IF4020 Kriptografi

09 – Digital Watermarking

Oleh: Rinaldi Munir

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
InstitutTeknologi Bandung
2023

Prolog

”Sebuah gambar bermakna lebih dari seribu kata”

(*A picture is more than a thousand words*)

Termasuk gambar-gambar animasi ini

Fakta

- Jutaan gambar/citra digital bertebaran di internet via *email*, *website*, *bluetooth*, dsb

- Siapapun bisa mengunduh citra dari internet, meng-*copy*-nya, menyunting, mengirim, memanipulasi, dsb.

- Memungkinkan terjadi pelanggaran HAKI:

  - mengklaim citra orang lain sebagai milik sendiri (pelanggaran kepemilikan)

  - meng-*copy* dan menyebarkan citra tanpa izin pemilik (pelanggaran *copyright*)

  - mengubah konten citra sehingga keasliannya hilang

Kasus 1: Alice dan Bob sama-sama mengklaim gambar ini miliknya

Siapa pemilik gambar ini sesungguhnya? Hakim perlu memutuskan!

Kasus 2: Alice memiliki sebuah gambar UFO hasil jepretannya. Bob menggandakan dan menyebarkannya tanpa izin dari Alice

Kasus 3: Alice memiliki sebuah gambar hasil fotografi. Bob memodifikasi gambar tersebut dengan menggunakan Photoshop

Mana gambar yang asli?

Original

Hasil pengubahan

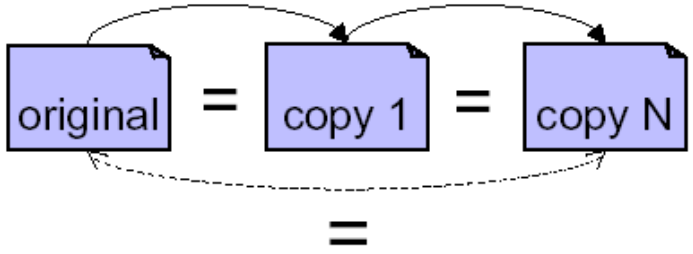
(a) Clinton and Monica

Foto mana yang asli?

(b) Clinton and Hillary

Semua kasus-kasus di atas karena karakteristik (kelebihan sekaligus kelemahan) gambar digital adalah:

- Tepat sama kalau digandakan



- Mudah didistribusikan (misal: via internet)

- Mudah di-edit (diubah) dengan *software*

Tidak ada perlindungan terhadap citra digital!!!!

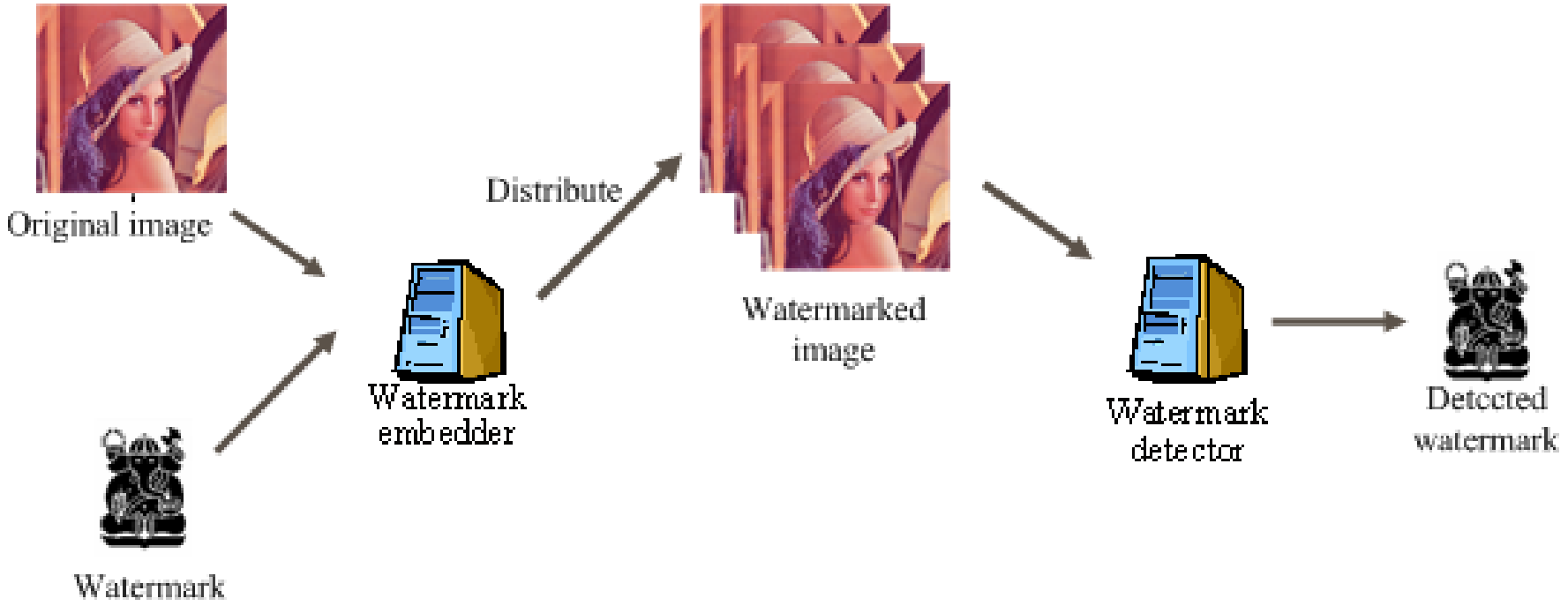
Solusi untuk masalah perlindungan citra di atas adalah:

Image Watermarking!!!!!!

Image Watermarking

- *Image Watermarking*: teknik menyisipkan informasi yang mengacu pada pemilik gambar (disebut *watermark*) untuk tujuan melindungi kepemilikan, *copyright* atau menjaga keaslian konten
- *Watermark*: teks, gambar logo, audio, data biner (+1/-1), barisan bilangan riil
- Penyisipan *watermark* ke dalam citra sedemikian sehingga tidak merusak kualitas citra.

Model Image Watermarking



- *Watermark* melekat di dalam citra
- Penyisipan *watermark* tidak merusak kualitas citra
- *Watermark* dapat dideteksi/ekstraksi kembali sebagai bukti kepemilikan/*copyright* atau bukti adanya modifikasi

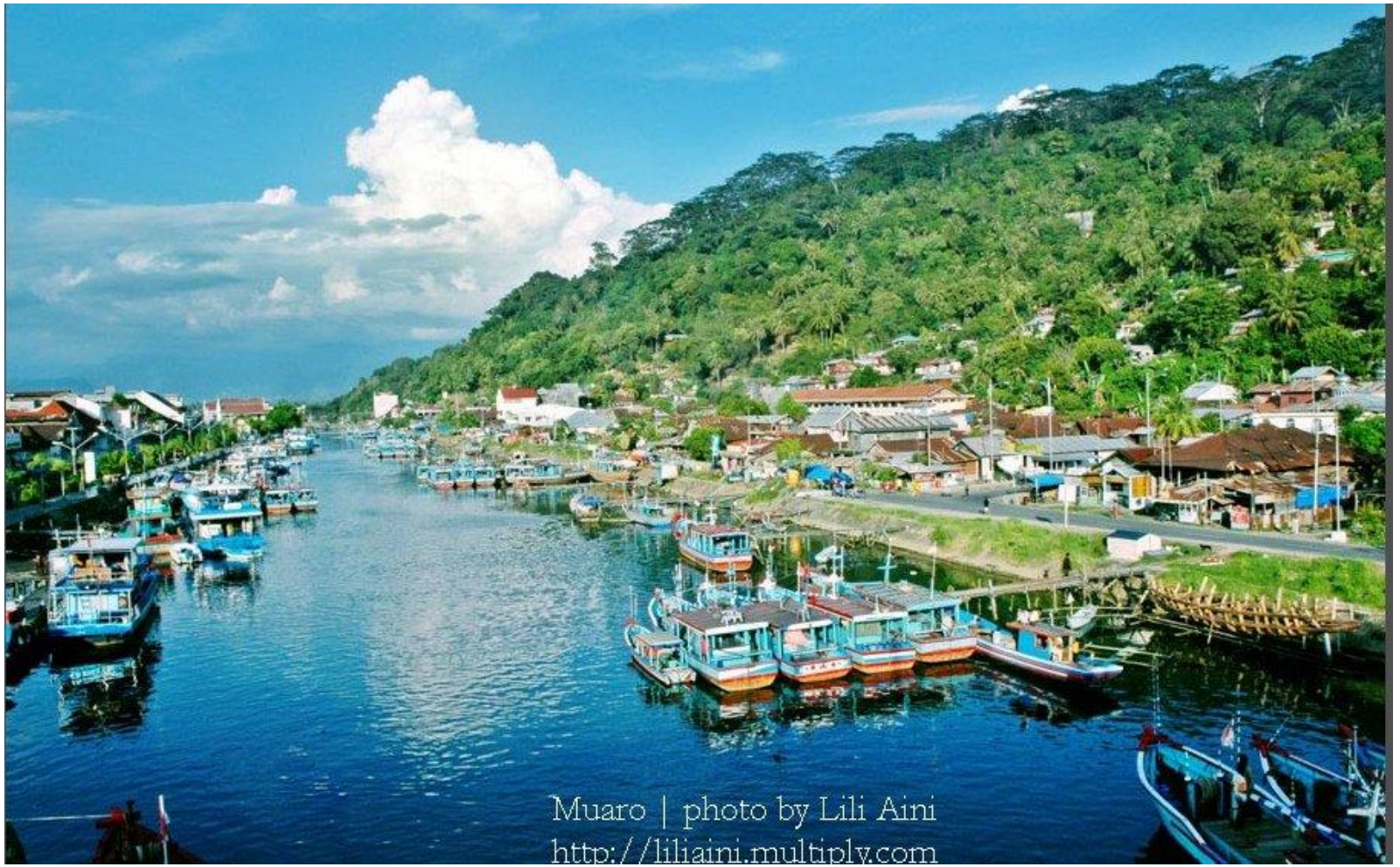
Cara-cara Konvensional Memberi Label *Copyright*

- Label *copyright* ditempelkan pada gambar.

- Kelemahan: tidak efektif melindungi *copyright* sebab label bisa dipotong atau dibuang dengan program pengolahan citra komersil (ex: *Adobe Photoshop*).

Original image + label *copyright*

Cropped image



Label kepemilikan

Dengan teknik *watermarking*…

- *Watermark* disisipkan ke dalam citra digital.
- *Watermark* terintegrasi di dalam citra digital
- Kelebihan:
  1. Penyisipan *watermark* tidak merusak kualitas citra, citra yang diberi *watermark* terlihat seperti aslinya.
  2. Setiap penggandaan (*copy*) citra digital akan membawa *watermark* di dalam salinannya.
  3. *Watermark* tidak bisa dihapus atau dibuang
  4. *Watermark* dapat dideteksi/ekstraksi kembali sebagai bukti kepemilikan /*copyright* atau deteksi perubahan

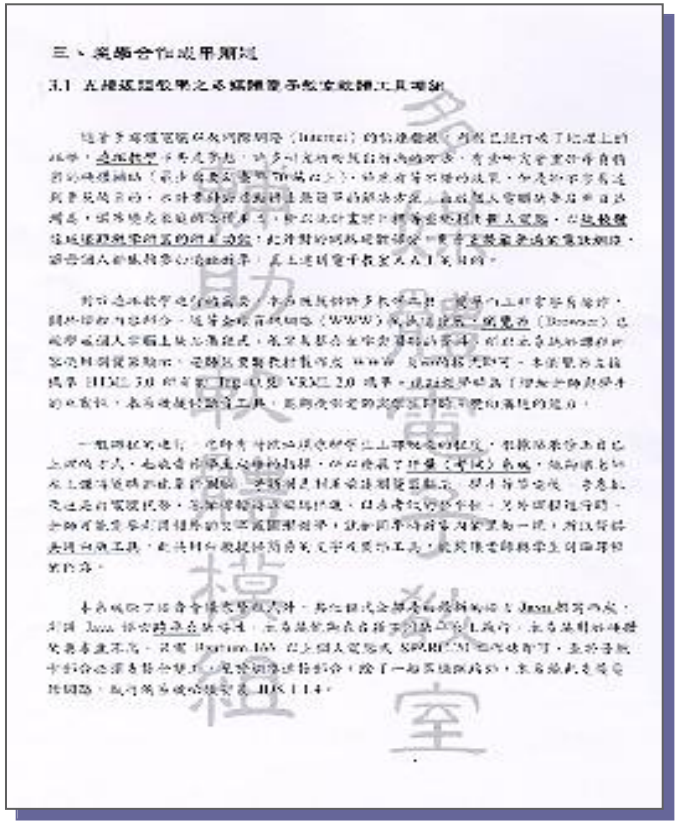
Sejarah *Watermarking*

- 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 dibubuhi tanda-air dijadikan identifikasi bahwa karya seni di atasnya adalah asli.

- Bangsa Cina melakukan hal yang sama pada pencetakan kertas



Klasifikasi *Watermarking*

1. *Paper watermarking*

Teknik memberikan impresi pada kertas berupa gambar/logo atau teks.

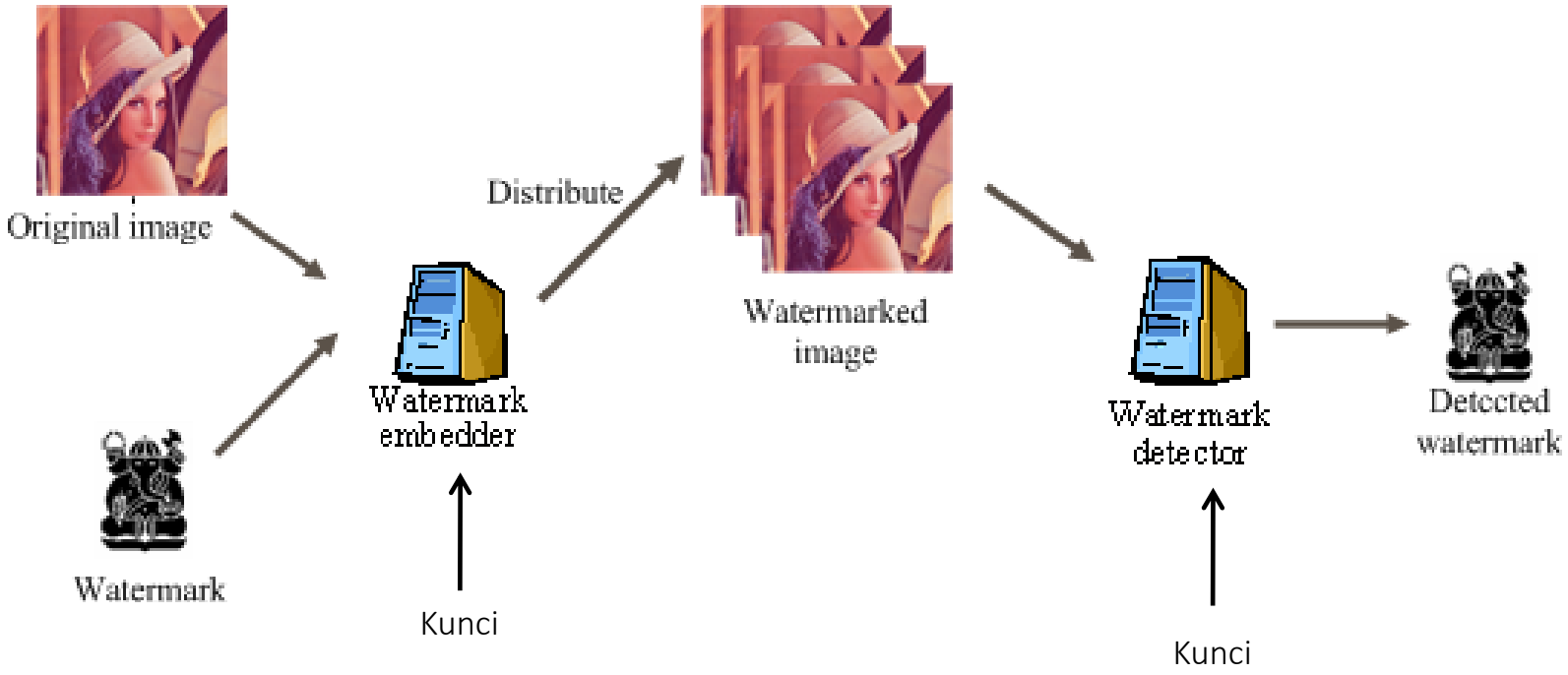
"Cannot be photocopied or scanned effectively"

Tujuan: Identifikasi keaslian (otentikasi)

Digunakan pada: uang, paspor, banknotes ,

2. *Digital Watermarking*

Menyisipkan sinyal digital ke dalam dokumen digital (gambar, audio, video, teks)



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*), keaslian/autentikasi
- Persyaratan: sulit dihapus (*remove*)
- Komunikasi: *one-to-many*
- Komentar lain: media penampung justru yang diberi proteksi, tidak mementingkan kapasitas *watermark*

Selain citra, data apa saja yang bisa diberi *watermark*?

- Citra → *Image Watermarking*
- Video → *Video Watermarking*
- Audio → *Audio Watermarking*
- Teks → *Text Watermarking*
- Perangkat lunak → *Software watermarking*

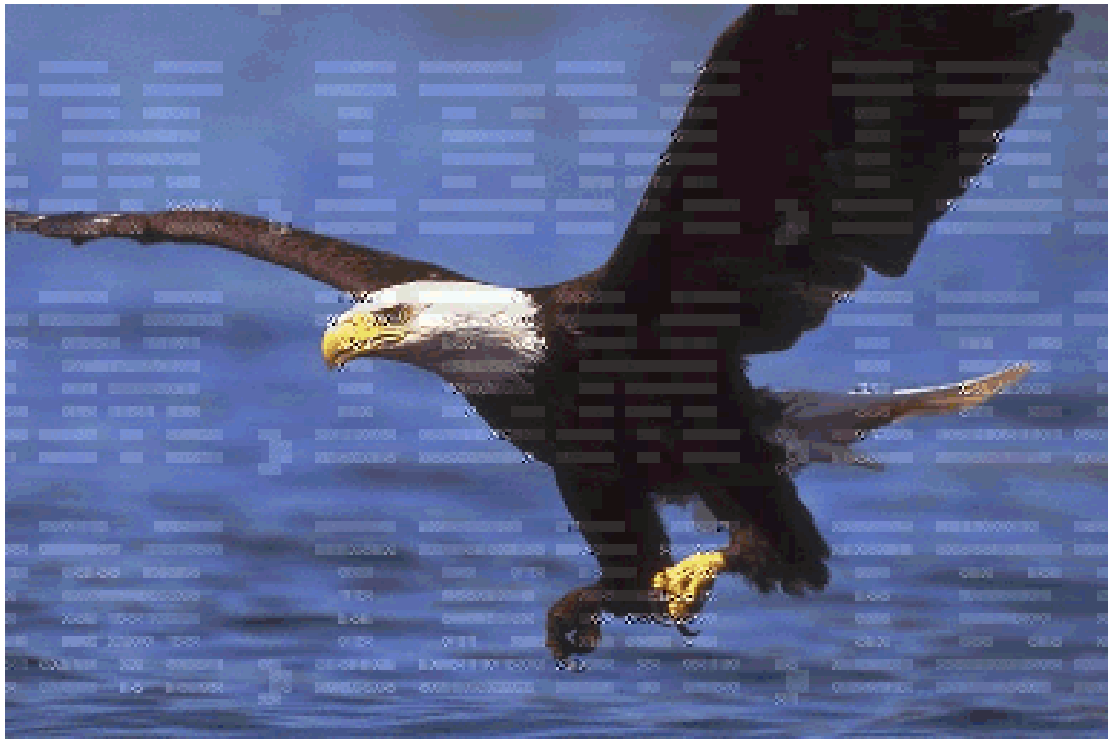
Image Watermarking

- Penyisipan *watermark* ke dalam citra menghasilkan citra ber-*watermark* (*watermarked image*)

- Terbagi menjadi 2 jenis: *visible watermarking* dan *invisible watermarking*

Invisible Watermark

Visible Watermark



Visible watermarking

Invisible watermarking

Klasifikasi (invisible) *Image Watermarking*

- ***Fragile watermarking***

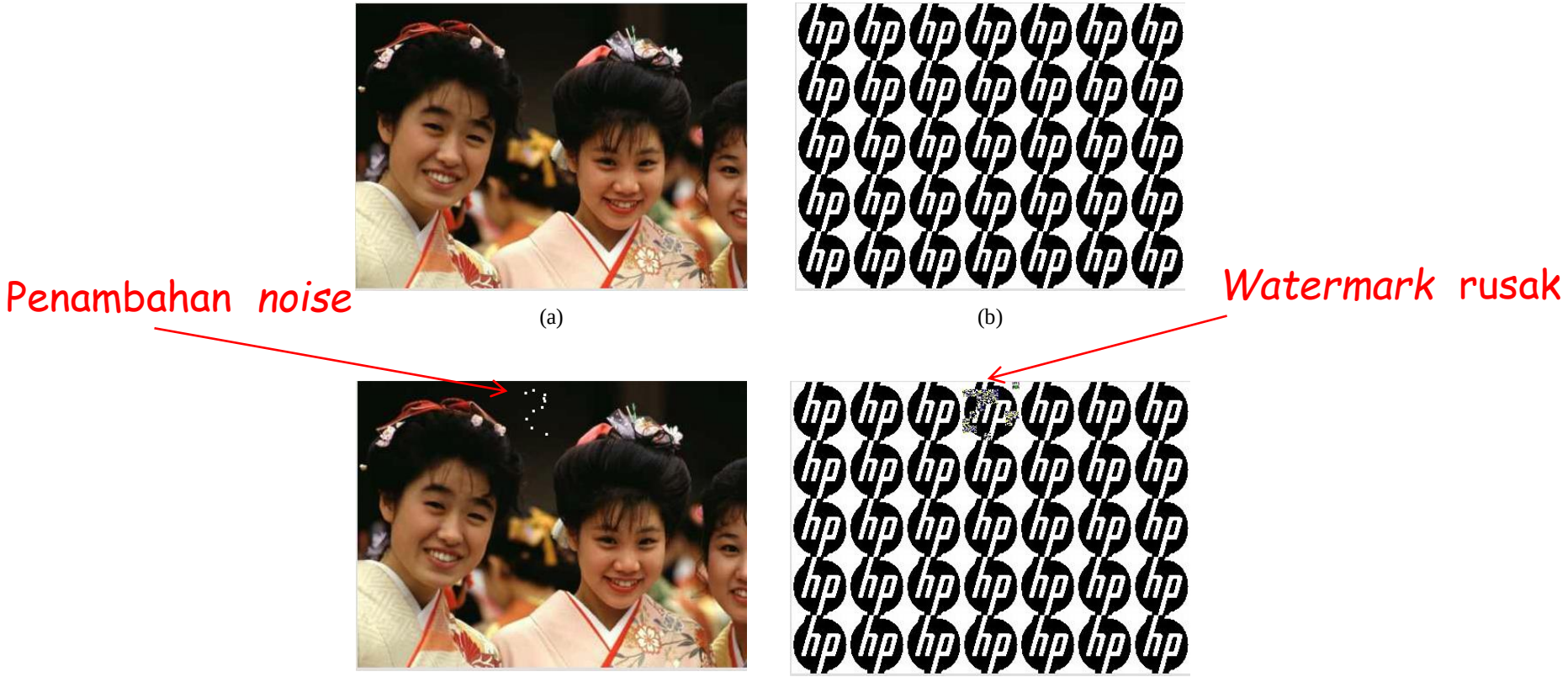
  Tujuan: untuk menjaga integritas/orisinilitas citra digital.

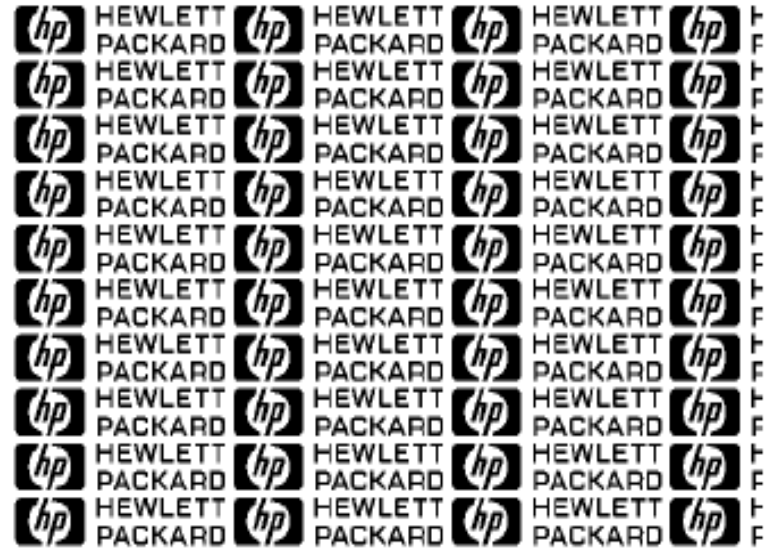
- ***Robust watermarking***

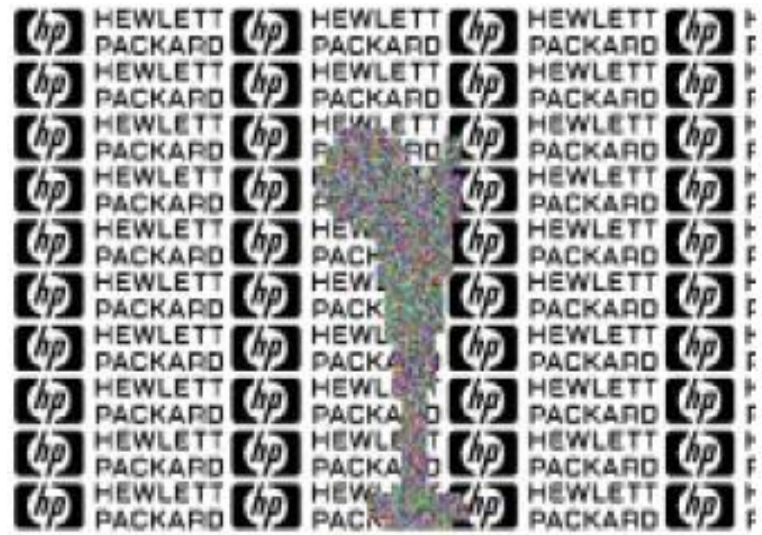
  Tujuan: untuk menyisipkan label kepemilikan/*copyright* citra digital.

Fragile Watermarking

- *Watermark* menjadi rusak atau pecah jika dilakukan manipulasi (*common imageprocessing*) pada citra ber-*watermark*.
- Tujuan: pembuktian keaslian dan *tamper proofing*







Contoh *fragile watermarking* lainnya (Wong, 1997)

Bagaimana caranya?

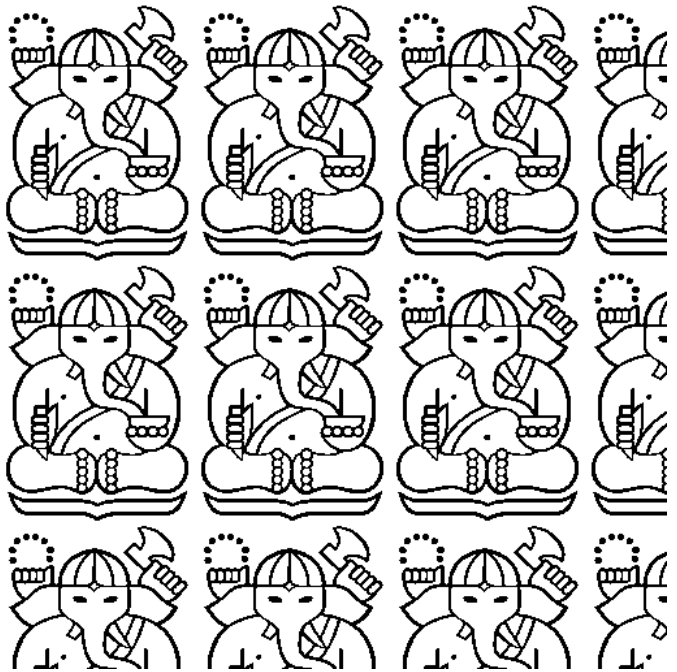
- Pertama, harus mengerti dulu konsep citra digital (sudah dijelaskan di dalam materi Steganografi)

- Kedua, mengerti metode LSB (sudah dijelaskan di dalam materi Steganografi)

Algoritma *Fragile Watermarking*

1. Nyatakan *watermark* seukuran citra yang akan disisipi (lakukan *copy and paste*)

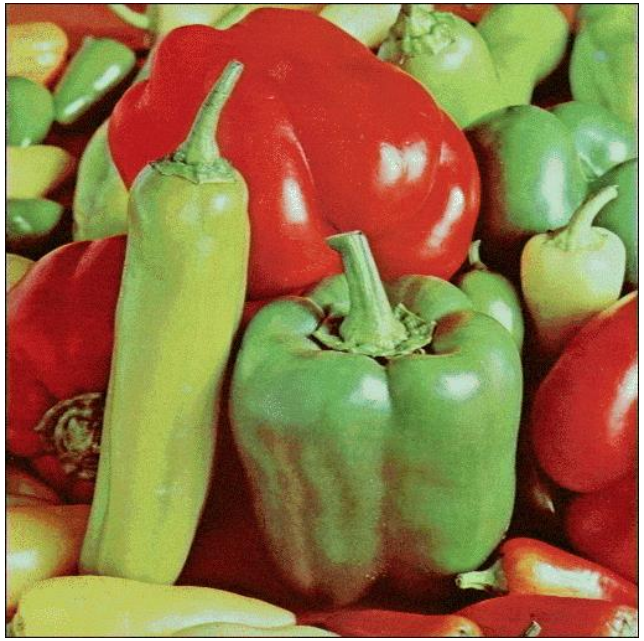
Citra asli



watermark

2. Sisipkan *watermark* pada seluruh *pixel* citra dengan metode LSB

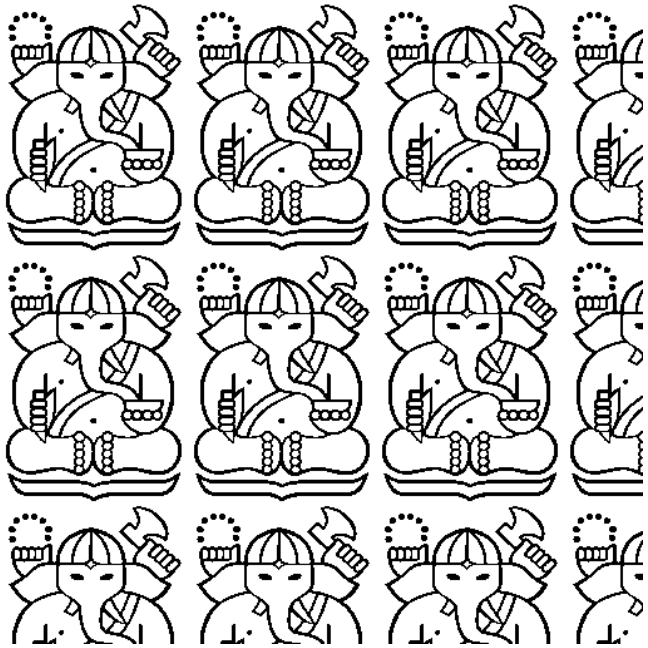
Citra asli



Citra ber-watermark

3. Ekstraksi *watermark* dengan mengambil bit-bit LSB pada setiap *pixel*, lalu satukan menjadi gambar *watermark* semula

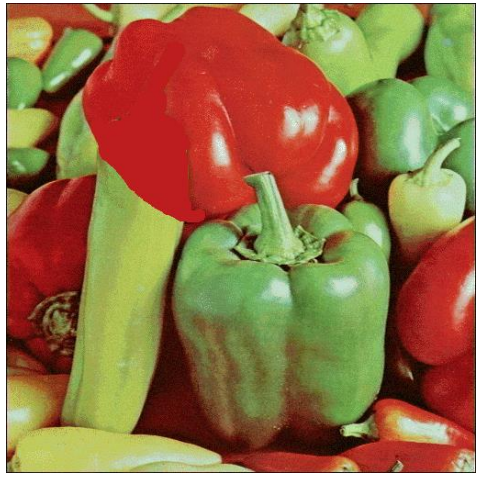
Citra ber-watermark

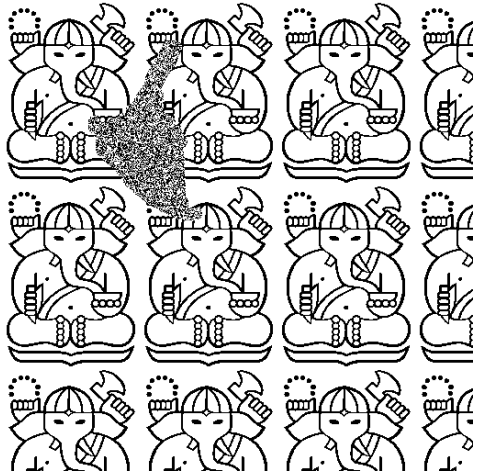


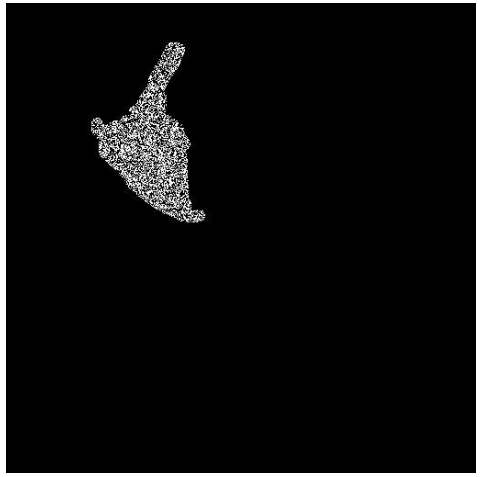
Watermark hasil ekstraksi

Test manipulasi pada citra ber-*watermark*

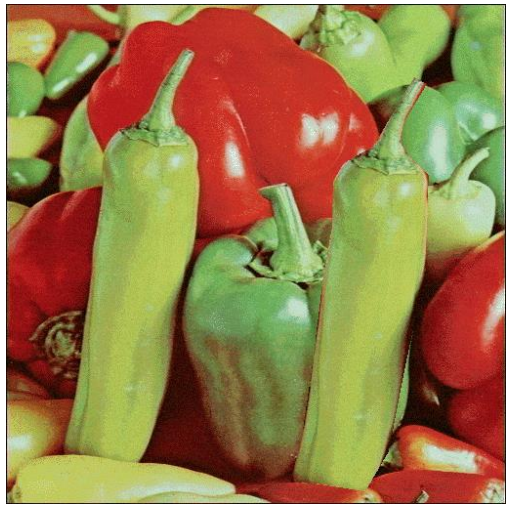
Deletion attack

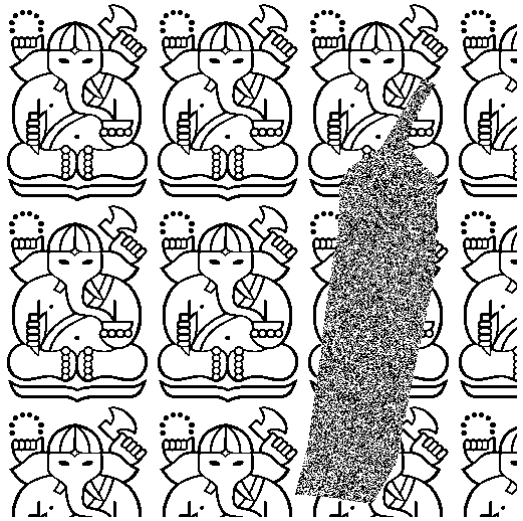


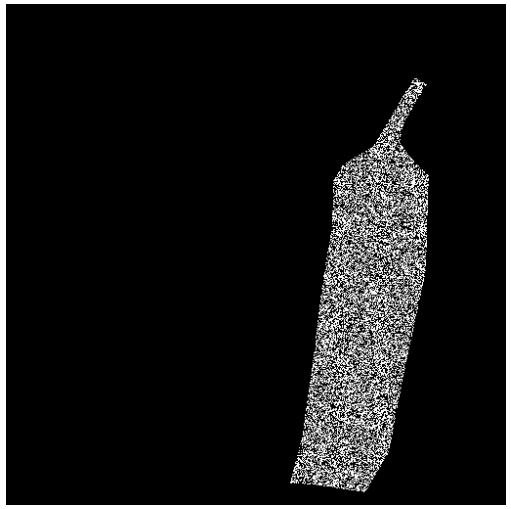


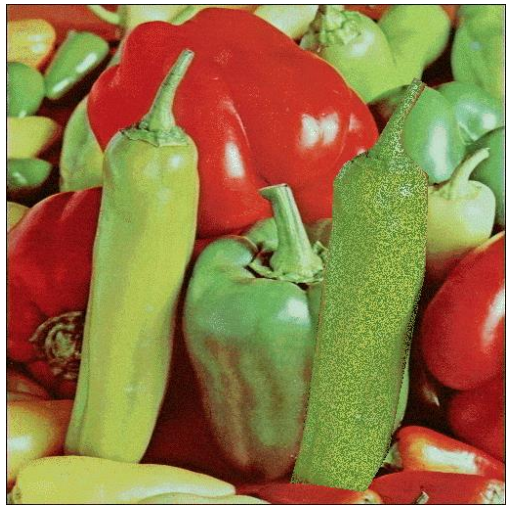


Insertion attack

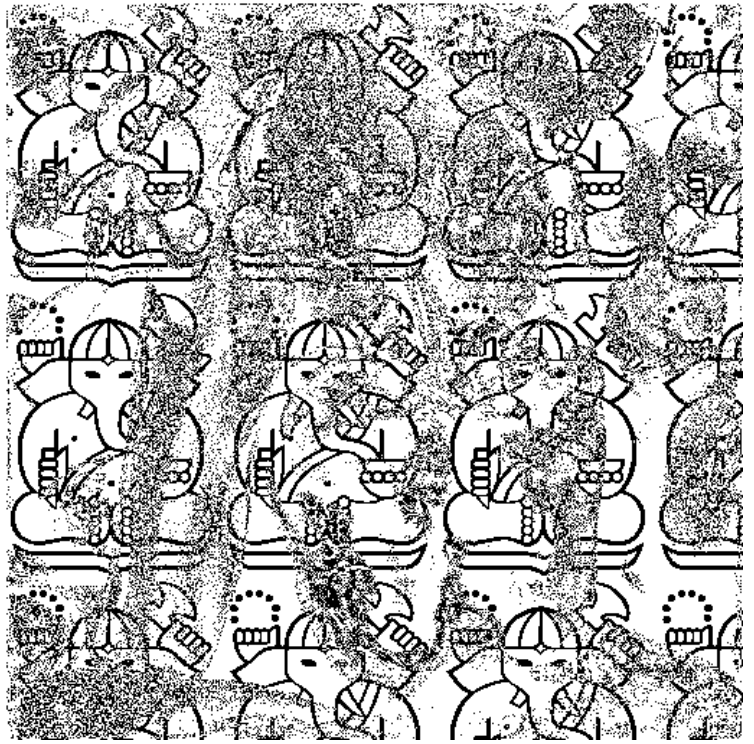








Brightness and contrast attack



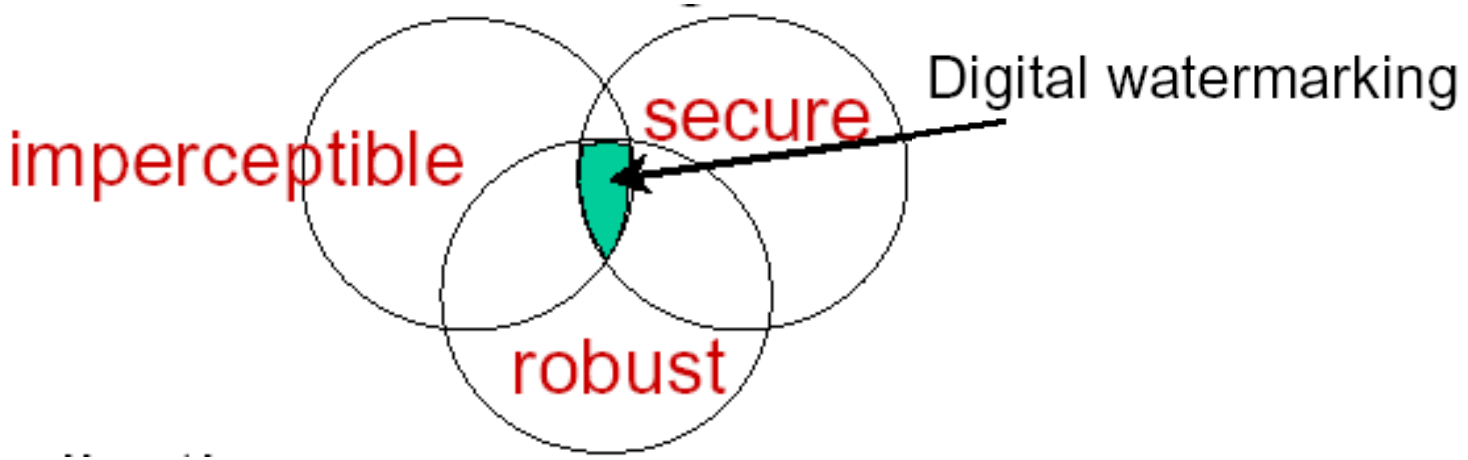
Robust Watermarking

- *Watermark* tetap kokoh (*robust*) terhadap manipulasi (*common digital processing*) yang dilakukan pada citra ber-watermark.

  Contoh manipulasi: kompresi, *cropping*, *editing*, *resizing, dll*

- Tujuan: perlindungan hak kepemilikan dan *copyright*

- Persyaratan umum *robust watermarking* :
  - *imperceptible*
  - *robustness*
  - *secure*



Original image

Watermarked image

watermark

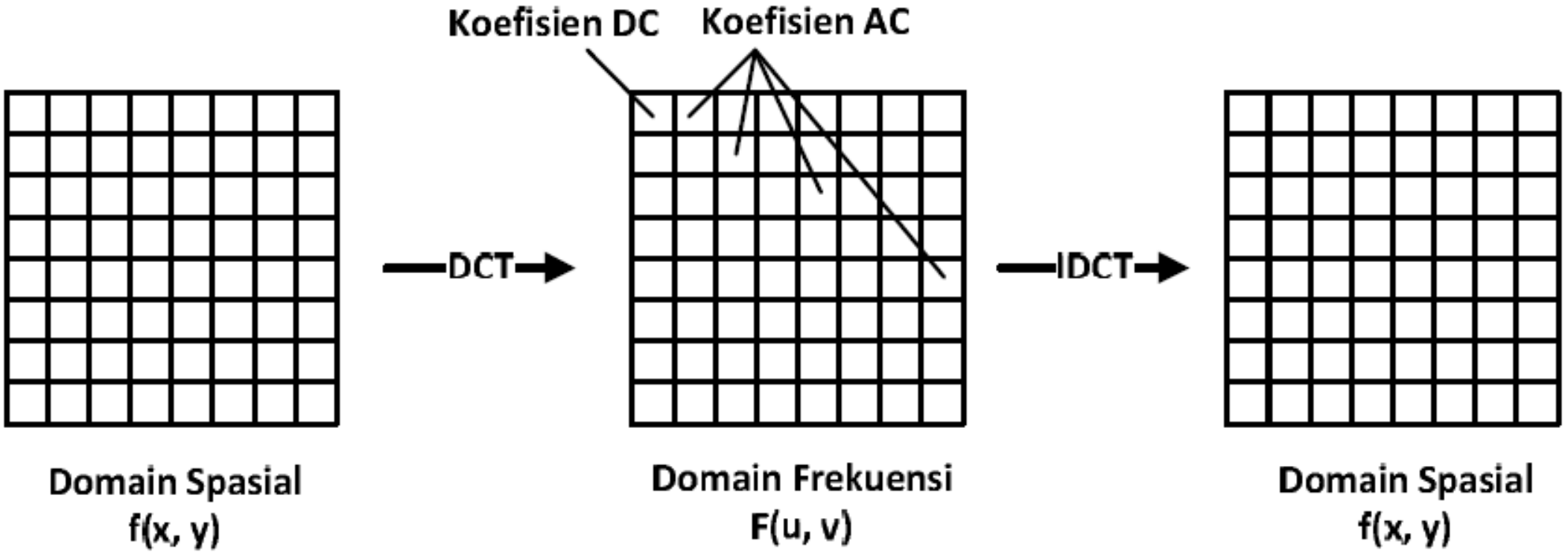
extracted watermark

Bagaimana caranya?

- Tidak seperti metode *fragile watermarking* yang mana *watermark* disisipkan pada domain spasial (*pixel-pixel* citra),
- maka pada metode *robust watermarking*, *watermark* disisipkan pada domain transform, misalnya domain frekuensi.

- Hal ini bertujuan agar *watermark* tahan terhadap manipulasi pada citra.

- Pertama-tama, citra ditransformasi dari ranah spasial ke ranah *transform* (frekuensi), misalnya menggunakan transformasi DCT (*Discrete Cosine Transform*)


Koefisien DC
Koefisien AC
DCT
IDCT
Domain Spasial
f(x, y)
Domain Frekuensi
F(u, v)
Domain Spasial
f(x, y)

- *Discrete Cosine Transform* (*DCT*)

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \qquad (1)$$

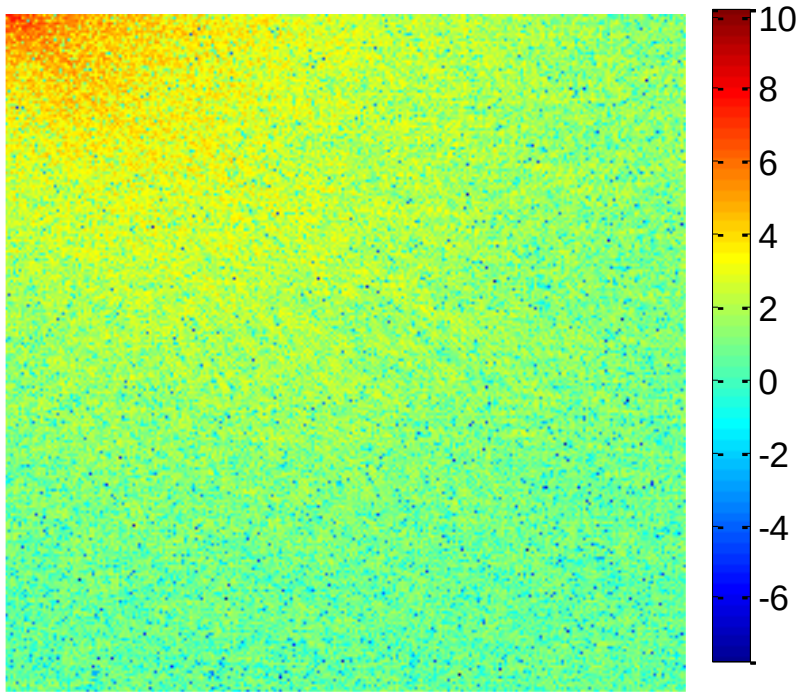
$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}} & ,u = 0 \\ \sqrt{\frac{2}{M}} & ,1 \le u \le M-1 \end{cases} \qquad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}} & ,v = 0 \\ \sqrt{\frac{2}{N}} & ,1 \le v \le N-1 \end{cases}$$

C(u,v) disebut koefisien-koefisien DCT

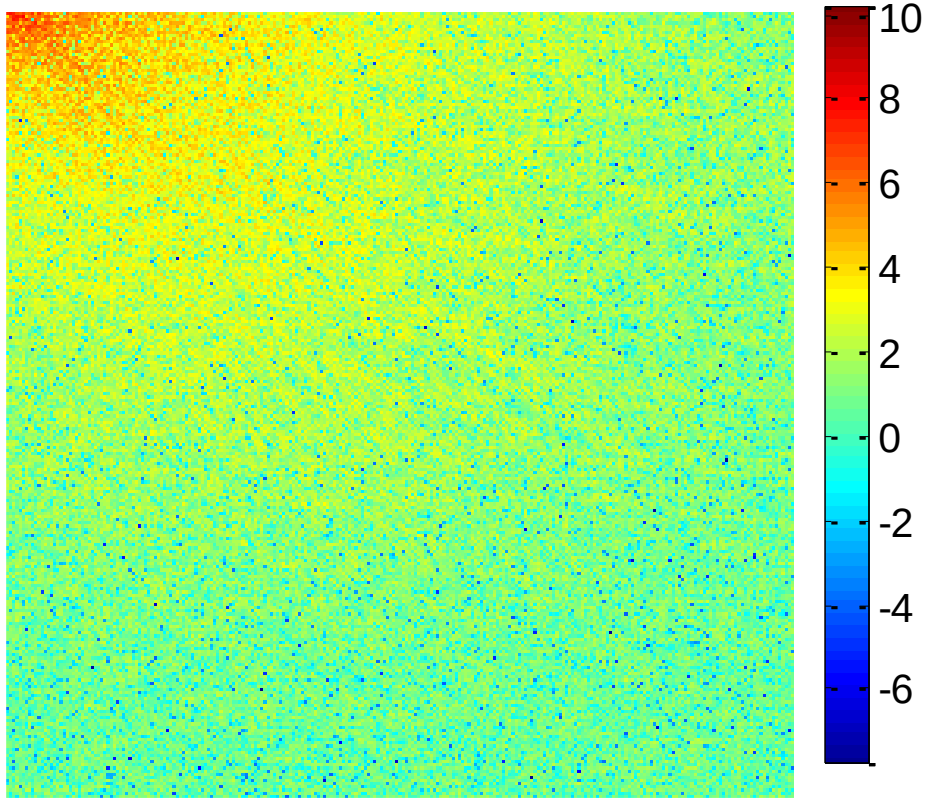
- *Inverse Discrete Cosine Transform* (*IDCT*)

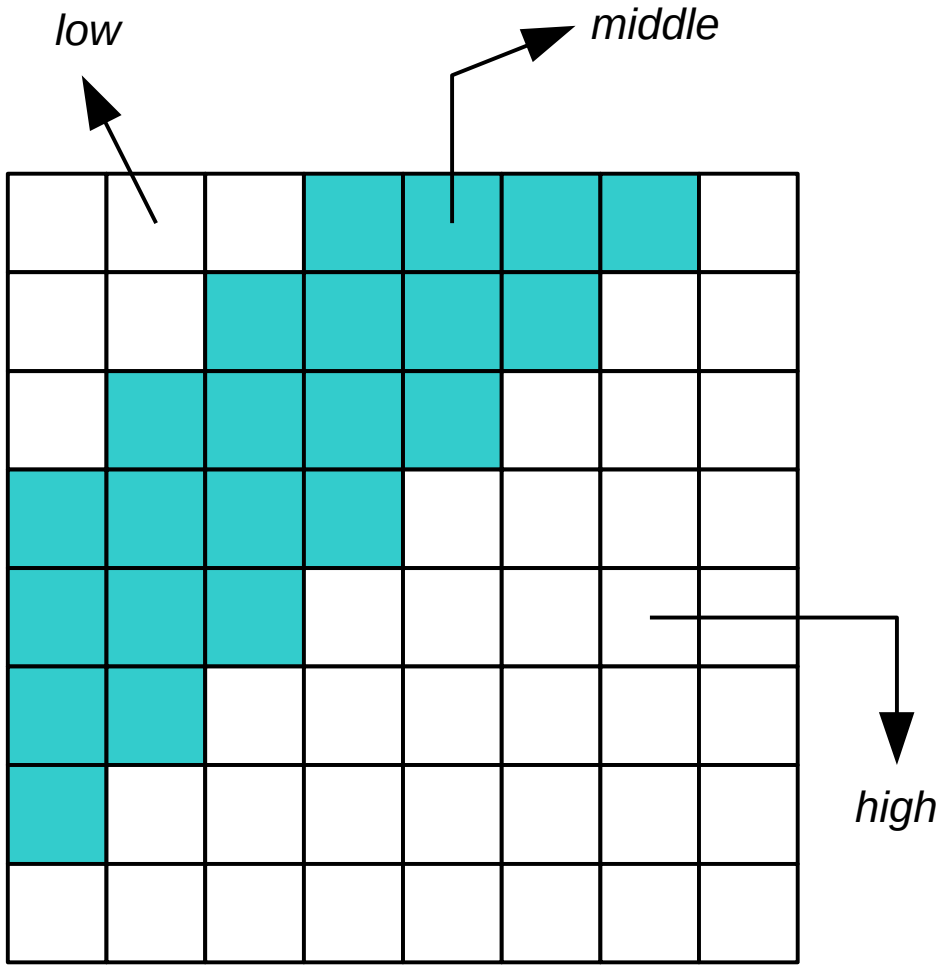
$$I(x,y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u,v) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \qquad (4)$$

Citra dalam ranah spasial



Citra dalam ranah frekuensi


10
8
6
4
2
0
-2
-4
-6


low
middle
high

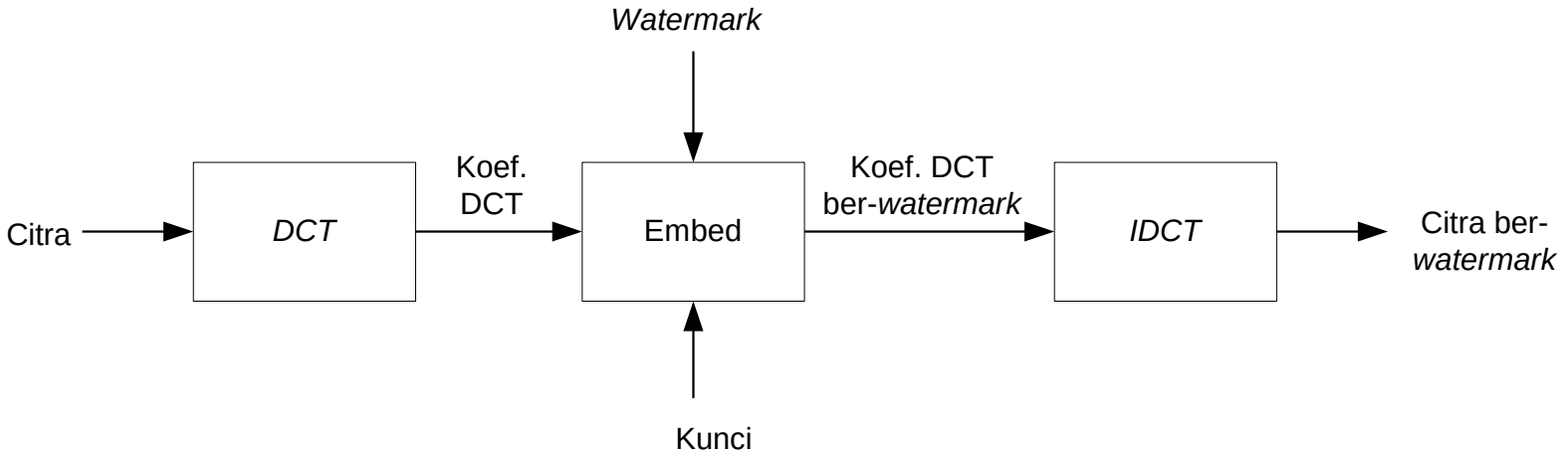
- Hasil tranformasi menghasilkan nilai-nilai yang disebut koefisien-koefisien transformasi (misalnya koefisien DCT).

- Bit-bit *watermark* (*w*) disembunyikan pada koefisien-koefisien tranformasi (*x*) tersebut dengan suatu formula, misalnya:

$$\hat{x}_i = x_i + \alpha w_i$$

α = kekuatan *robustness*

- Selanjutnya, citra ditransformasikan kembali (*inverse transformation*) ke ranah spasial untuk mendapatkan citra *ber-watermark*).



Wang Algorithm (1)

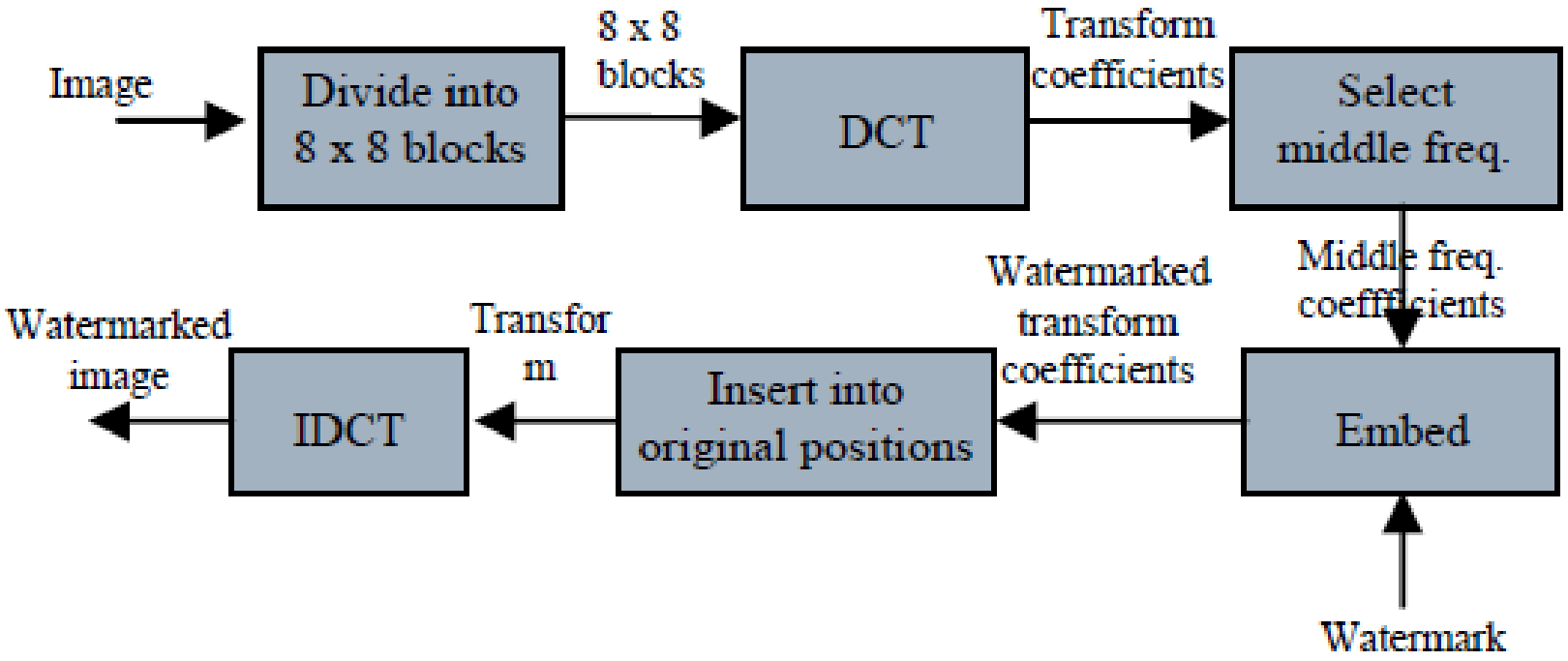


Fig. 1. Embedding process

J. Wang, et al, *A Novel Correlation Detection System for Multiplicative Robust Watermarking*, Proc. of *ISCCSP2006*, 2006.

Wang Algorithm (2)

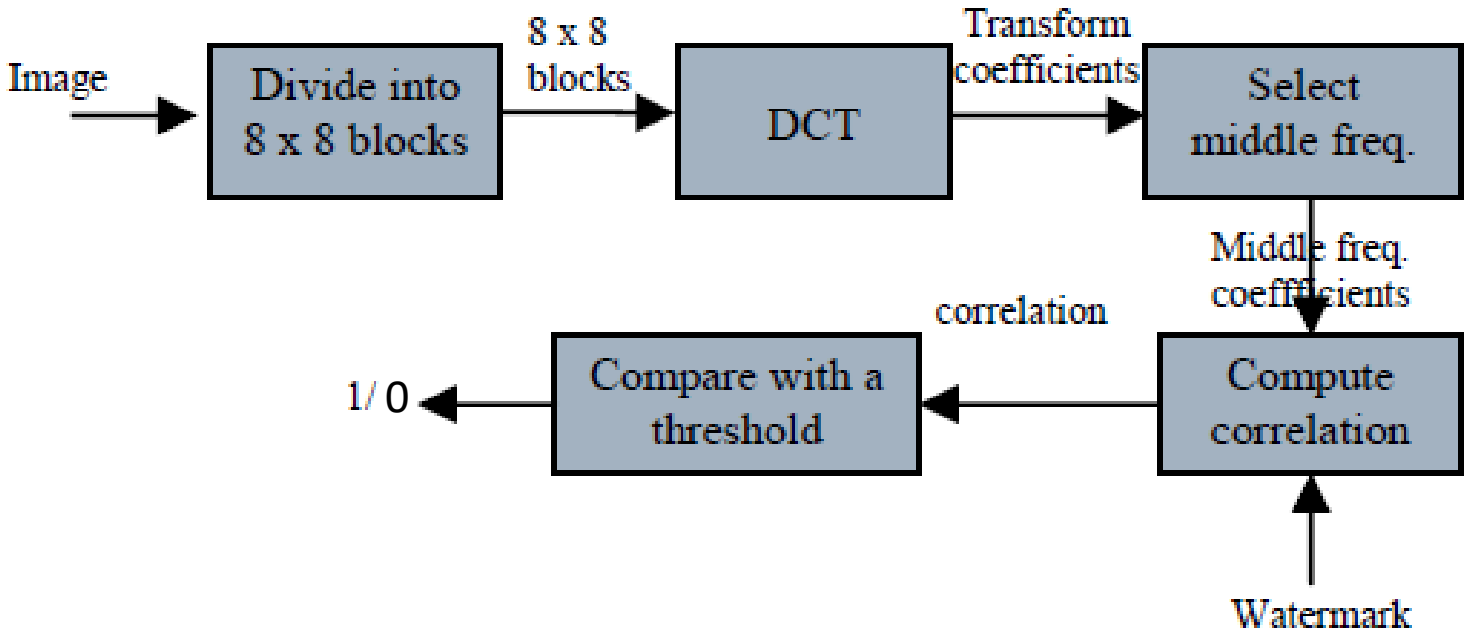


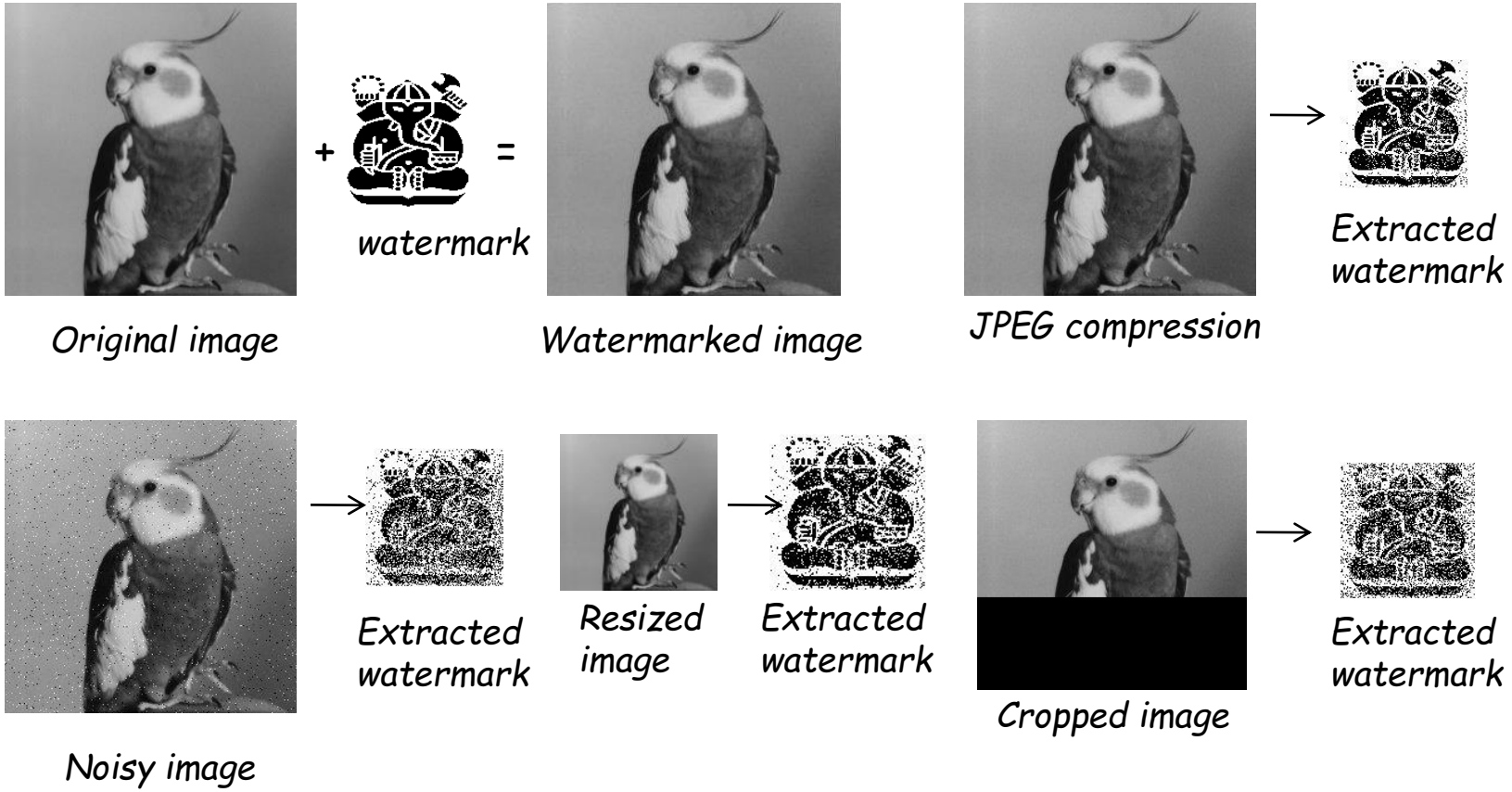
Fig. 2. Detection process

Correlation formula: $$c = \frac{1}{M}\sum_{i=i}^{M} x*(i)\cdot w(i)$$

Decision: $$\begin{cases} 1 & , c \geq T \\ 0 & , c < T \end{cases}$$

Test ketahanan *watermark* terhadap manipulasi terhadap citra.

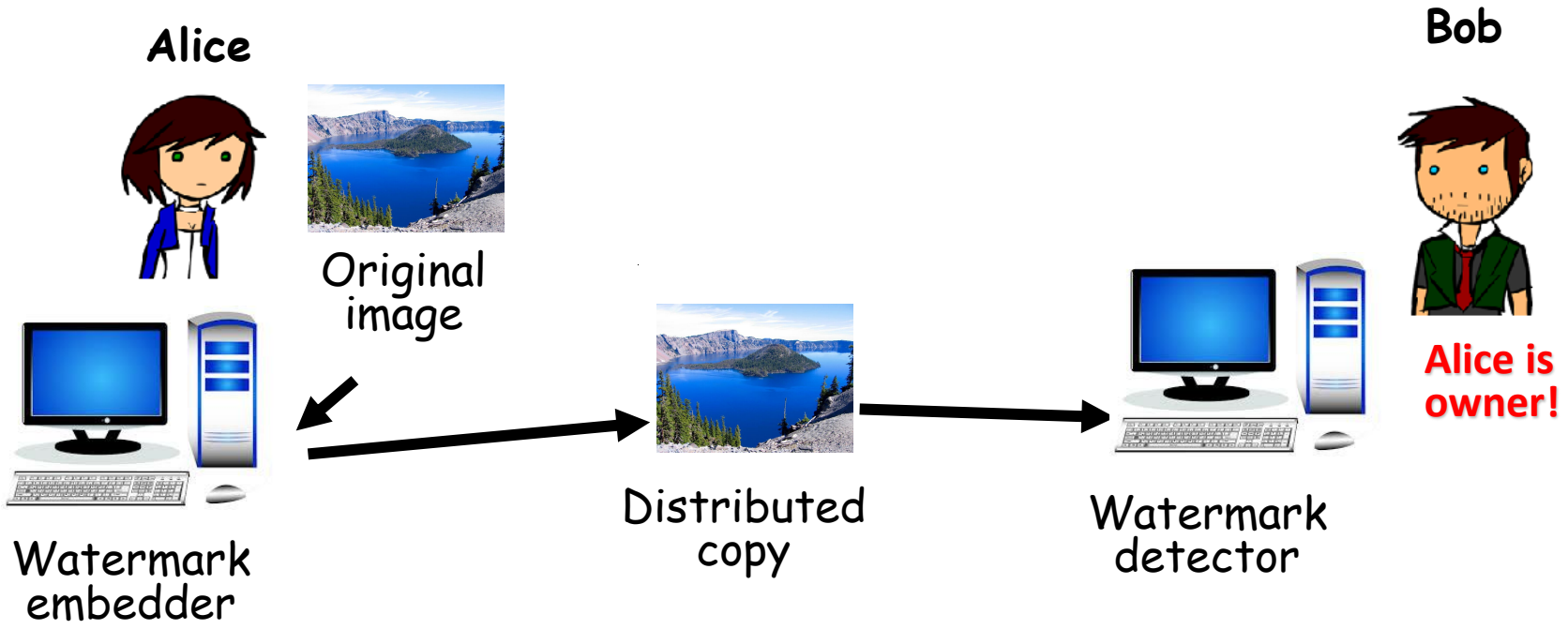
Contoh: kompresi, *cropping*, *editing*, *resizing, dll*



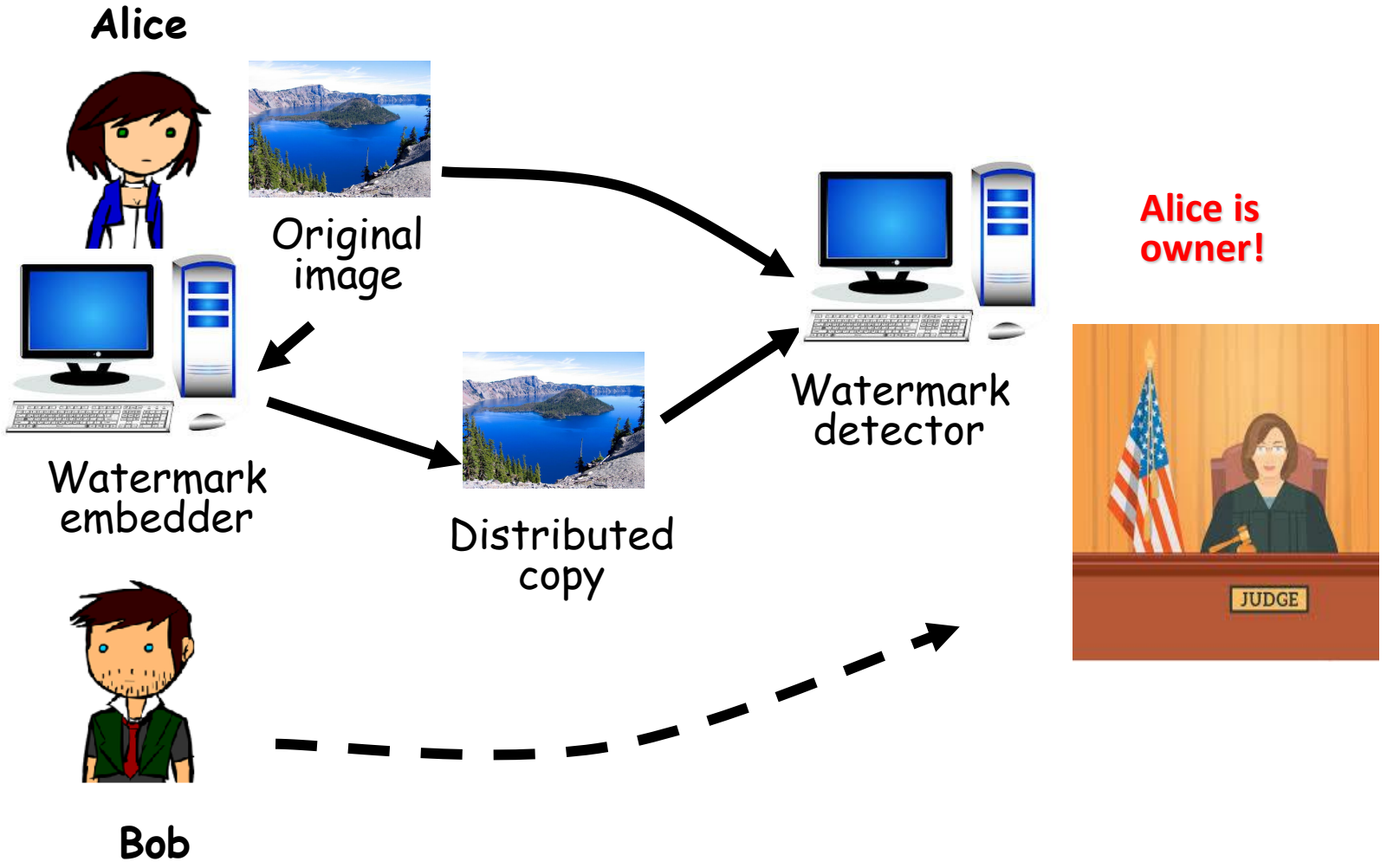
Aplikasi *Watermarking*

- Identifikasi kepemilikan (*ownership identification*)
- Bukti kepemilikan (*proof of ownership*)
- Memeriksa keaslian isi karya digital (*tamper proofing*) ➔ *Content authentication*
- *Transaction tracking*
- *Piracy protection/copy control*: mencegah penggandaan yang tidak berizin.
- *Broadcast monitoring*

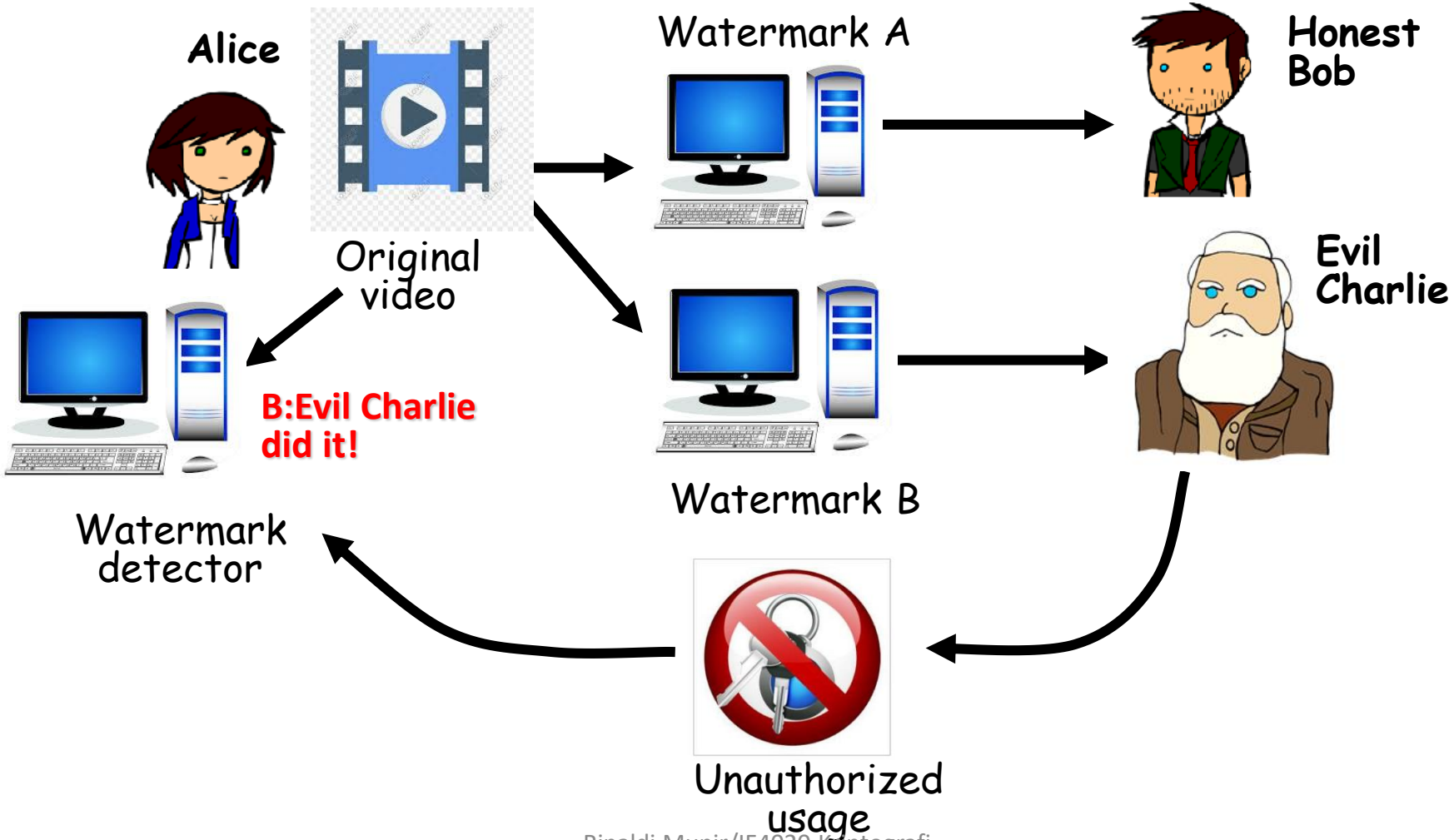
Aplikasi watermarking: *Owner identification*



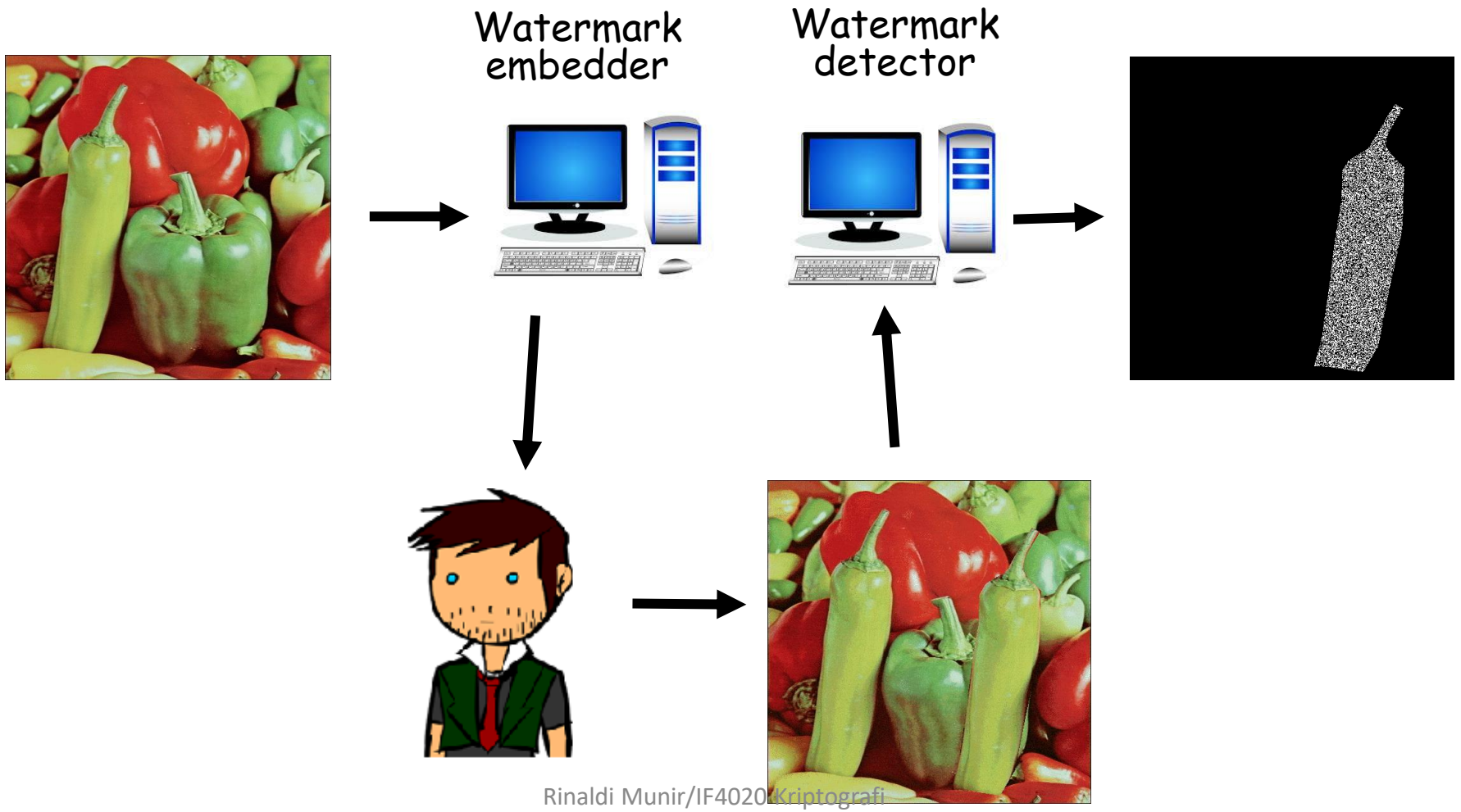
Aplikasi watermarking: *Proof of ownership*



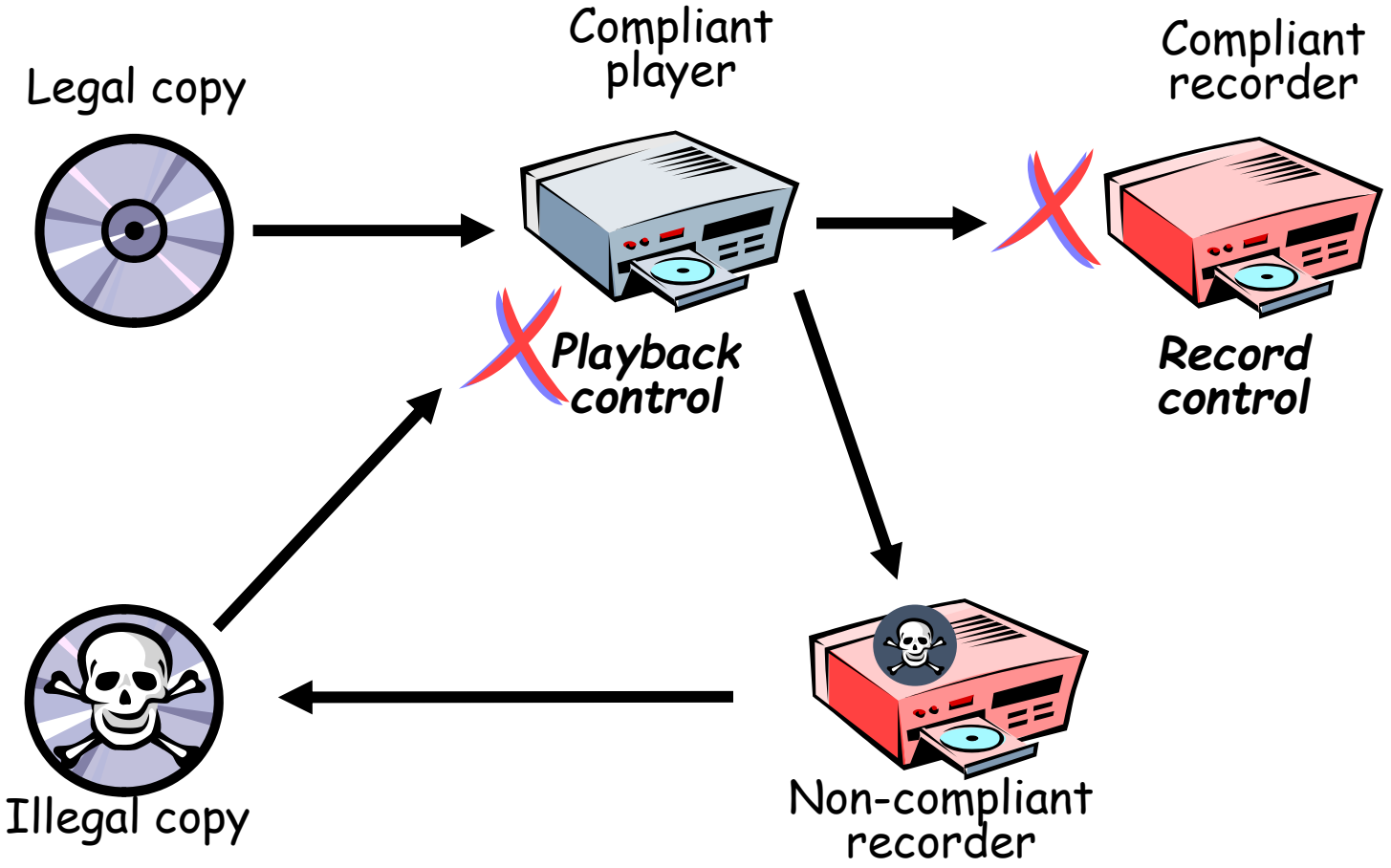
Aplikasi watermarking: *Transaction tracking/fingerprinting*



Aplikasi watermarking: *Content authentication*

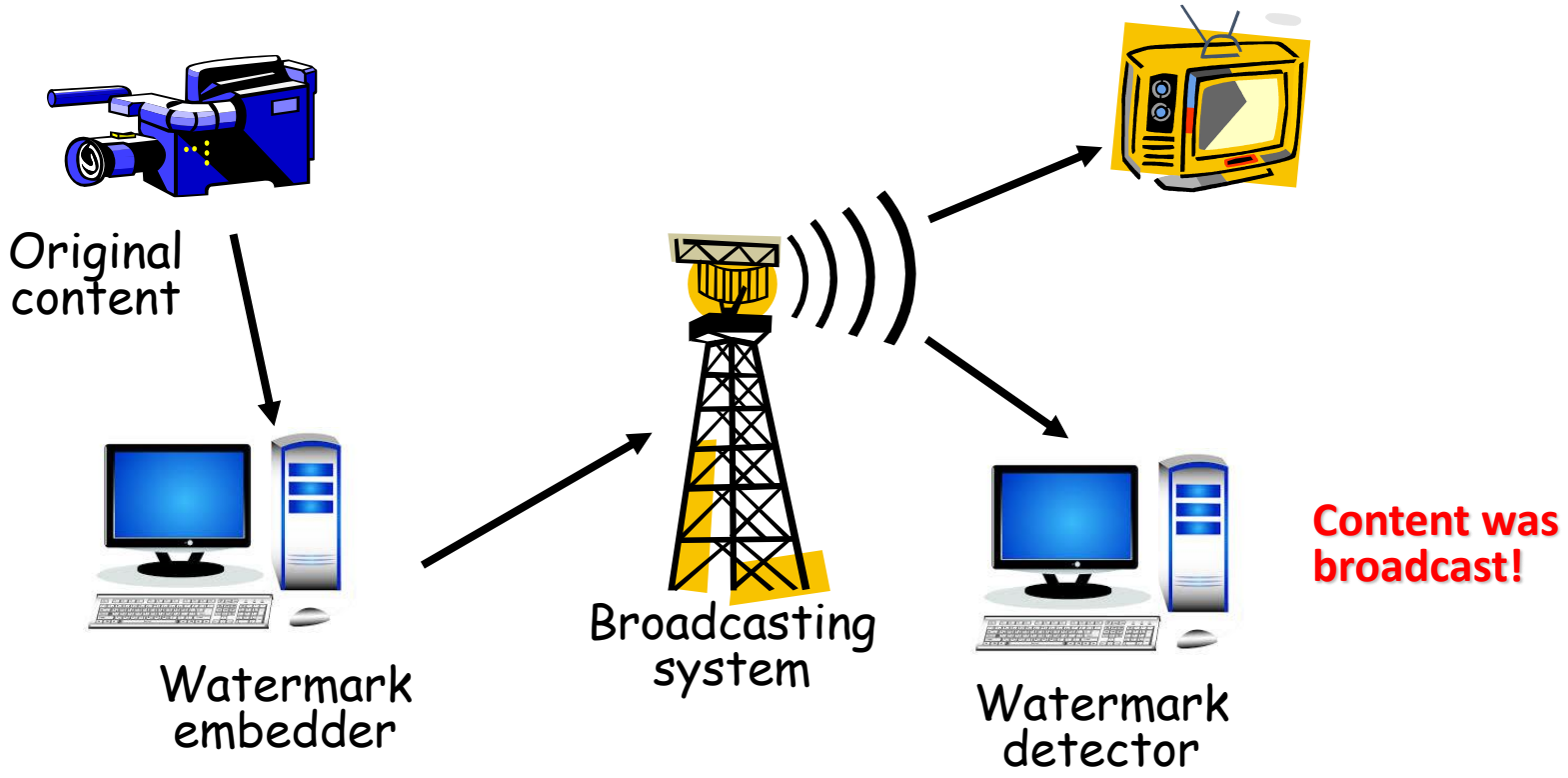


Aplikasi watermarking: *Copy control/Piracy Control*



Watermark digunakan untuk mendeteksi apakah media digital dapat digandakan (copy) atau dimainkan oleh perangkat keras.

Aplikasi watermarking: *Broadcast monitoring*



Watermark digunakan untuk memantau kapan konten digital ditransmisikan melalui saluran penyiaran seperti TV dan radio.

TERIMA KASIH