Watermarking – scurt istoric

- subdomeniu al steganografiei
- **steganografie**:
  - *steganos* (acoperit, ascuns)
  - *graphia* (scris)
  - steganografia = *scrierea ascunsă*
- criptografia - codează mesajul pentru a fi neinteligibil pentru persoane neautorizate
- steganografia - ascunde existenţa mesajului

Watermarking – scurt istoric

Exemple istorice:

- Egipt, acum 4000 de ani
  - informaţii în mormântul unui nobil prin substituiri de simboluri hieroglifice
- Grecia Antică
  - mesaj scris sub vopseaua unei mese
  - tunderea mesagerului şi tatuarea mesajului sau a unei imagini pe cap
  - marcarea diferitelor litere dintr-un text cu cerneală invizibilă

Watermarking – scurt istoric

Exemple istorice:

- watermark vizibil pentru marcarea bancnotelor
- Johannes Trithemius (1462-1526), un călugăr german, a codat litere folosind cuvinte religioase
- Giovanni Baptista Porta (1593) - utilizarea unei măști

Honor Militiae tuus suit Carolus pater, nam cum infini to victus est, cum minima exercitu inuitus parte hostis fugit, ac prope ultimum diem iniurius peribit, necabunt Bere illum; atque extemplo puer Arato peribit, res omnes deprehensae bonae si sunt, ante Sillam, & optimo capite non poenitentias amplius decidere sperabit. Vale.

Watermarking – scurt istoric

Exemple istorice:

- sec. XVII, episcopul Francis Godwin
  - watermarking pentru protecția drepturilor de autor
  - nume în prima literă a fiecărui capitol din cartea sa
- Bach – watermark audio scriind B-A-C-H în note muzicale prin numărul de apariţii ale unor note
- 1950 Muzak Corporation
  - identificare autor prin watermarking audio
  - aplicarea intermitentă a unui filtru îngust în semnalul audio folosind un cod bazat pe codul Morse

Watermarking – scurt istoric

- în al doilea război mondial tehnicile de steganografie erau deja larg răspândite
- serviciul poştal din SUA a interzis mai multe obiecte ce ar fi putut ascunde mesaje (jocuri de şah, reviste de cuvinte încrucişate, fragmente de ziar)
- mesaj transmis de un spion german:

  Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

- extrăgând a doua literă a fiecărui cuvânt se obţine:

  Pershing sails from NY June 1.

Watermarking – scurt istoric

- tehnicile steganografice folosite ca amprentă:
  - Premierul Margaret Thatcher a ordonat ca editoarele de text să fie reprogramate
  - identitatea utilizatorului să fie codată în spaţierea dintre cuvinte
- în 1988, Komatsu şi Tominaga au fost primii care au folosit termenul „digital watermarking” pentru sistemul lor de autentificare a imaginilor
- începutul unei cercetări intense a fost o lucrarea scrisă de Cox şi al. în 1996: *Secure Spread Spectrum Watermarking for images, audio and video*

Watermarking digital

- **watermark digital** = semnal digital inserat într-un document digital (text, audio, imagine, video)
- Clasificare în funcție de perceptibilitate
  - **watermark vizibil**
    - descurajarea utilizării neautorizate
    - reducere a valorii comerciale a documentului
  - **watermark invizibil**
    - watermark imperceptibil pentru ochiul/urechea umană
    - poate fi extras de ex. pentru a caracteriza proprietarul

Watermark vizibil

Watermark vizibil

+

=

Watermark digital

Motivație:

- distribuția conținutului multimedia digital este tot mai rapidă, mai facilă
- utilizatorii multimedia au posibilitatea să modifice, să producă copii ale conţinutului digital și să le distribuie ilegal
- produsele şi serviciile multimedia digitale nu pot fi lansate corespunzător în comerţul electronic
- necesitatea rezolvării acestei probleme de securitate

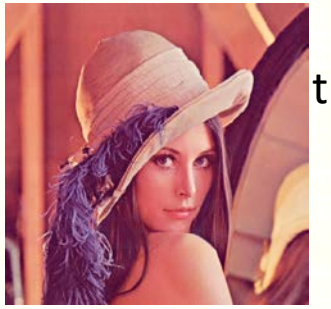
Criptare vs. watermarking

- **Criptografie**
  - odată ce documentul digital este decriptat, nu mai este protejat
  - poate fi copiat și retransmis
- **Watermarking**
  - Informația este ascunsă în documentul digital
  - nu se pierde la copiere/retransmitere
  - obiectivul este să rămână permanent în documentul gazdă și să nu poată fi eliminat

Cerințele unui sistem de watermarking

- **Transparenţă perceptuală**
  - să nu poată fi detectat de ochiul/urechea umană
  - să nu afecteze datele gazdă
- **Robustețe**
  - să rămână permanent în datele gazdă
  - rezistent la procesări de semnal și distorsiuni neintenționate
  - rezistent la atacuri intenționate
- **Securitate**
  - cunoaşterea exactă a algoritmului de ascundere şi de extragere a watermark-ului nu ajută o parte neautorizată să extragă watermark-ul

Robustețea watermark-ului



imagine cu watermark

transmisie

Distorsiuni intenționate sau neintenționate

- **Conversie D/A – A/D**
- **Adăugare de zgomot**
- **Filtrare numerică**
- **Atacuri geometrice**
- **Compresie cu pierderi**

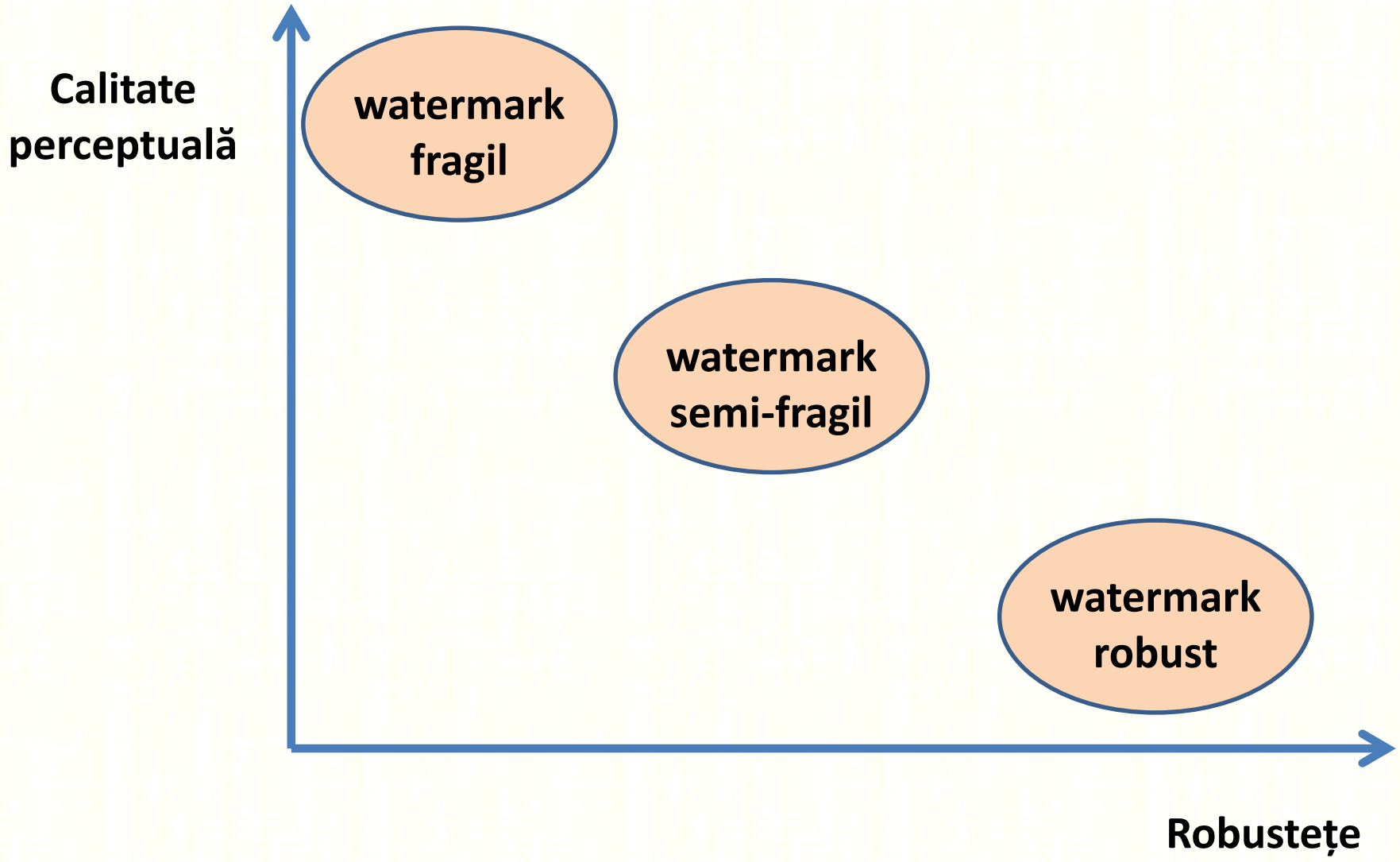
transmisie

imagine cu watermark alterată

Robustețea watermark-ului

- nu e ușor să inserezi un watermark robust
- teoretic orice watermark poate fi eliminat
- practic, eliminarea poate face datele inutilizabile
- efortul de eliminare > valoarea datelor originale
- provocare: compresia datelor
  - orice spațiu liber pentru inserare poate fi eliminat prin compresie

Calitate perceptuală vs. robustețe

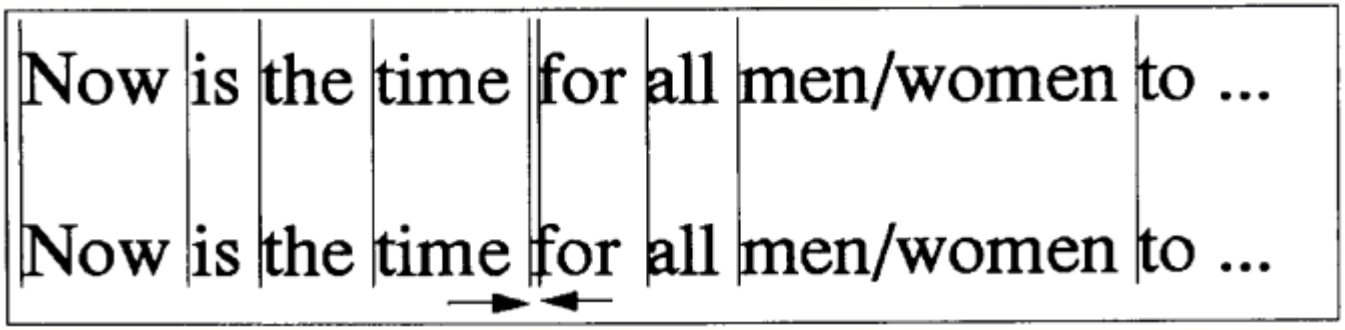


Domenii de aplicabilitate

- Protecţia drepturilor de autor
- Amprentarea
- Protecţia la copiere
- Monitorizarea emisiei
- Autentificarea datelor
- Indexarea
- Siguranţa medicală
- Ascunderea datelor

Watermarking invizibil pentru text

- Codarea distanței între linii (Line Shift Coding)
- Codarea distanței între cuvinte (Word Shift Coding)



- Codarea caracterelor (Feature Coding)

Tehnici de watermarking pentru imagini și video

Criteriu de clasificare	Clasificare
Transparenţă perceptuală	vizibil, invizibil
Robusteţea watermark-ului	robust, semi-fragil, fragil
Tipul watermark-ului inserat	secvență pseudo-aleatoare, text, siglă, imagine
Domeniul de procesare	domeniul spaţial
	domeniul transformat (DCT, DFT, DWT)
	domeniul comprimat (JPEG, JPEG2000, MPEG1-4, H.26x)
Mod de inserare	LSB, spectru împrăștiat, cuantizare
Date necesare pentru detecție/extragere	privat public (blind)

Tehnici de watermarking pentru imagini

Tehnici de watermarking pentru imagini

Cele mai utilizate tipuri de metode:

1. Metode LSB (Least Significant Bits)
2. Metode cu spectru împrăștiat (spread spectrum)
3. Metode bazate pe cuantizare

Metode LSB

- cele mai simple metode de watermarking
- biții cei mai puțini semnificativi conțin informație invizibilă pentru ochiul uman
- se modifică acești biți pentru a insera biții de watermark
- de regulă se aplică în domeniul spațial
- metode rapide
- metode puțin robuste la atacuri

Metode LSB

A. Înlocuire a planului de biți

- se înlocuiește bitul *i* cel mai puțin semnificativ al luminanței sau componentei de culoare cu un bit de watermark
- un bit de watermark în LSB al fiecărui pixel → capacitate mare:

$$C = M \times N$$

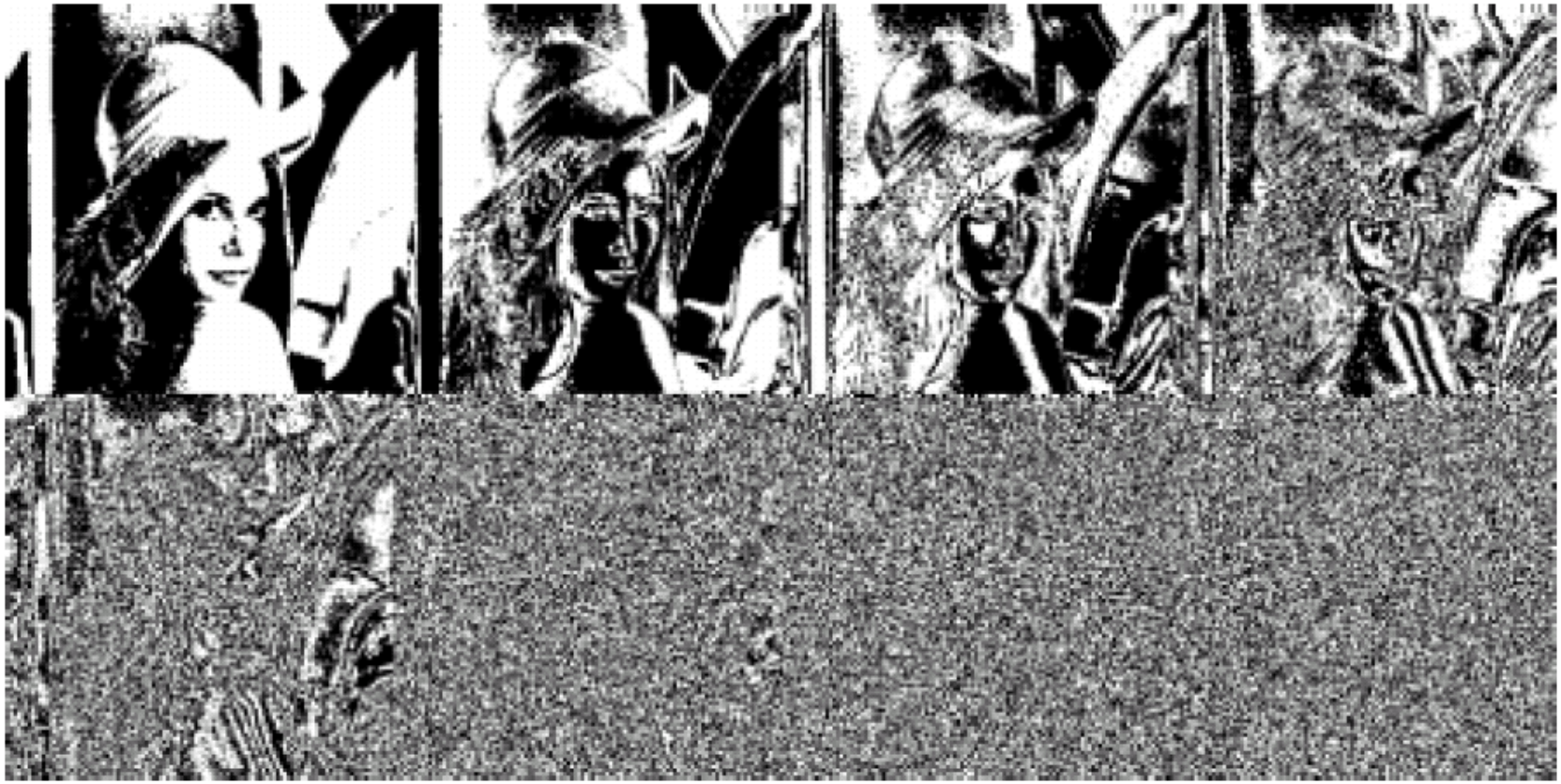
- Imagine cu nuanțe de gri de 512x512 pixeli:

$$C = 512 \times 512 = 32\,kB$$

Metode LSB

A. Înlocuire a planului de biți

Planurile de biți pentru imaginea Lena



Metode LSB

A. Înlocuire a planului de biți

imagine gazdă | watermark | imagine cu watermark | watermark

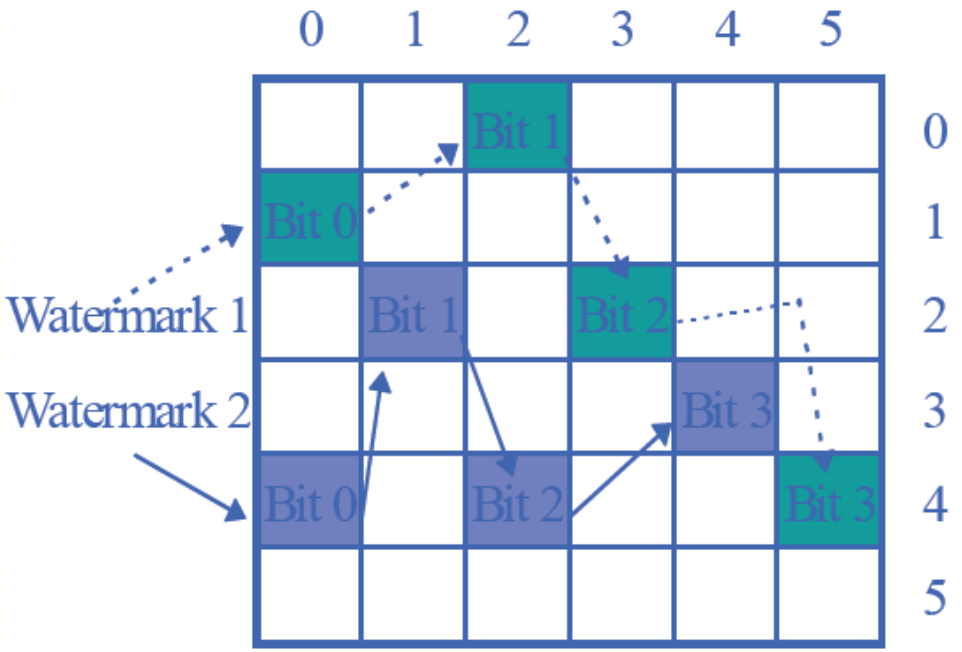
1 bit

4 biţi

7 biţi

Metode LSB

B. Înlocuire LSB a pixelilor selectați cu o cheie secretă

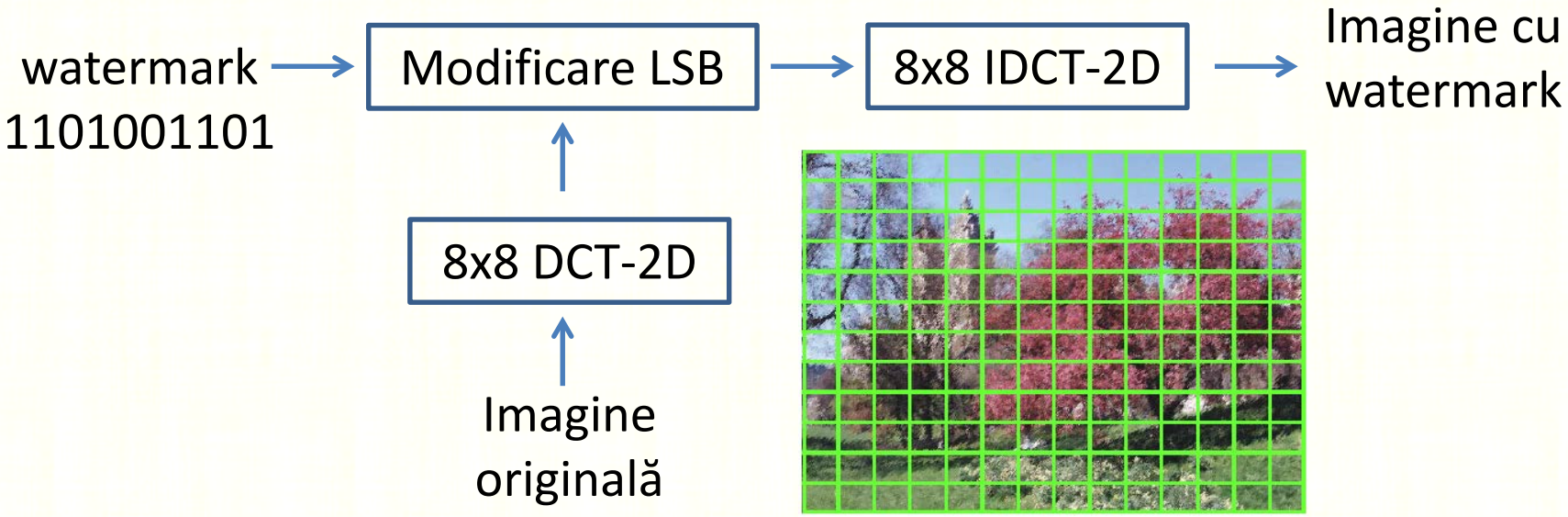


0	1	2	3	4	5	
55	73	71 71	123	123	205	0
120 121	123	70	72	147	199	1
130	123 123	67	68 68	73	123	2
140	133	120	72	70 70	117	3
158 159	142	123 122	123	69	71 70	4
195	178	150	112	67	70	5

- se selectează aleator câte 4 pixeli pentru inserare
- se inserează watermark 1: 0 1 0 1
- se inserează watermark 2: 0 1 1 0

Metode LSB

C. Modificare LSB în domeniul DCT



$$\begin{bmatrix} 1024 & -24 & 10 & 7 & -9 & -4 & 0 & -6 \\ 160 & 15 & 6 & -5 & 3 & -1 & 2 & 0 \\ 36 & -18 & 5 & -8 & 6 & -4 & 2 & -1 \\ -86 & -3 & 5 & 4 & 3 & 0 & 0 & 0 \\ -35 & 12 & -7 & 5 & 2 & -2 & 1 & 0 \\ 12 & 8 & -5 & 2 & 0 & 0 & 0 & 0 \\ -10 & -9 & 7 & 5 & 1 & 1 & 0 & 0 \\ 8 & 5 & -3 & 2 & 0 & 0 & 0 & 0 \end{bmatrix}$$

selectare 10 coef.

$$\begin{bmatrix} 1024 & -24 & 10 & 7 \\ 160 & 15 & 6 & \\ 36 & -18 & & \\ -86 & & & \end{bmatrix}$$

modif. LSB

$$\begin{bmatrix} 1025 & -23 & 10 & 7 \\ 160 & 14 & 7 & \\ 37 & -18 & & \\ -85 & & & \end{bmatrix}$$

Watermarking cu spectru împrăștiat

- watermarking = sistem de comunicații
- imaginea (sau o transformată) = canal de comunicație
- watermark = semnal transmis prin canal
- watermark-ul este împrăștiat în banda disponibilă, ponderat și însumat peste semnal

Watermarking cu spectru împrăștiat

imagine gazdă

k

imagine cu watermark

cheie

watermark

Secvenţă pseudo-aleatoare {-1,1}

Watermarking cu spectru împrăștiat

- inserare watermark:

$$I(x,y) = I(x,y) + k \cdot W(x,y)$$

- detecție watermark: corelaţie dintre imaginea cu watermark şi secvenţa de zgomot pseudo-aleator

$$R_{I'_W(x,y)W(x,y)} = \frac{1}{Z}\sum_{i=1}^{Z} I'_{W_i}(x,y)W_i(x,y)$$

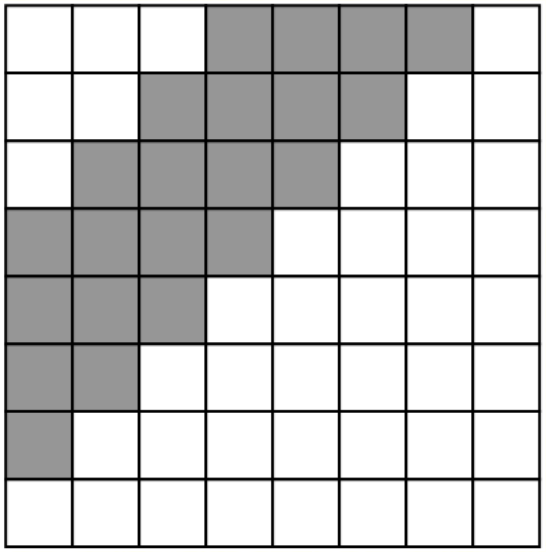
$$R_{I'_W(x,y)W(x,y)} > T \quad \rightarrow \quad W(x,y)\ detectat$$

$$< T \quad \rightarrow \quad W(x,y)\ nedetectat$$

Watermarking cu spectru împrăștiat

Metodă în domeniul DCT

- watermark = semnal 2-D pseudo-aleator de medie 0
- watermark inserat în coeficienții DCT-2D 8 x 8 de frecvenţă medie:



Watermarking cu spectru împrăștiat

Metodă în domeniul DCT

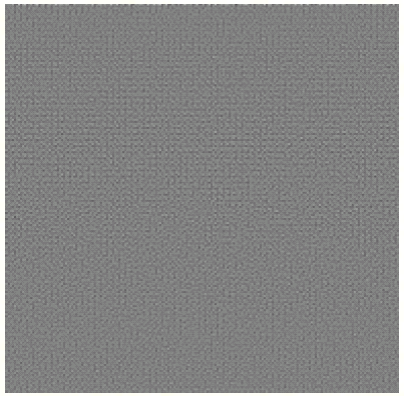
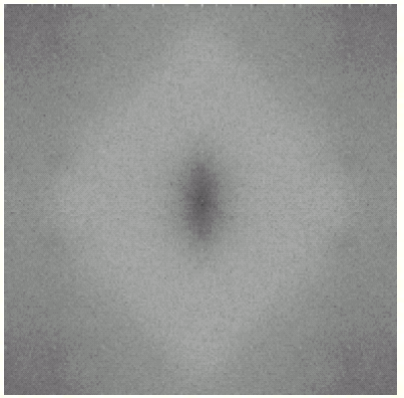
- Watermark independent de conţinutul imaginii

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + k \cdot W_{x,y}(u,v) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \quad x,y = 1,8,16,\ldots$$

- Watermark dependent de conţinutul imaginii

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) \cdot (1 + k \cdot W_{x,y}(u,v)) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \quad x,y = 1,8,16,\ldots$$

Watermarking cu spectru împrăștiat

	k mic	*k* mare	$W(x,y) = I(x,y) - I_W(x,y)$	Spectru watermark
Watermark dependent				
Watermark independent