

Recuperarea zonelor neautentice din imagini

- după autentificare → regiuni neautentice
- restaurarea zonelor neautentice doar prin watermarking
- restaurare ROI
- watermark de restaurare invizibil
- watermark: versiune comprimată sau de rezoluție scăzută a imaginii originale
- extragere la detector chiar dacă materialul a fost supus unor atacuri intenționate

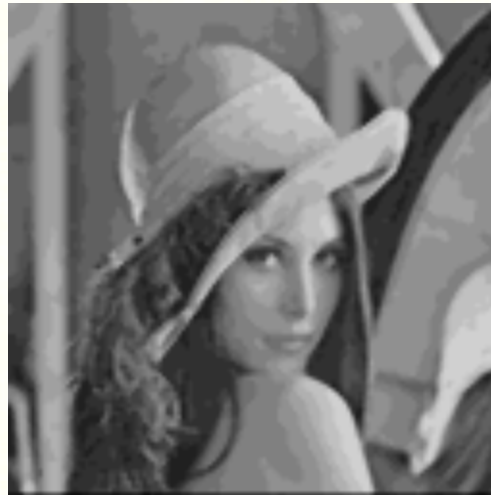
Recuperarea zonelor neautentice din imagini



imagine originală



imagine atacată



imagine recuperată

Recuperarea zonelor neautentice din imagini

Exemplu:

- W = versiune puternic comprimată a imaginii originale
- W generat conform algoritmului următor:
 - se aplică $IntDWT2 \rightarrow LL1, HL1, LH1$ și $HH1$
 - $LL1$ pentru watermark-ul de recuperare
 - $LL1$ = imagine la $M/2 \times N/2$
 - se aplică $IntDCT2$ subbenzii $LL1 \rightarrow$ coeficienți DCT :
$$d = IntDCT2(LL1)$$
 - Scanare zigzag a coeficienților

Recuperarea zonelor neautentice din imagini

- Pastrăm un nr. de coef. DCT
- Codare Huffman:

$$h = \text{codare_huffman}(d)$$

- h = vector binar
- Huffman funcționează mai bine pe valori întregi
- XOR cu o secvență pseudo-aleatoare binară, ce asigură securitatea sistemului

$$w = h \oplus P_{Rand}$$

- P_{Rand} generat pe baza unei chei secrete

Recuperarea zonelor neautentice din imagini

- codare BCH:

$$bch = \text{codor_bch}(w)$$

– bch de lungime mai mare decât w

- Permutare aleatoare:

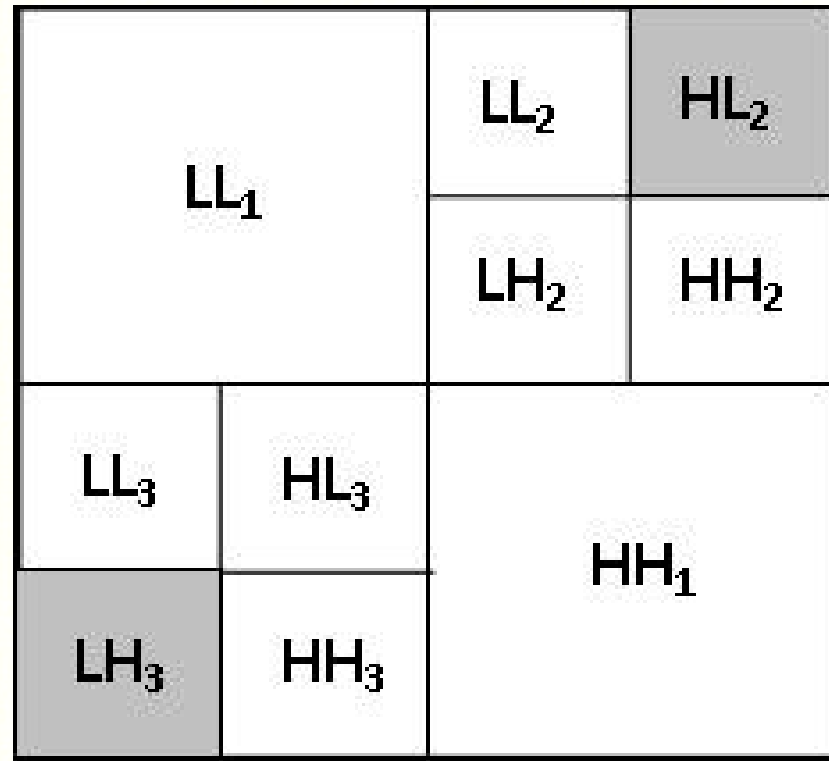
$$W = p(bch)$$

– p = permutarea aleatoare bazată pe cheia secretă.

Recuperarea zonelor neautentice din imagini

- W inserat în HL2 și LH3
 - În funcție de dimensiunea lui W, locațiile de inserare pot varia.
 - codor BCH (31,16,3):
 - dim. simbolul de informație 16 biți,
 - dimensiunea cuvântului de cod 31 de biți
 - capacitatea de a corecta 3 biți
 - codare BCH (31,16,3) → în fiecare coeficient *IntDWT2* din subbenzile HL2 și LH3 vor fi inserați câte doi biți
 - înlocuirea biților de poziția 3 și 4 cea mai semnificativă cu biții W
- Aplicare *IntDWT2* Inversa

Recuperarea zonelor neautentice din imagini



Recuperarea zonelor neautentice din imagini

Extragere watermark:

- aplicarea funcțiilor inverse
- Imaginea cu watermark descompusă folosind *IntDWT2*
- selectare subbenzi HL2 și LH3 ce conțin watermark-ul
- Extragere biți 3 și 4 din fiecare coef. din HL2 și LH3
→ vector binar W'
- Permutare inversă:

$$p' = p_inv(W')$$

- decodare BCH

$$w' = decoder_bch(p')$$

Recuperarea zonelor neautentice din imagini

- XOR între w' și secvența pseudo-aleatoare binară generată local pe baza cheii secrete:

$$h' = w' \oplus P_{Rand}$$

- Decodare Huffman:

$$d' = huffman_deco(h')$$

- Ordonare zigzag a coeficienților
- Aplicare *IntDCT2* inversă

$$LL1' = inverse_idct2(d')$$

Recuperarea zonelor neautentice din imagini

- subbanda LL1' poate fi extrasă, chiar dacă unele regiuni din imagine au fost modificate intenționat.
- robustețe la procesări de imagini neagresive ușoare

Recuperarea zonelor neautentice din imagini



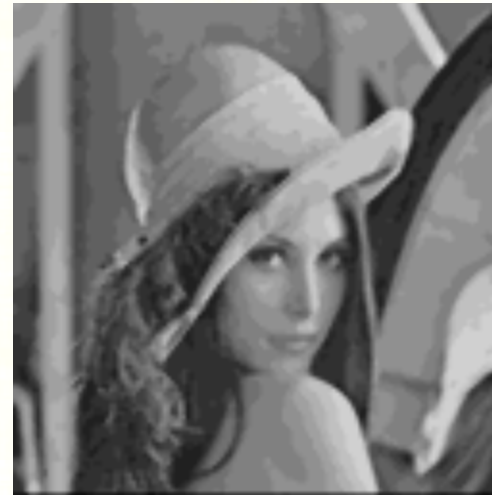
imagine originală



imaginea cu watermark-ul de restaurare



Imagine atacată, bloc 64x64



imaginea recuperată

Tehnici pasive de autentificare

- Dezavantaj tehnici bazate pe watermarking
 - watermark-ul trebuie inserat în momentul capturii
- Altă abordare: folosirea tehnicilor pasive de autentificare a imaginilor
 - funcționează în absența oricărui tip de watermark/semnătură
 - materialul gazdă nu este alterat
 - bazate pe proprietățile intrinseci ale materialului multimedia

Tehnici pasive de autentificare

Clasificare:

- tehnici la nivel de pixel
- tehnici bazate pe formatul materialului multimedia
- tehnici bazate pe analiza artefactelor introduse de camerele digitale prin intermediul lentilelor, senzorilor sau procesărilor interne
- tehnici ce exploatează anomalii între obiecte fizice, lumină și cameră
- tehnici geometrice

Metode de autentificare la nivel de pixel

- **Clonarea**

- una dintre cele mai întâlnite falsificări
- copiere și alipire
- vizual dificil de detectat
- regiunea clonată poate avea orice formă și poziție → nu pot fi căutate toate posibilitățile



Metode de autentificare la nivel de pixel

Exemple de algoritmi:

1. Căutarea exhaustivă
2. Maximul autocorelației
3. Potrivirea blocurilor

Metode de autentificare la nivel de pixel

1. Căutarea exhaustivă



- Calcul diferențe

$$\Delta x_{ij} = |x_{ij} - x_{i+k \bmod(M) \ j+l \bmod(N)}|$$

- Comparare cu un prag t + operații morfologice
- Complexitate aritmetică mare: $(MN)^2$
- Alegere problematică a lui t

Metode de autentificare la nivel de pixel

2. Maximul autocorelației

$$r_{k,l} = \sum_{i=1}^M \sum_{j=1}^N x_{i,j} x_{i+k,j+l}, \quad i, k = 0, \dots, M-1, j, l = 0, \dots, N-1$$

- Zonele originale și copiate produc maxime ale autocorelației pentru o pereche (k,l)

Pași:

- FTS a imaginii
- Calcul autocorelație
- Găsirea maximului lui r , găsirea lui (k,l) și luarea unei decizii pe baza dimensiunii minime a zonei falsificate

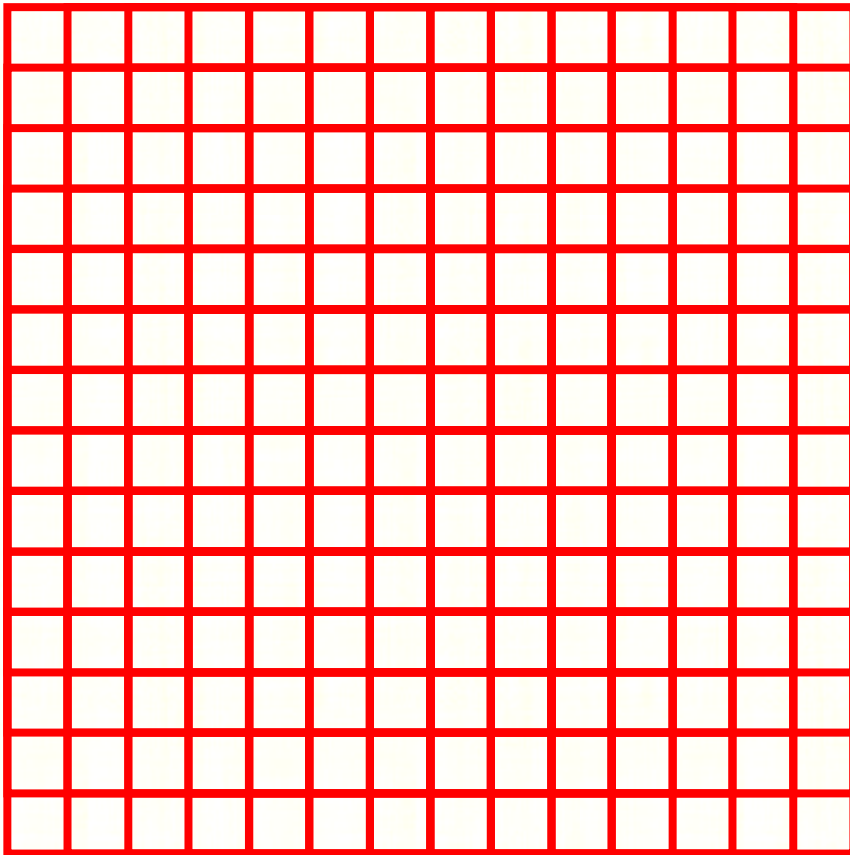
Metode de autentificare la nivel de pixel

3. Potrivirea blocurilor

- Dimensiune minimă bloc duplicat $B \times B$
- Deplasare fereastră de $B \times B$ cu câte un pixel de la strânga la dreapta și de sus în jos

Metode de autentificare la nivel de pixel

3. Potrivirea blocurilor

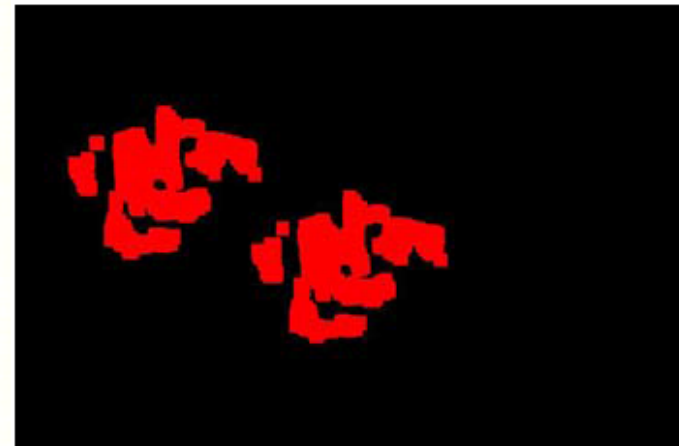


- Ptr. fiecare poziție un vector X_i cu coloanele blocului i
- Matrice A de dim. $B^2 \times (M-B+1)(N-B+1)$ cu $A(i,:) = X_i$
- Fiecare rând corespunde unei poziții a ferestrei
- 2 rânduri identice $\rightarrow$ 2 blocuri identice
- Sortare lexicografică și găsirea a 2 rânduri consecutive identice
- Complexitate: $MN \log_2(MN)$ pași

Metode de autentificare la nivel de pixel

3. Potrivirea blocurilor

— Exemplu:



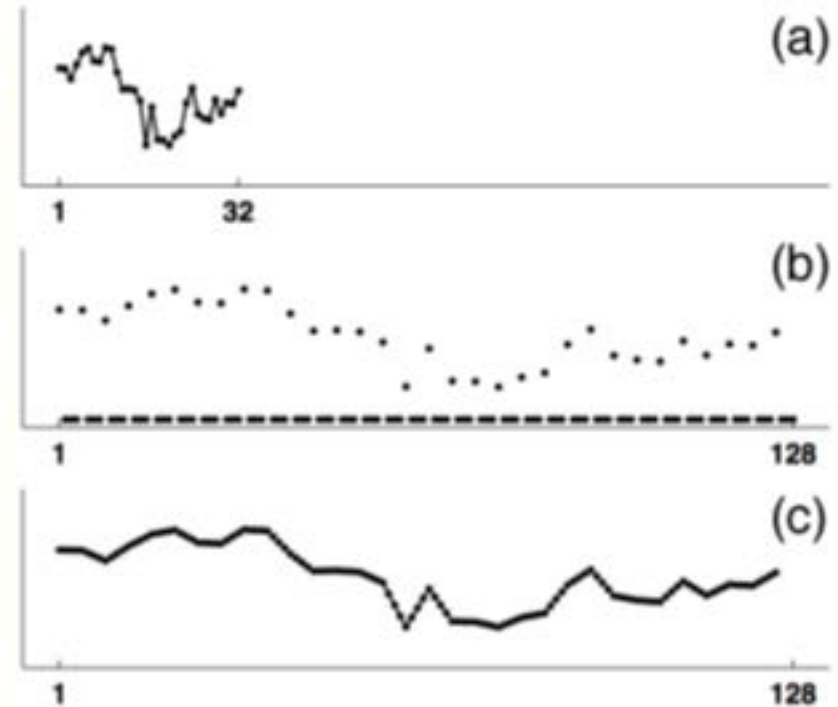
Metode de autentificare la nivel de pixel

- Provocări:
 - reducerea complexității computaționale
 - robustețe la variații minore în imagine datorate zgomotului aditiv sau compresiei cu pierderi

Metode de autentificare la nivel de pixel

- **Re-eșantionarea**

- Falsificare prin rotire și redimensionare
- corelații periodice specifice între pixeli vecini
- Probabilitate foarte mică ca aceste corelații să apară în mod natural



Metode de autentificare la nivel de pixel

- Fie un semnal 1-D $x(t)$ de lungime m .
- $y(t)$ – semnal supraeșantionat cu 2 folosind interpolare

$$y(2i-1) = x(i), i = 1, \dots, m$$

$$y(2i) = 0.5x(i) + 0.5x(i+1)$$

- Prin înlocuire, obținem:

$$y(2i) = 0.5y(2i-1) + 0.5y(2i+1)$$

- un semnal re-eșantionat poate fi detectat prin observarea corelației fiecărui eșantion cu vecinii
- În practică, nu se cunoaște forma corelației introduse de re-eșantionare, nici pixelii care sunt corelați cu vecinii

Metode de autentificare la nivel de pixel

- Colajul
 - alipirea a două sau mai multe imagini, formând o singura imagine compozită.
 - Daca este executată cu atenție, zona de contact a imaginilor este imperceptibilă vizual.
 - aceste manipulări modifică statistica Fourier de ordin superior
 - Fie $x(t)$ un semnal 1-D $x(t)$
 - $X(\omega)$ transformata sa Fourier
 - Spectrul de putere: $P(\omega) = X(\omega)X^*(\omega)$
 - Bispectrul folosit pentru detecția colajului:

$$B(\omega_1, \omega_2) = X(\omega_1)X(\omega_2)X^*(\omega_1 + \omega_2)$$

Metode de autentificare la nivel de pixel

- Bispectrul măsoară corelații de ordin superior între tripletele de frecvențe ω_1 , ω_2 și $\omega_1 + \omega_2$.
- Discontinuități rezultate din alipire se manifestă printr-o creștere în amplitudine a bispectrului

Metode de autentificare pe baza formatului

- Cuantizarea JPEG
 - format JPEG la achiziție
 - gradul de compresie în funcție de cameră
- Dubla compresie JPEG
 - manipulare prin decodare + recodare
 - imaginea falsificată suferă o dublă compresie JPEG
 - dubla compresie va introduce artefacte specifice, ce nu sunt prezente în imaginile compresate o singură dată
 - Acestea pot fi folosite ca detecție a manipulării

Metode de autentificare pe baza formatului

- Detecția zonelor cu dublă compresie JPEG
 - permite localizarea zonelor dintr-o imagine ce au suferit o dublă cuantizare JPEG
 - JPEG cuantizează separat fiecare bloc de dimensiune 8x8 pixeli

Metode de autentificare pe baza camerei

- **Aberațiile cromatice**

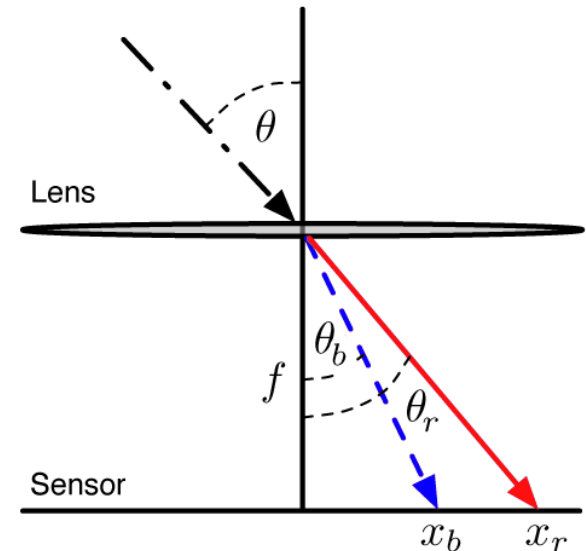
- Modelul ideal de imagistică:

- lumina trece prin lentilă și este concentrată într-un singur punct pe senzor

- Sistem optic real:

- deviază de la acest model ideal
- nu focalizează perfect lumina de orice lungime de undă → aberații cromatice
- deplasare spațială a locațiilor în care lumina de diferite lungimi de undă ajunge pe senzor

- Comparatie estimat local și global al aberațiilor



Aberații cromatice

Metode de autentificare pe baza camerei

- **Matricea de filtre de culoare**
 - Multe aparate digitale au un singur senzor
 - obțin imaginile color folosind o matrice de filtre de culoare (CFA)
 - filtre pentru R, G, B.
 - pentru fiecare locație de pixel este salvată o singură culoare.

$r_{1,1}$	$g_{1,2}$	$r_{1,3}$	$g_{1,4}$	$r_{1,5}$	$g_{1,6}$	
$g_{2,1}$	$b_{2,2}$	$g_{2,3}$	$b_{2,4}$	$g_{2,5}$	$b_{2,6}$	
$r_{3,1}$	$g_{3,2}$	$r_{3,3}$	$g_{3,4}$	$r_{3,5}$	$g_{3,6}$	
$g_{4,1}$	$b_{4,2}$	$g_{4,3}$	$b_{4,4}$	$g_{4,5}$	$b_{4,6}$	$\dots$
$r_{5,1}$	$g_{5,2}$	$r_{5,3}$	$g_{5,4}$	$r_{5,5}$	$g_{5,6}$	
$g_{6,1}$	$b_{6,2}$	$g_{6,3}$	$b_{6,4}$	$g_{6,5}$	$b_{6,6}$	
			$\vdots$			$\ddots$

Matrice Bayer

Metode de autentificare pe baza camerei

- Celelalte două culori estimate din eșantioanele vecine
- Procedeu = interpolare CFA sau demozaicare
- corelații statistice specifice între subseturi de pixeli pentru fiecare canal de culoare
- CFA aranjată într-un model periodic → corelații periodice
- deviații de la acest model reprezintă urme de falsificare

Metode de autentificare pe baza camerei

- **Zgomotul senzorului**
 - Fiecare pixel din senzorul unei camere digitale măsoară o anumită cantitate de lumina incidentă ce ajunge la acesta.
 - Mici imperfecții în procesul de fabricare introduc mici cantități de zgomot în imaginea salvată.
 - Acest zgomot este consistent de-a lungul timpului, putând fi folosit în scopuri de detecție a autenticității

Metode de autentificare pe baza iluminării

- Iluminarea 2-D
 - estimarea direcției sursei de iluminare pleacă de la următoarele presupuneri simplificatoare:
 1. suprafața de interes este Lambertiană (perfect difuză)
 2. suprafața are un indice de reflexie constant;
 3. sursă punctiformă de lumină
 4. unghiul dintre normala suprafeței și direcția iluminării se află în intervalul $[-90^\circ, 90^\circ]$



Direcția iluminării (săgeata galbenă) este inconsistentă