

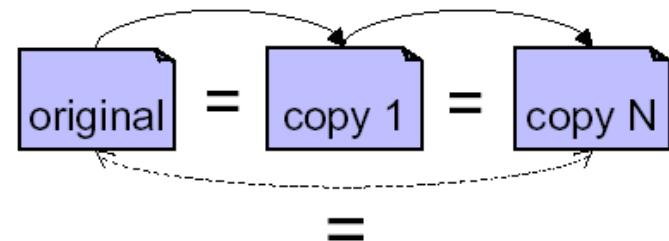
# PENGOLAHAN CITRA DIGITAL

STEGANOGRAPHY

GKV - IF 2020

# Pendahuluan

- Dokumen digital
  - citra (*JPEG/GIF/BMP/TIFF Images*)
  - audio (*MP3/WAV audio*)
  - video (*MPEG video*)
  - teks (*MsWord document*)
- Tepat sama kalau digandakan
- Mudah didistribusikan (misal: via internet)
- Mudah di-edit (diubah)
- Tidak ada perlindungan terhadap kepemilikan, *copyright, editing*, dll.
- Solusi: ***digital watermarking***.



- *Digital watermarking*: penyisipan informasi (disebut *watermark*) ke dalam dokumen digital untuk tujuan:
  - perlindungan *copyright*/kepemilikan
  - *fingerprinting*
  - otentikasi (*integritas content*)
  - dll
- *Watermark* dapat berupa teks, logo, suara, dsb.
- *Watermarking* merupakan aplikasi steganografi.



+ shanty =



Citra semula

Watermark

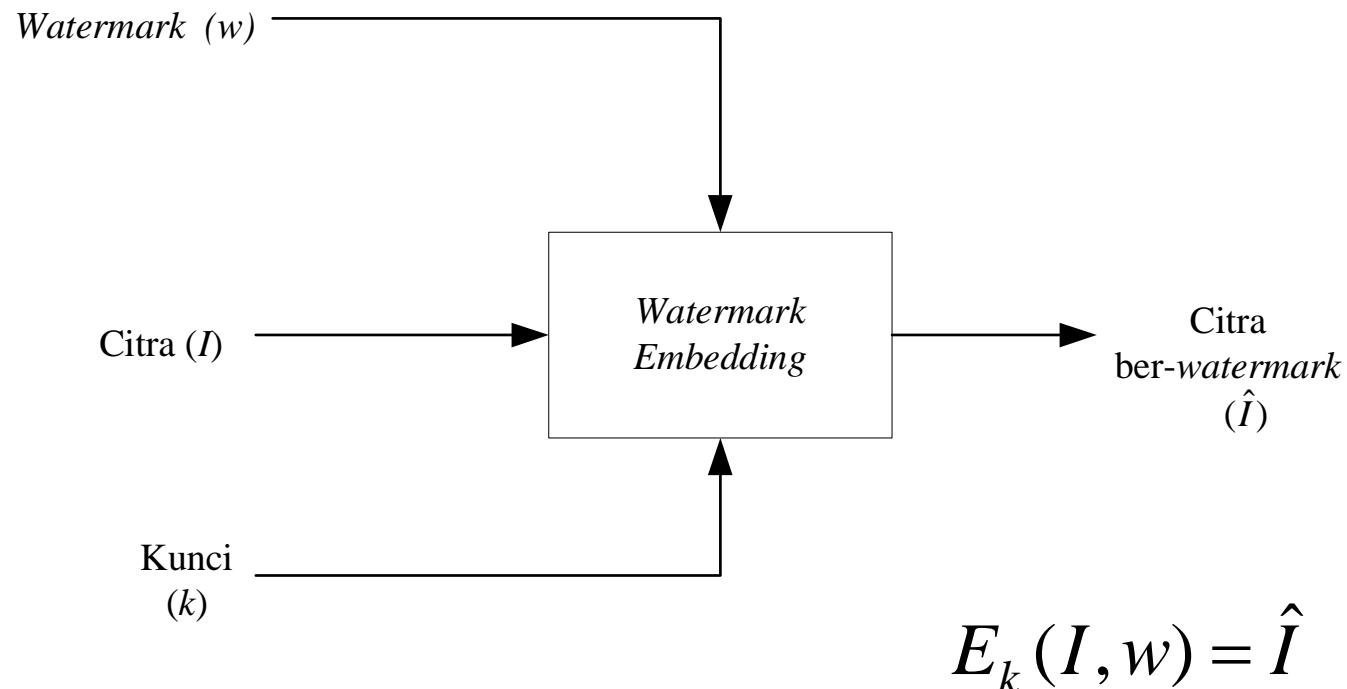
Citra ber-watermark

# Jenis-jenis Watermarking

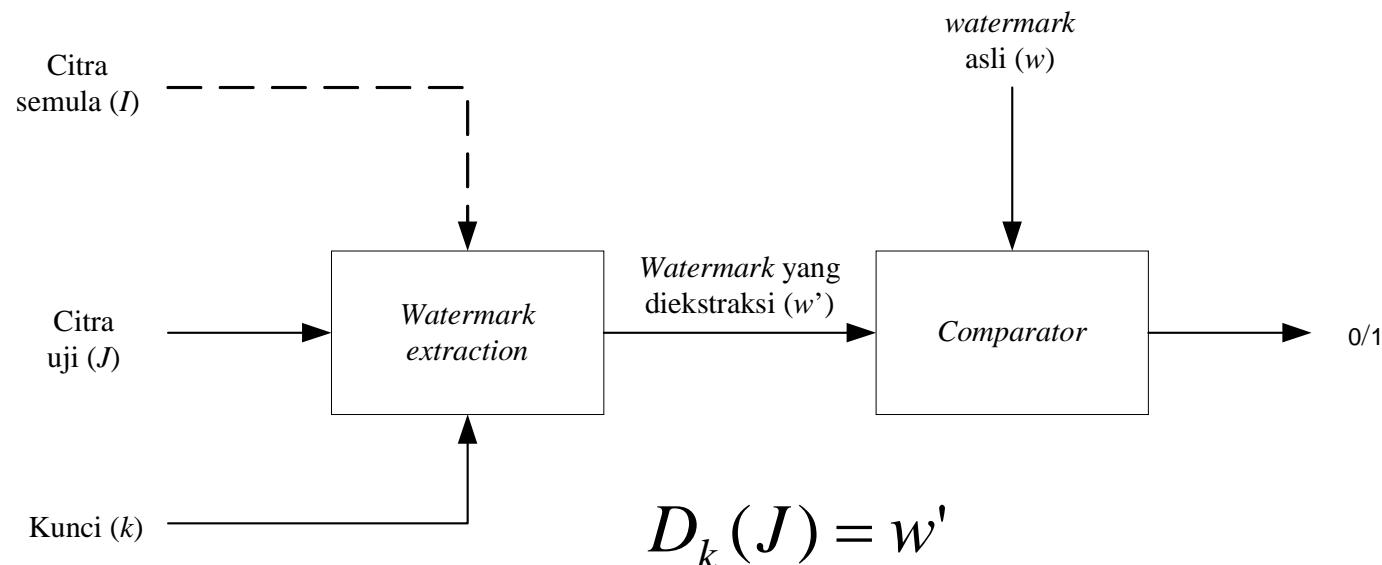
- Bergantung media yang di-watermark, *watermarking* ada beberapa jenis:
  - *Image Watermarking*
  - *Video Watermarking*
  - *Audio Watermarking*
  - *Text Watermarking*

# Digital Image Watermarking

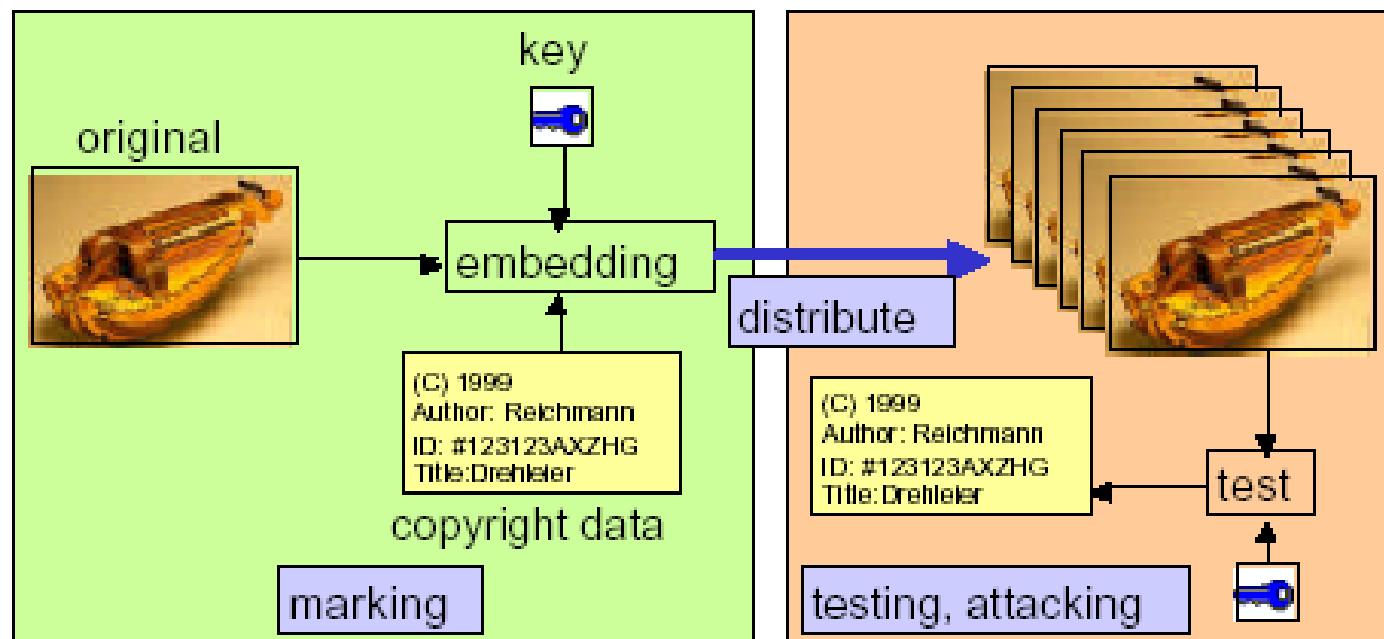
- Penyisipan watermark



- Ekstraksi/deteksi *watermark*



$$C_t(w, w') = \begin{cases} 1, & c \leq t \\ 0, & c > t \end{cases}$$

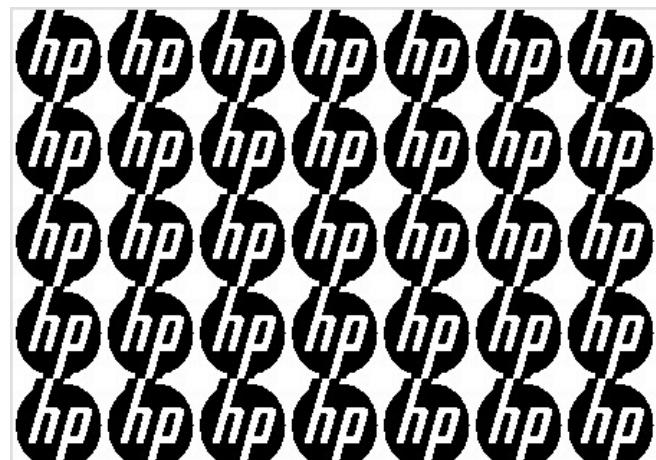




(a)



(b)



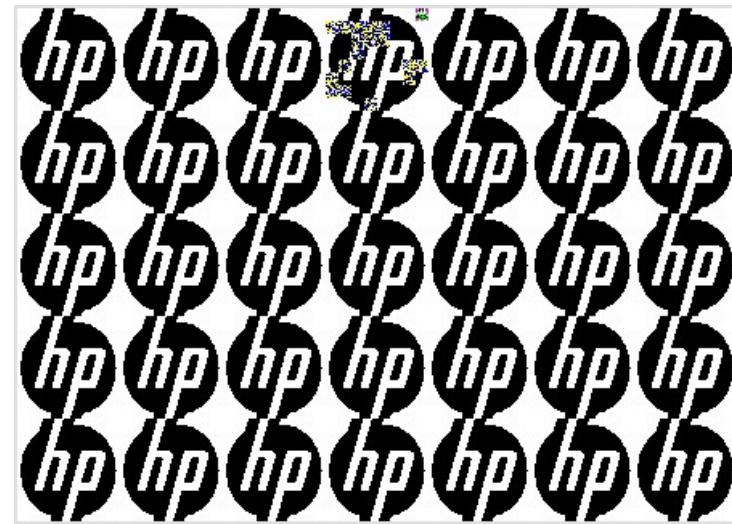
(c)



(d)



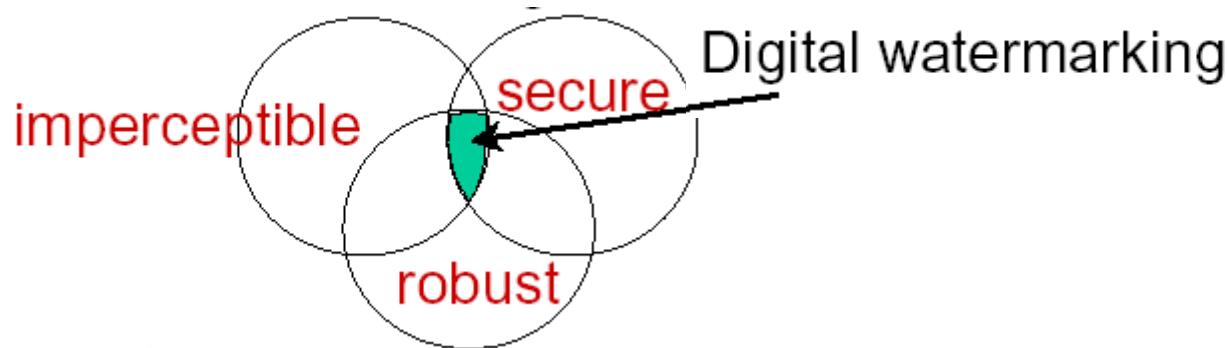
(e)



(f)

- *Watermark* dapat dianggap sebagai **sidi<sup>k</sup> digital** (*digital signature*) atau stempel digital (*finger print*) dari pemilik yang sah atas produk multimedia tersebut.
- Pemberian *signature* dengan teknik *watermarking* ini dilakukan sedemikian sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi.

- Persyaratan umum *watermarking*:
  - *imperceptible*: *watermark* tidak dapat dipersepsi secara visual/auditori karena *watermark* tidak boleh merusak kualitas media *host*.
  - *robustness*: kokoh terhadap manipulasi yang ditujukan untuk merusak atau menghapus *watermark*.
  - *secure*: hanya pihak yang punya otoritas dapat mengakses *watermark*.



# Perbedaan Steganografi dan Watermarking

## Steganografi

- Tujuan: mengirim pesan rahasia apapun tanpa menimbulkan kecurigaan
- Persyaratan: aman, sulit dideteksi, sebanyak mungkin menampung pesan (*large capacity*)
- Komunikasi: *point-to-point*
- Media penampung tidak punya arti apa-apa (*meaningless*)

## *Watermarking:*

- Tujuan: perlindungan *copyright*, pembuktian kepemilikan (*ownership*), *fingerprinting*
- Persyaratan: *robustness*, sulit dihapus (*remove*)
- Komunikasi: *one-to-many*
- Komentar lain: media penampung justru yang diberi proteksi, *watermark* tidak rahasia, tidak mementingkan kapasitas *watermark*

# Jenis-jenis Watermarking

- *Fragile watermarking*

Tujuan: untuk menjaga integritas/orisinalitas media digital.

- *Robust watermarking*

Tujuan: untuk menyisipkan informasi kepemilikan media digital.

## Watermarking pada Citra

- *Visible Watermarking*
- *Invisible Watermarking*

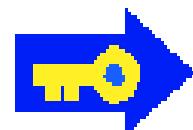
# *Visible Watermarking*



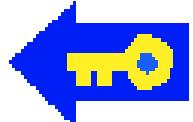
# *Visible Watermarking*



Embed



Remove



# *Invisible Watermarking*



# Aplikasi Watermark

- Memberi label kepemilikan (*ownership*) pada karya digital
- Melindungi isi karya digital (*copyright*).
- Memeriksa integritas isi karya digital (*tamper proofing*) → *Data authentication*
- *User authentication/fingerprinting*: mengotentikasi pengguna spesifik.  
Contoh: distribusi DVD
- Aplikasi medis: foto sinar-X diberi *watermark* berupa ID pasien (memudahkan identifikasi pasien).
- *Convert communication*: untuk sistem komunikasi di negara2 di mana kriptografi tidak dibolehkan.
- *Piracy protection*: mencegah penggandaan yang tidak berizin.

# Sejarah Watermarking

- Abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* dengan cara menekan bentuk cetakan gambar pada kertas yang baru setengah jadi.
- Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas ini biasanya digunakan oleh seniman/sastrawan untuk menulis karya seni.
- Kertas yang sudah dibubuh tanda-air dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

- *Watermark* pada data digital umumnya audio atau gambar.
- *Watermark* berupa teks mengandung kelemahan karena kesalahan satu bit akan menghasilkan hasil teks yang berbeda pada waktu verifikasi (ekstraksi).

## Contoh *robustness*

Citra asli



Citra ber-watermark



Citra ber-watermark  
dikompresi 75%



Citra ber-watermark di-crop



## *Domain Image Watermarking*

- *Spasial*

Menyisipkan watermark langsung pada nilai *byte* dari *pixel* citra.

- *Frekuensi*

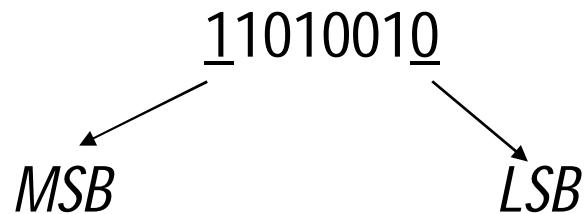
Menyisipkan watermark pada koefisien frekuensi dari citra.

- *Wavelet*

Menyisipkan watermark pada koefisien wavelet dari citra.

## Domain Spasial – *LSB coding*

- Sama seperti steganografi.
- Mengganti bit *LSB* dengan bit data.



*LSB = Least Significant Bit*

*MSB = Most Significant Bit*

- Mengubah bit *LSB* hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya

- Misalkan sebagian pixel adalah citra

00110011

10100010

11100010 01101111

(sekelompok *pixel* berwarna merah)

- Misalkan *watermark*: 0111
- *Encoding*:

00110010

10100011 11100011 01101110

(*pixel* berwarna “merah berubah sedikit”)

- Kelemahan:
  1. tidak kokoh terhadap perubahan
  2. mudah dihapus dengan mengganti semua bit *LSB* dari media ber-watermark.

# Metode *Spread Spectrum*

- Diusulkan pertama kali oleh Cox dalam makalah "*Secure Spread Spectrum Watermarking for Multimedia*" (1997)
- *Watermark* disebar (*spread*) di dalam citra.
- *Spread spectrum* dapat dilakukan dalam 2 ranah:
  1. Domain spasial  
Menyisipkan *watermark* langsung pada nilai *byte* dari *pixel* citra.
  2. Domain *transform* (*frekuensi* dan *wavelet*)  
Menyisipkan *watermark* pada koefisien transformasi dari citra.

# DCT

- Penyisipan dalam ranah frekuensi lebih *robust* dibandingkan dalam ranah spasial.
- Pada metode Cox, komponen frekuensi yang disisipi adalah komponen yang signifikan secara persepsi.
- Ada *trade-off* antara *robustness* dan *visibility* ( $\alpha$ )
- Citra ditransformasi ke dalam ranah frekuensi dengan *DCT (Discrete Cosine Transform)*
- Setelah penyisipan, ranah frekuensi dikembalikan ke ranah spasial dengan *IDCT (Inverse Discrete Cosine Transform)*

- *DCT*:  $C(p, q) = \alpha_p \alpha_q \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} I(m, n) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}$
- *IDCT*:  $I(m, n) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q C(p, q) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}$
- Keterangan: Citra berukuran  $M \times N$

$$0 \leq p \leq M - 1 \quad 0 \leq q \leq N - 1$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & , p = 0 \\ \sqrt{\frac{2}{M}} & , 1 \leq p \leq M - 1 \end{cases} \quad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & , q = 0 \\ \sqrt{\frac{2}{N}} & , 1 \leq q \leq N - 1 \end{cases}$$

# Koefisien DCT

The figure shows a 6x6 grid divided into 36 smaller squares. The grid is shaded as follows:

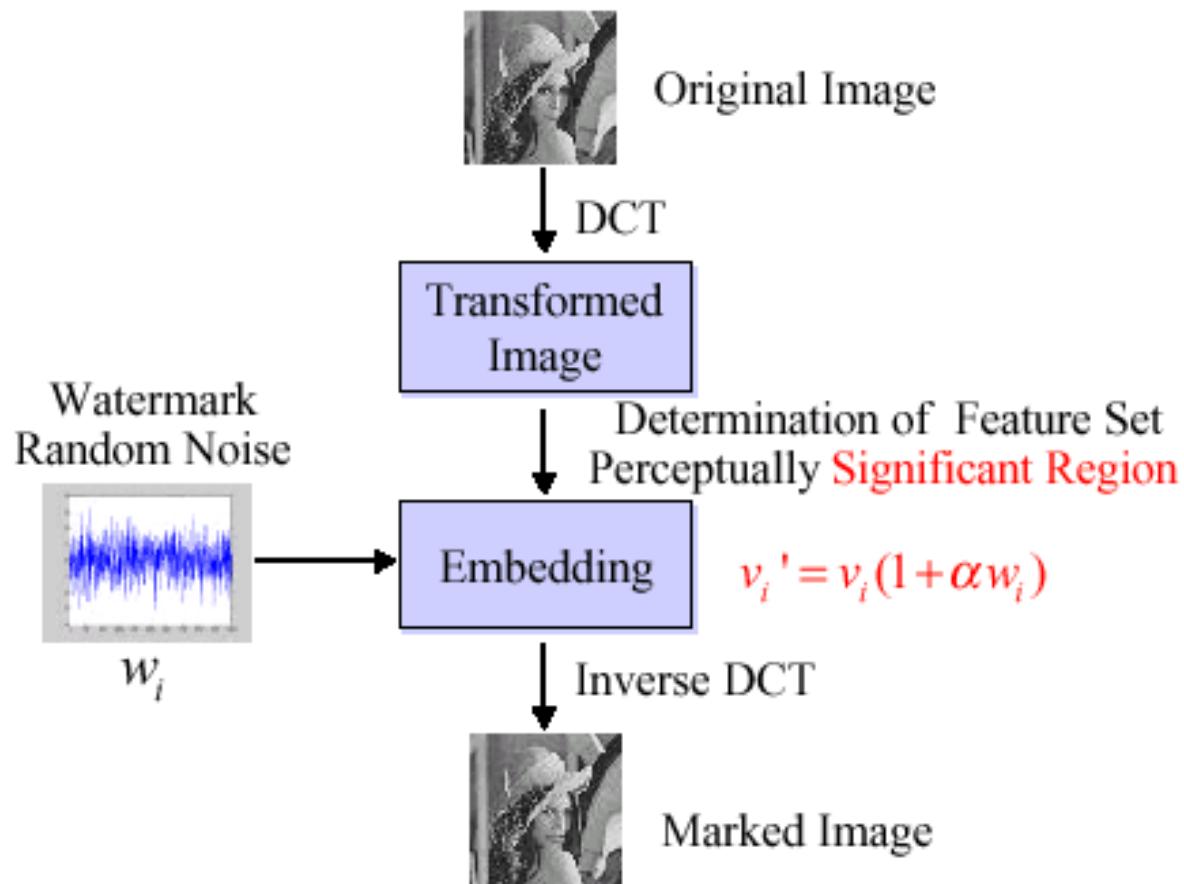
- Force  $F_L$ :** Located in the top-left corner (row 1, column 1). It consists of a single white square with a black border.
- Force  $F_M$ :** Located in the middle-left column (rows 2-4, column 1). It consists of three gray squares stacked vertically.
- Force  $F_H$ :** Located in the bottom-right row (row 6, columns 3-6). It consists of four white squares arranged in a horizontal row.

- $\text{Watermark } W = w_1, w_2, \dots, w_n$
- $\text{Watermark}$ : bilangan riil acak (*pseudo-noise*) yang mempunyai distribusi Normal:

$$p(w) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{w^2}{2\sigma^2}\right)$$

- Cox memilih  $\text{watermark}$  mempunyai distribusi  $N(0, 1)$ , yaitu *mean* = 0, variansi = 1.
- Menurut Cox,  $\text{watermark}$  tsb mempunyai kinerja lebih baik daripada data yang terdistribusi *uniform*.

- Penyisipan *watermark*:



- Pendeksiyan *watermark*:

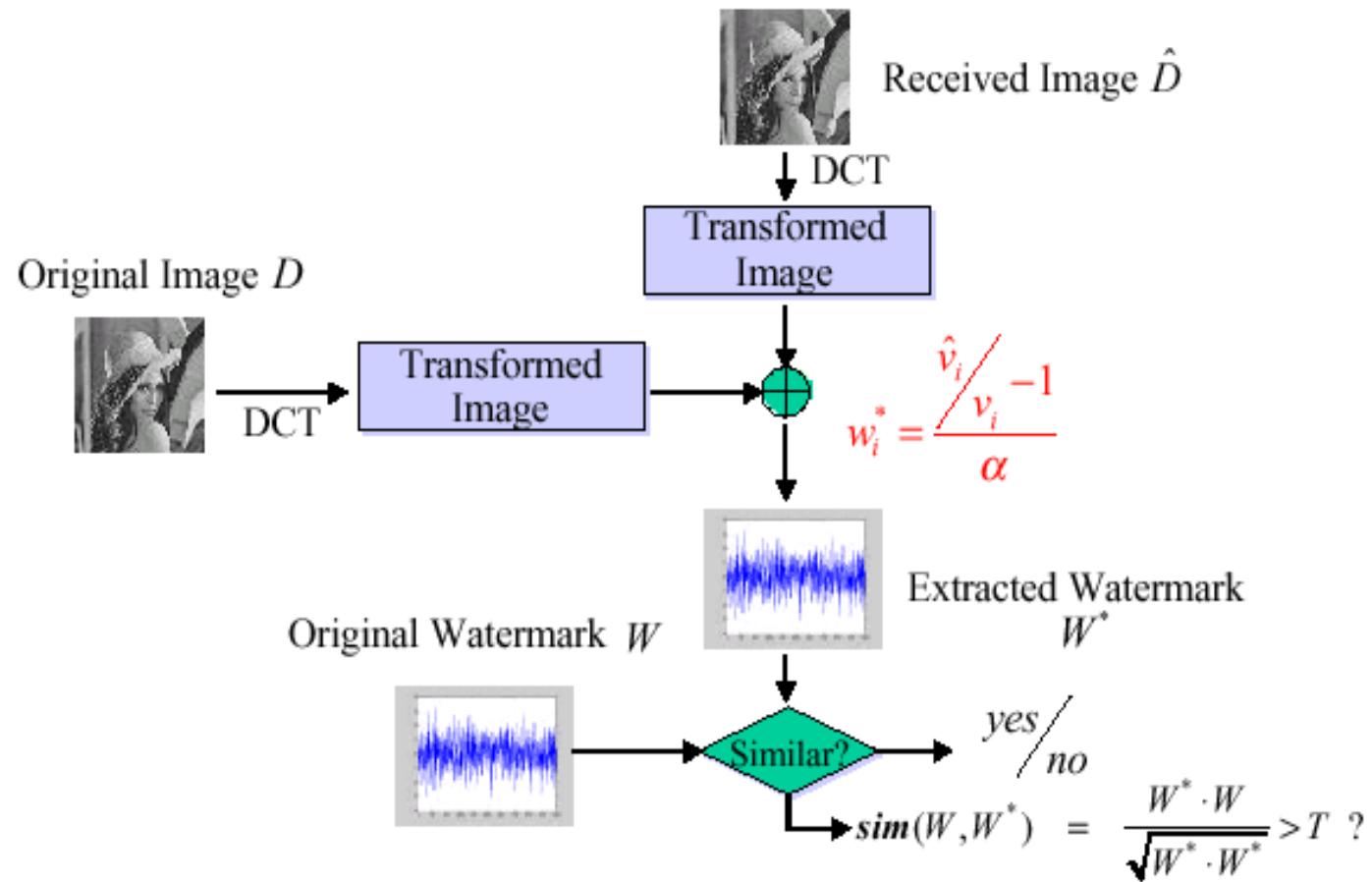




Fig. 4. Bavarian couple image courtesy of Corel Stock Photo Library.

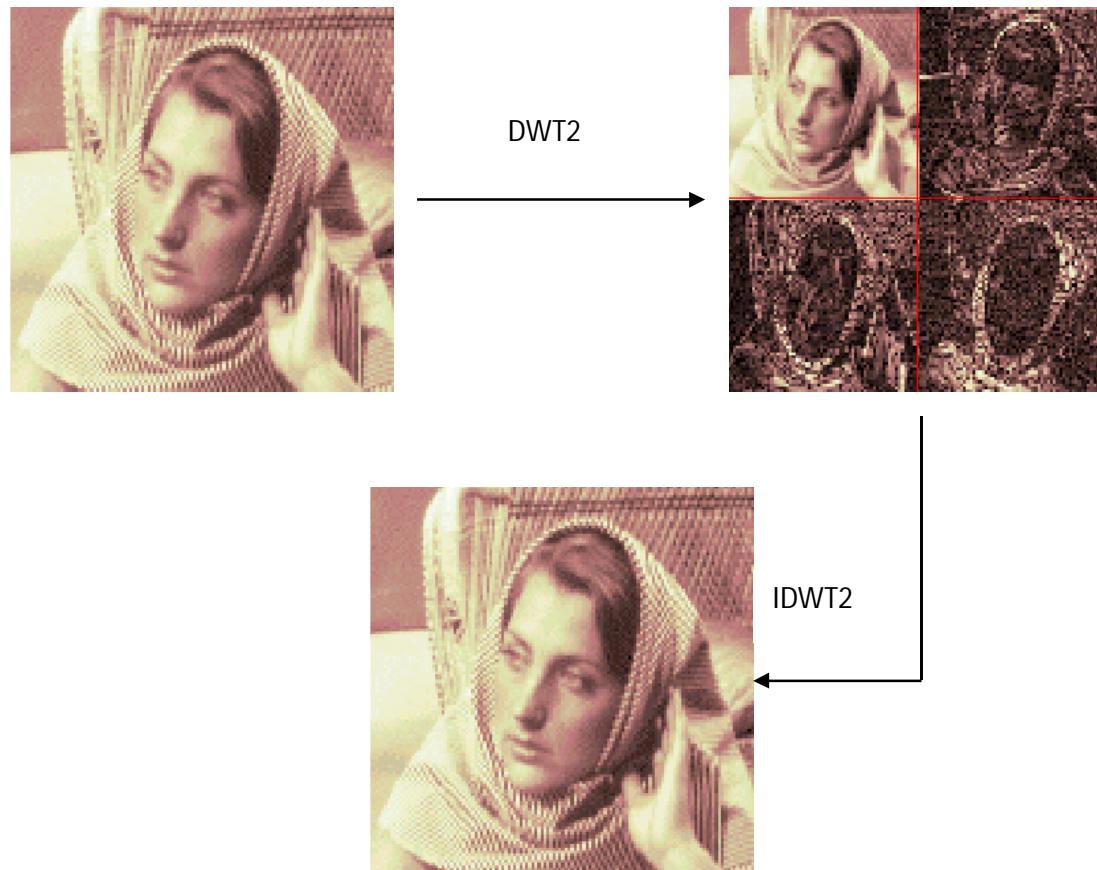


Fig. 5. Watermarked version of Bavarian couple.

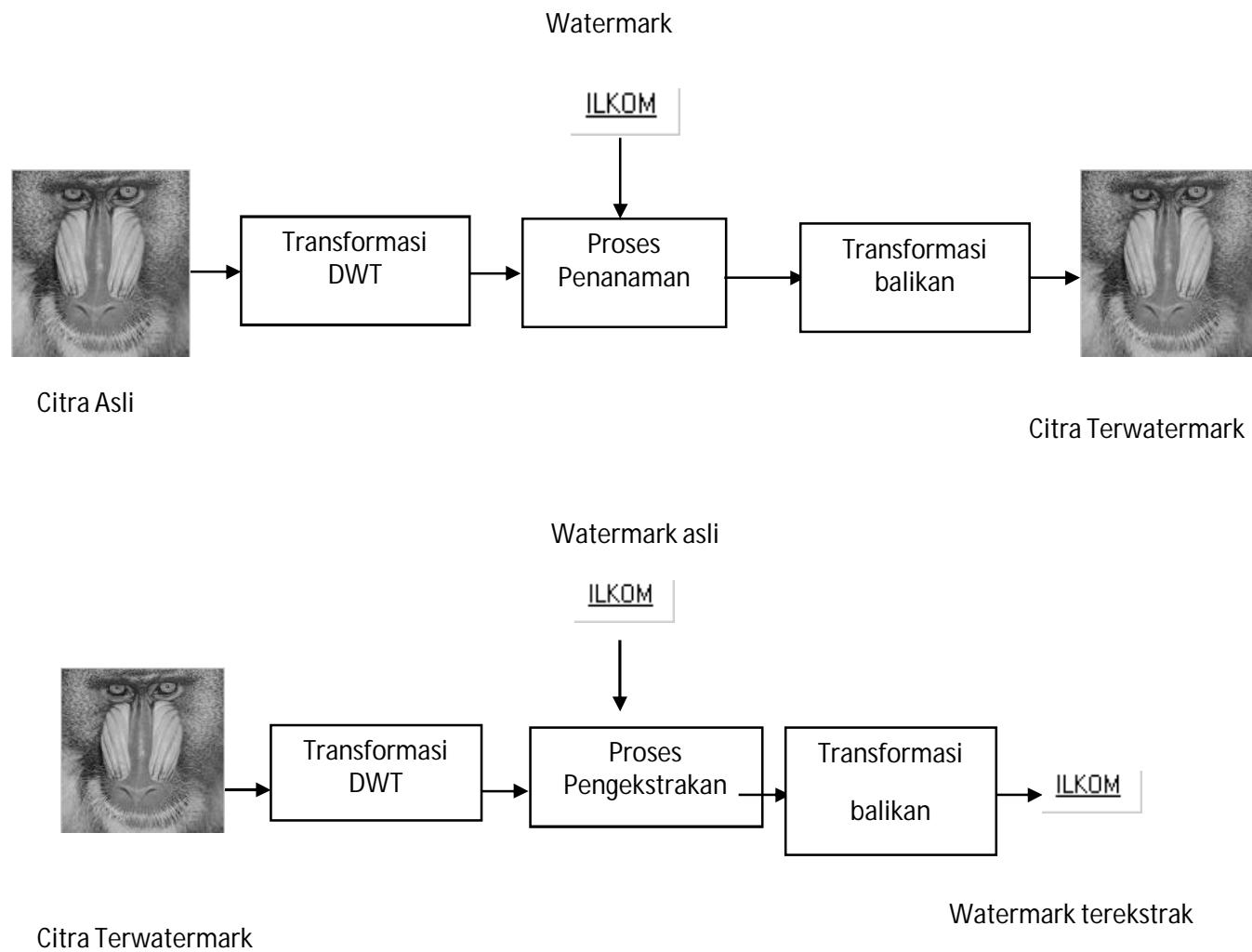
- Panjang *watermark* =  $n = 1000$
- Cox menggunakan 1000 koefisien terbesar. Inilah yang dinamakan *frequency spreading*.
- Cox memilih  $\alpha = 0.1$  dan  $T = 6$
- Kelemahan: perlu citra asli untuk deteksi *watermark* (*non-blind watermarking*).
- Kelebihan: kokoh terhadap
  - konversi analog-ke-digital
  - Konversi digital-ke-analog
  - *Cropping*
  - Kompresi, rotasi, translasi, dan penskalaan

# Domain Wavelet

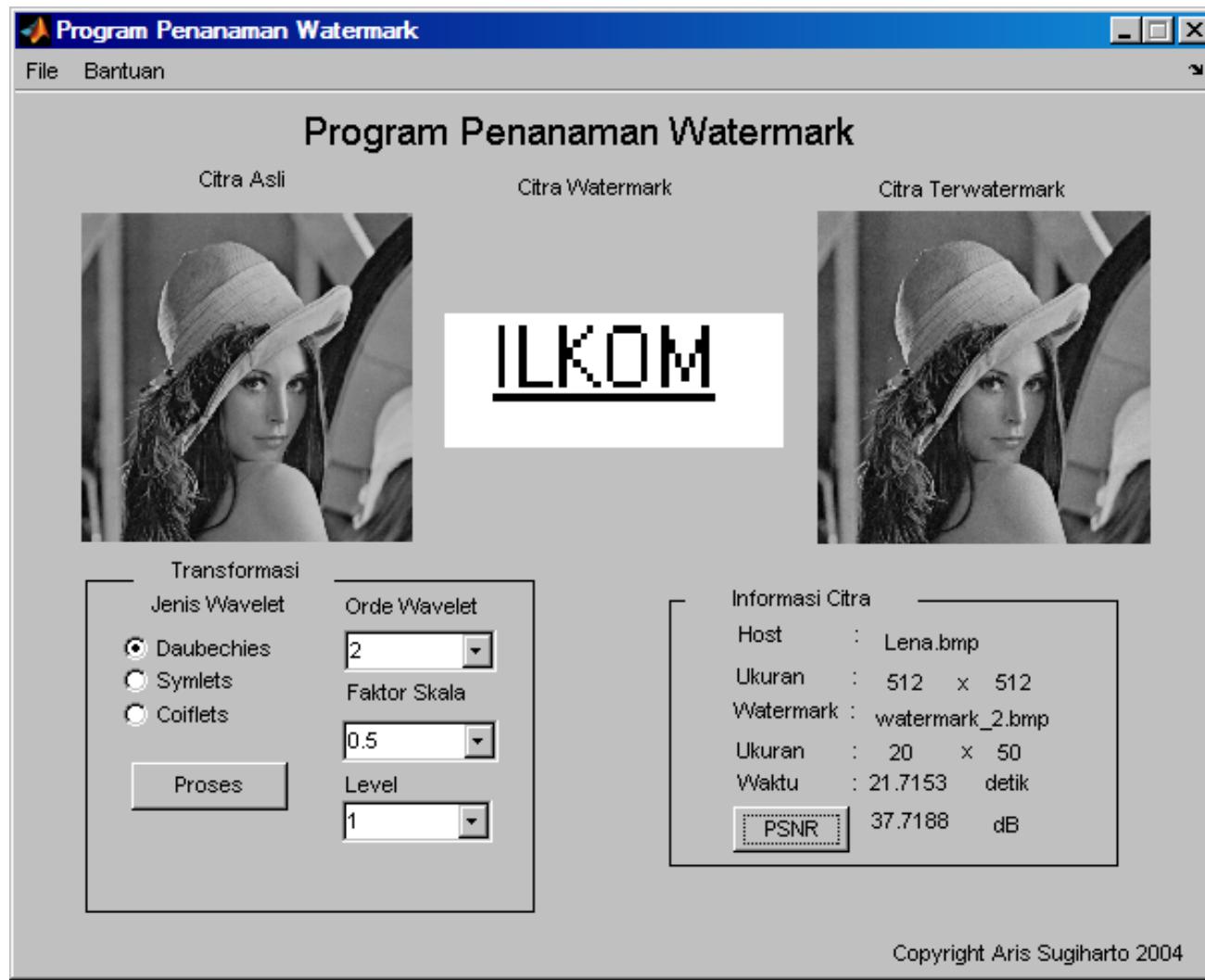
- Merubah Citra menjadi koefisien wavelet



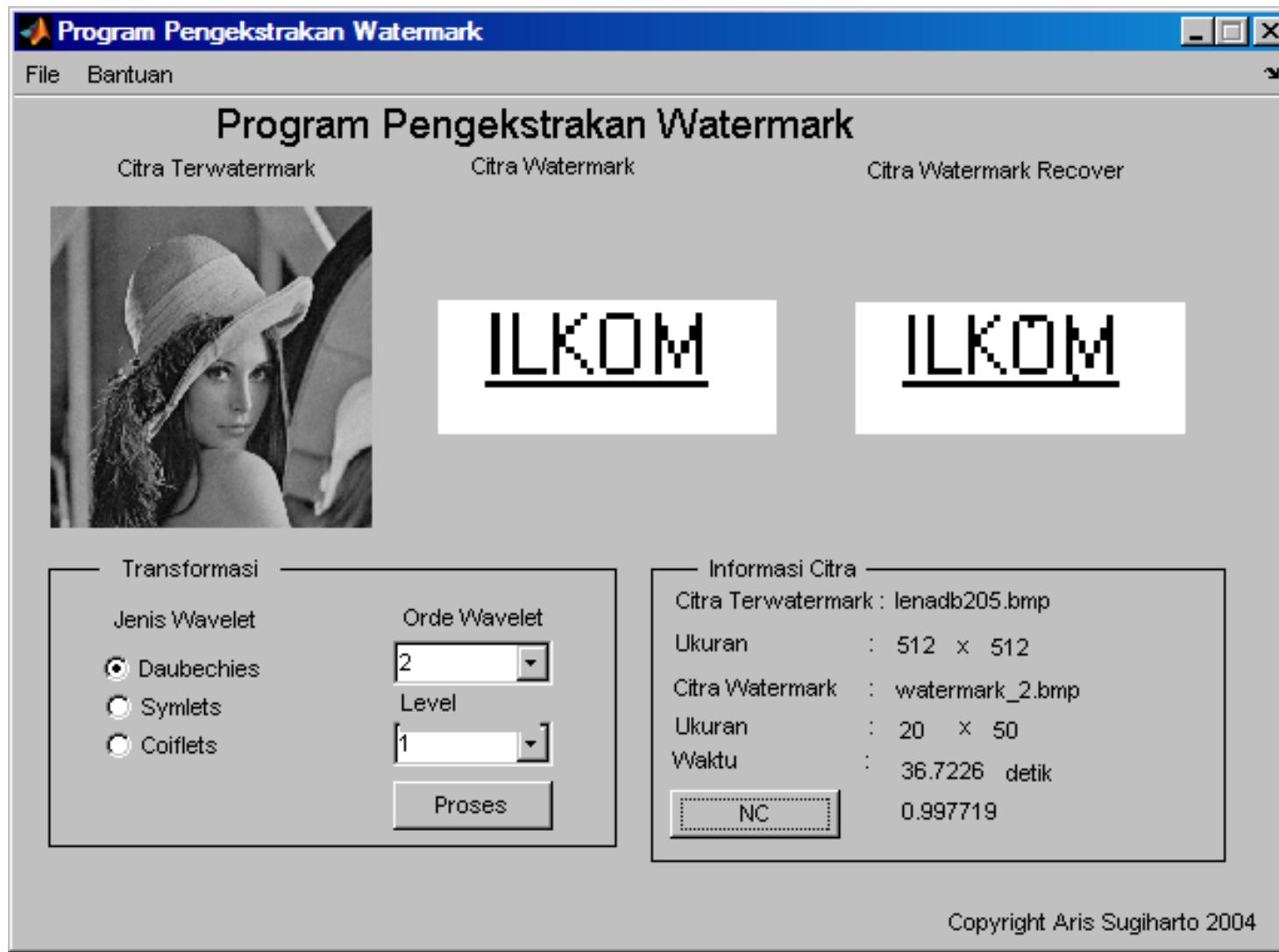
# Operasi Penanaman dan Pengekstrakan



# Interface Penanaman watermark



# Interface Pengekstrakan watermark



# Serangan (attack)

- Serangan Pasif
- Serangan Aktif