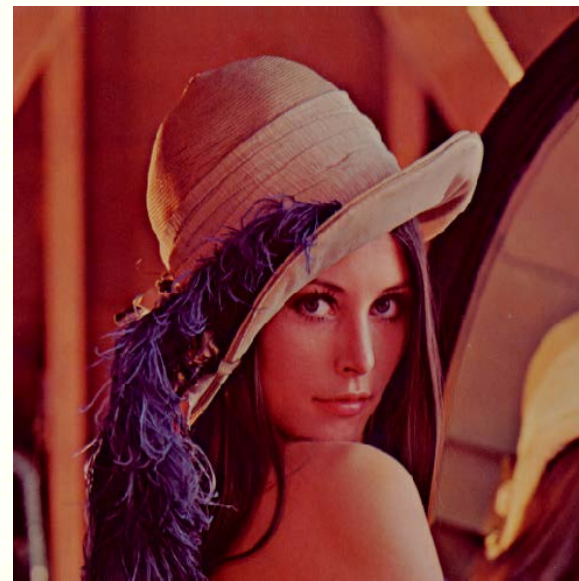


imaginea originală



creșterea luminozității
cu 50

$$I_2 = I_1 + 50$$



scăderea luminozității
cu 50

$$I_3 = I_1 - 50$$

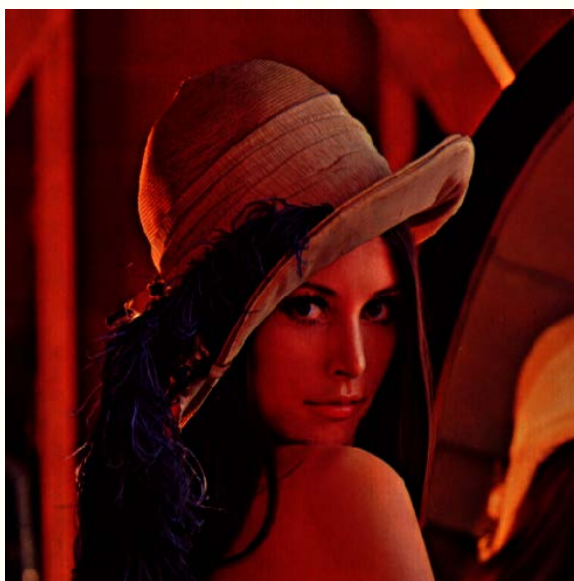
Distorsiuni și atacuri specifice imaginilor

Corecția de gama

$$\begin{bmatrix} R' \\ G' \\ B' \end{bmatrix} = \begin{bmatrix} R^{1/\gamma} \\ G^{1/\gamma} \\ B^{1/\gamma} \end{bmatrix}$$



imaginea originală



Corecția de gama cu
 $\gamma = 2$



Corecția de gama cu
 $\gamma = 0,5$

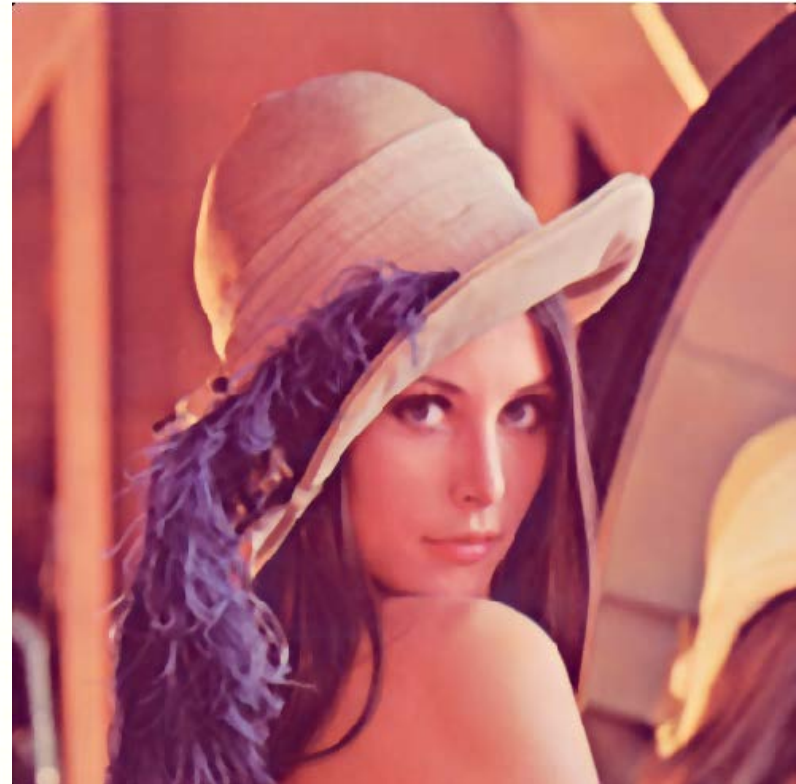
$$I_2 = I_1^{(1/\text{gama})}$$

Distorsiuni și atacuri specifice imaginilor

Filtrare mediană



imaginea originală



imagine filtrată cu un filtru median
de dimensiune 5x5

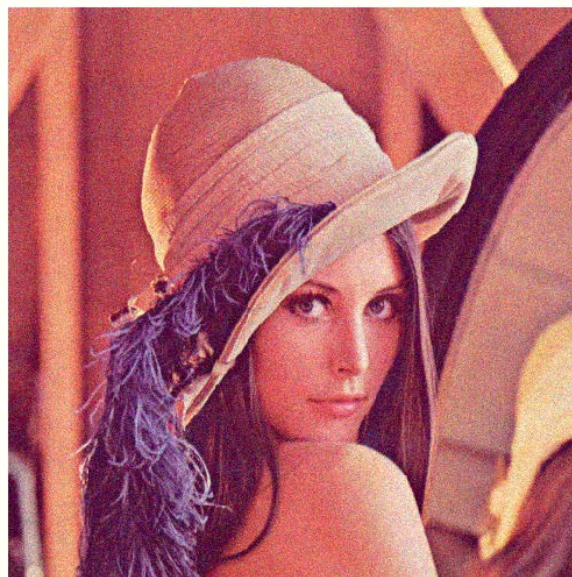
$$I_2 = \text{medfilt2}(I_1, [5 \ 5])$$

Distorsiuni și atacuri specifice imaginilor

Adăugarea de zgomot

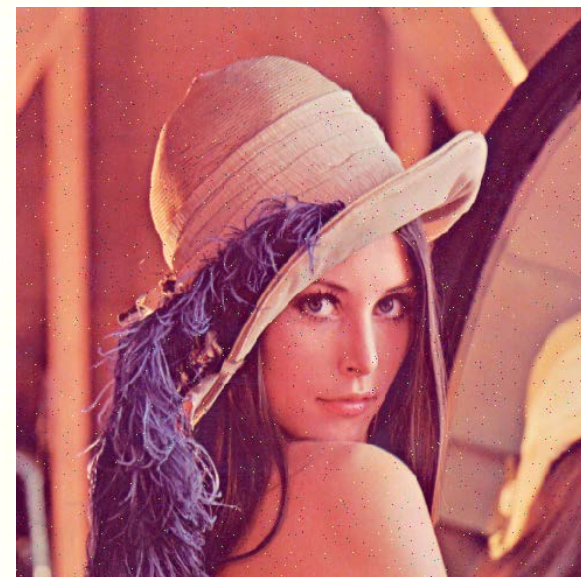


imaginea originală



zgomot gaussian de
medie 0 și varianță
0.005

`I2 = imnoise(I1,'gaussian',0,0.005)`



zgomot
“saltandpepper” de
densitate $d = 0.005$
($d * \text{nr_pixeli afectati}$)

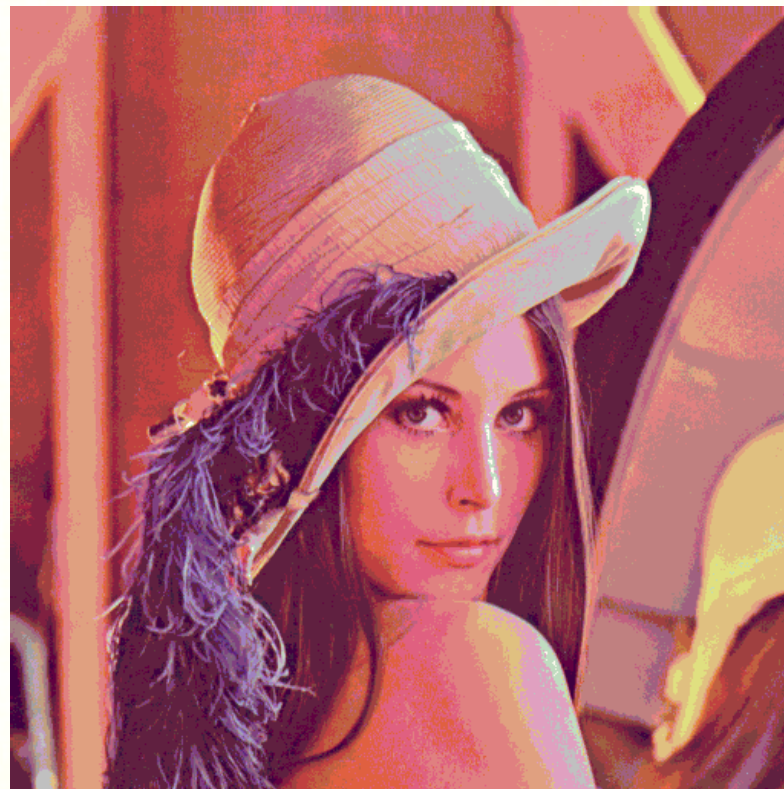
`I2 = imnoise(I1, 'salt & pepper',0.005)`

Distorsiuni și atacuri specifice imaginilor

Conversie analog/numerică



imaginea originală la 24 biți/pixel



imaginea la 8 biți/pixel

Distorsiuni și atacuri specifice imaginilor

Printare/scanare



imaginea originală



Printare/scanare la
300 dpi



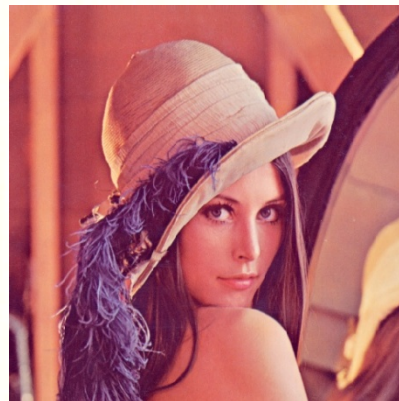
Printare/scanare la
600 dpi

Distorsiuni și atacuri specifice imaginilor

Schimbarea rezoluției



imaginea originală la o rezoluție
de 512x512 pixeli



imaginea la o rezoluție 256x256
pixeli

$I_2 = \text{imresize}(I_1, 0.5)$

Distorsiuni și atacuri specifice imaginilor

Schimbarea ratei de aspect



imaginea originală la o rată de aspect 1:1



imaginea la rata de aspect 16:9

$I_2 = \text{imresize}(I_1, [512 \ 512 * 16/9])$

Distorsiuni și atacuri specifice imaginilor

Rotirea



imaginea originală



imaginea după o rotație cu 45°

$$I_2 = \text{imrotate}(I_1, 45)$$

Distorsiuni și atacuri specifice imaginilor

Decuparea unor părți din imagine (cropping)



imaginea originală



imaginea după decuparea unei forme dreptunghiulare

Distorsiuni și atacuri specifice imaginilor

Compresie JPEG



imaginea originală

```
I1 = imread('lena.bmp')
```



imaginea codată JPEG cu factorul de calitate Q=20

```
imwrite(I1,'lena.jpeg','JPEG','Quality',20)  
I2 = imread('lena.jpeg')
```

Distorsiuni și atacuri specifice pentru video

Distorsiuni fotometrice	➤ cele de la imagini, aplicate fiecărui cadru ➤ reeșantionarea componentelor de cromaticitate (4:4:4, 4:2:2, 4:2:0, 4:1:1)
Distorsiuni geometrice	➤ cele de la imagini, aplicate fiecărui cadru ➤ schimbările formatului de afișare (4/3, 16/9 și 2.11/1) ➤ schimbările rezoluției spațiale (NTSC, PAL, SECAM și formate video comune) ➤ jitter pozițional (apare la transmisiunile analogice fără fir) ➤ atacul prin camera de mână
Distorsiuni în domeniul comprimat	➤ compresie H.26x ➤ compresie MPEG

Creșterea robusteții la atacuri

- posibilități de a crește robustețea la atacuri a unei metode date:
 - inserare redundantă a aceluiași watermark
 - **Ex:** același watermark în fiecare bloc de 8x8 coeficienți DCT
 - inserarea de watermark-uri diferite
 - **Ex:** watermark-uri care sa fie rezistente la diferite tipuri de atacuri
 - utilizare de coduri corectoare de erori

Creșterea robusteții la atacuri

Utilizare de coduri corectoare de erori

- Permit decodorului să decodeze corect mesajul într-un mediu zgomotos
- Exemplu:
 - A -> 00 -> 00000
 - B -> 01 -> 10110
 - C -> 10 -> 01011
 - D -> 11 -> 11101
- cod $[m, n]$ cu dimensiunea cuvântului de informație de n biți și dimensiunea cuvântului de cod de m biți
- acesta reduce dimensiunea utilă a watermark-ului de $R = m/n$ ori

Creșterea robusteții la atacuri

- distanța Hamming $d(x,y)$ dintre două cuvinte de cod x și y este nr. de poziții în care biții diferă
- **Ex:** pentru exemplul anterior:
$$d(A,B) = 3,$$
$$d(A,D) = 4, \dots$$
- fie C un cod $[m, n]$
- distanța Hamming a codului C este:
$$d = \min \{ d(x,y) \mid x, y \text{ fac parte din } C, x \neq y \}$$
- **Ex:** pentru codul din exemplu $d = 3$

Creșterea robusteții la atacuri

- Fie C un cod $[m, n]$ având distanța Hamming $d=2e+1$
- Atunci:
 - C poate corecta e erori
 - C poate detecta $2e$ erori
- pentru codul din exemplu $d=3$
 - poate corecta 1 eroare
 - poate detecta 2 erori