

II4021 Kriptografi

11 – Digital Watermarking



Oleh: Rinaldi M

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026

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

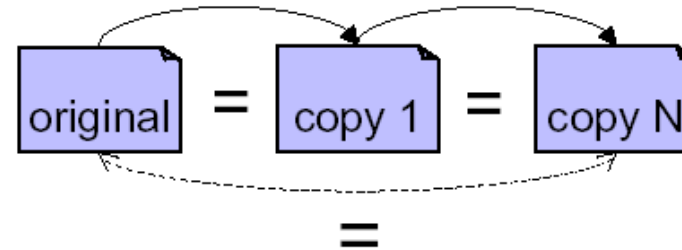
Foto mana yang asli?



(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*

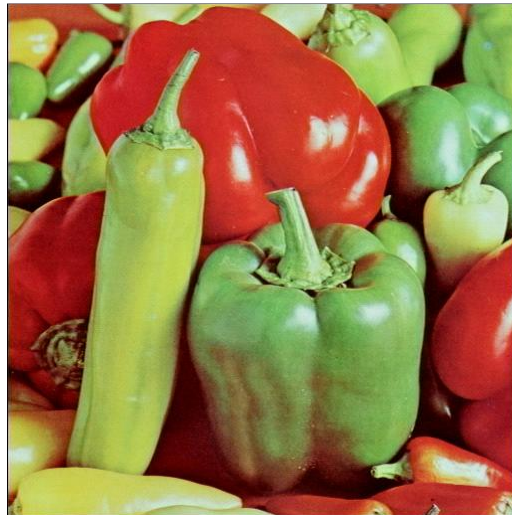
Tidak ada perlindungan terhadap citra digital!!!!

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.



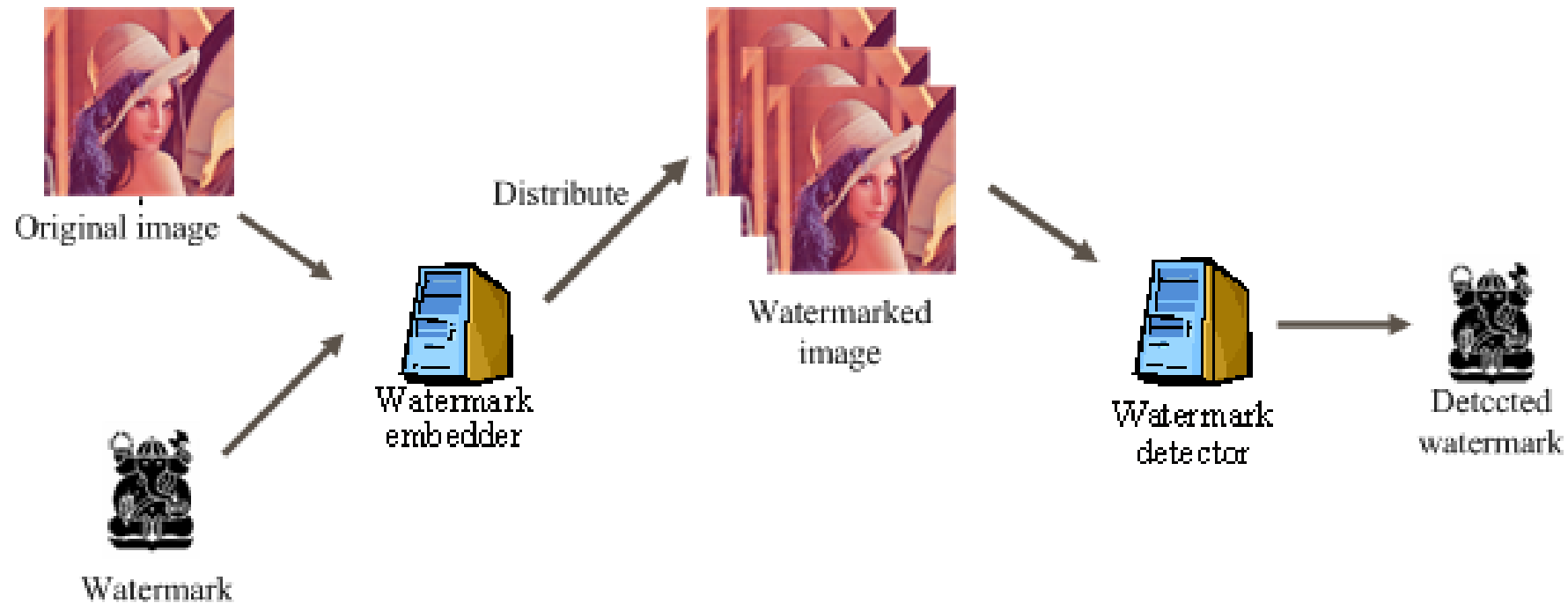
+

shanty

=



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*

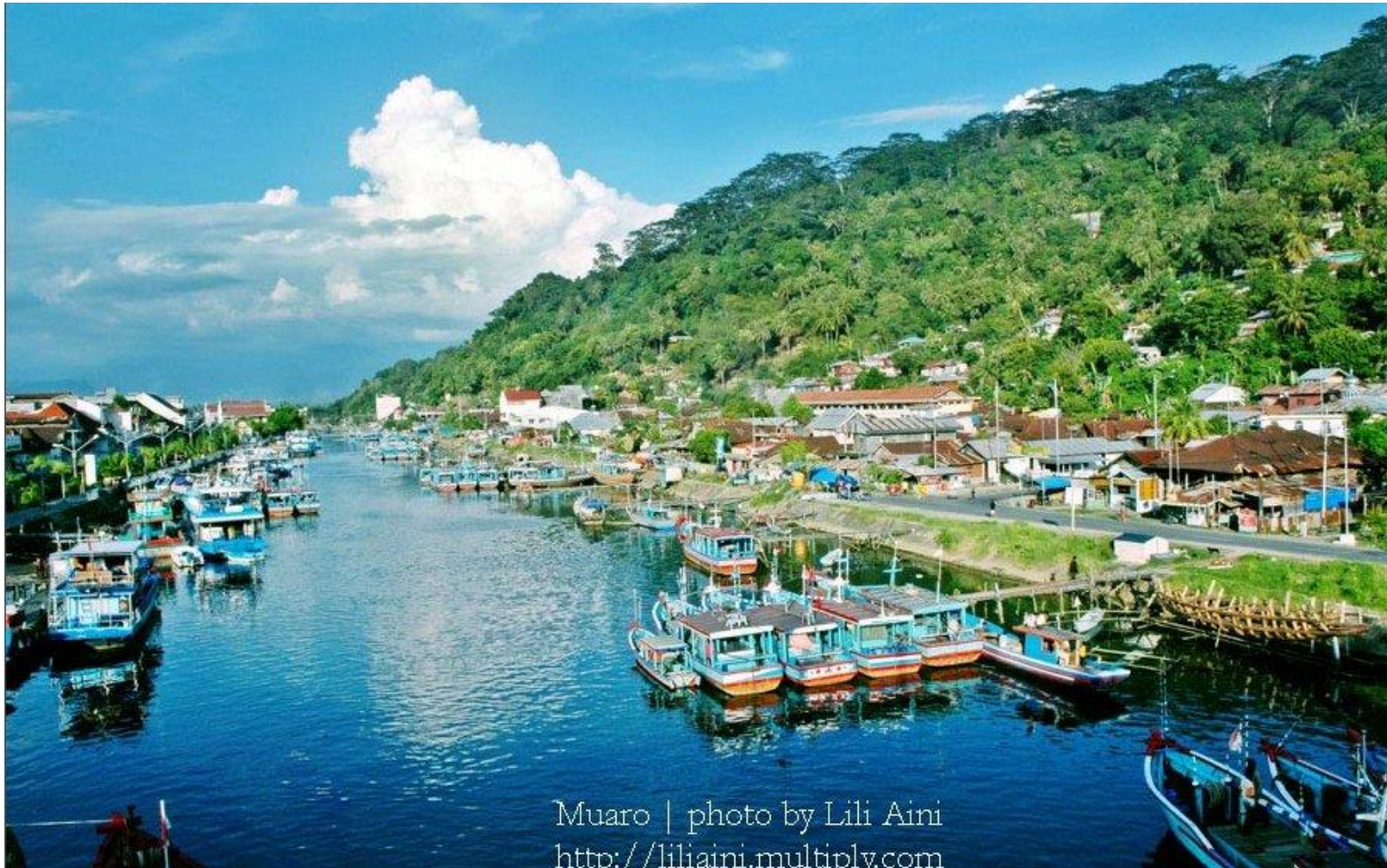
- Label *copyright* ditempelkan pada gambar.
- Kelemahan: tidak efektif melindungi *copyright* sebab label bisa dipotong atau dibuang dengan program pengolahan citra komersil (ex: *Adobe Photoshop*).



Original image + label copyright



Cropped image



Muaro | photo by Lili Aini
<http://liliaini.multiply.com>

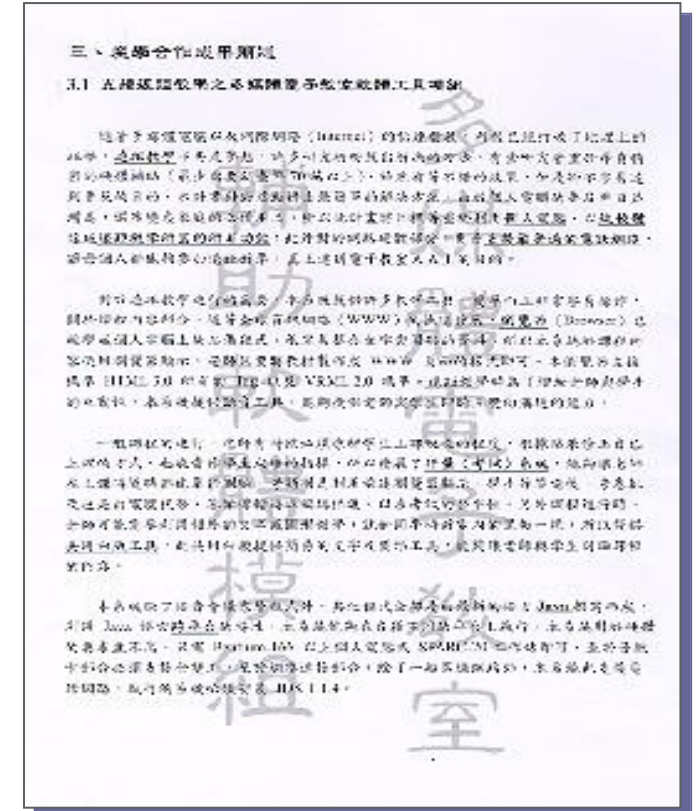
Label kepemilikan

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”

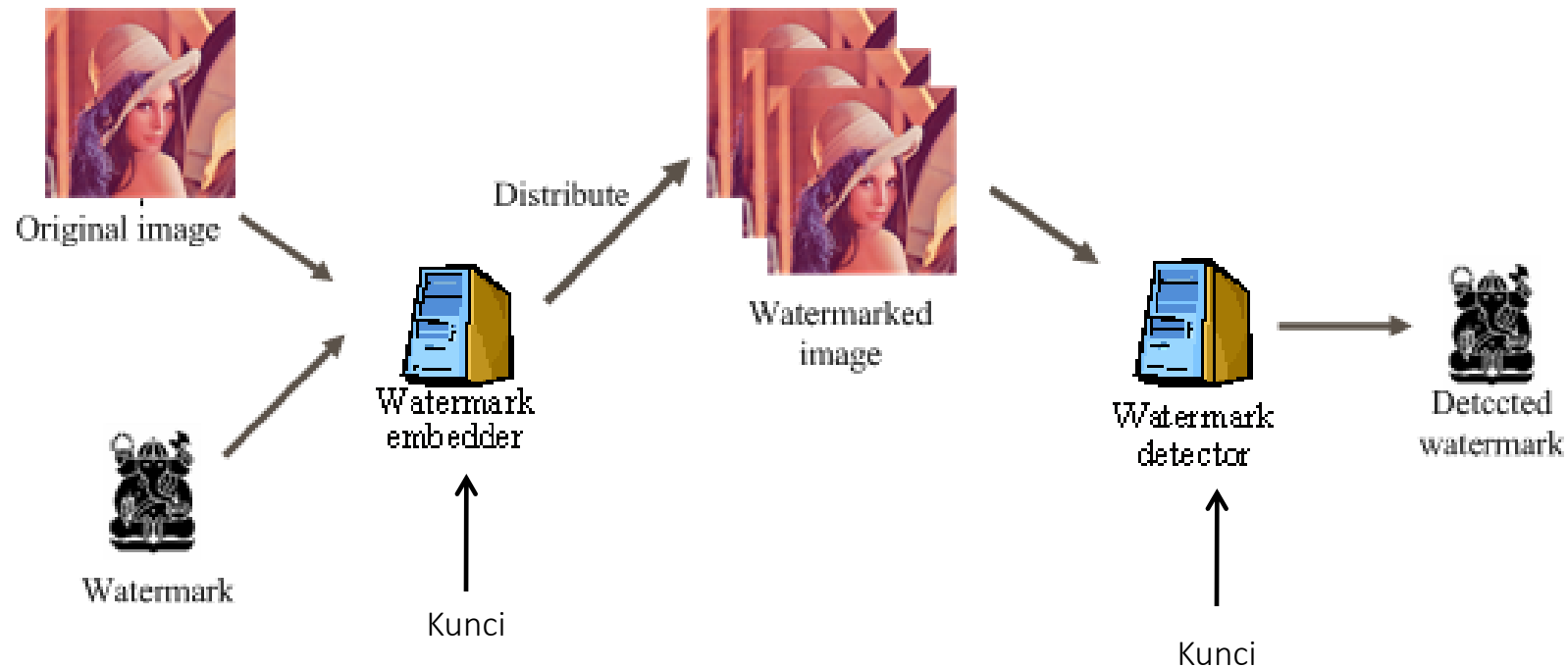
Tujuan: Identifikasi keaslian (otentikasi)

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

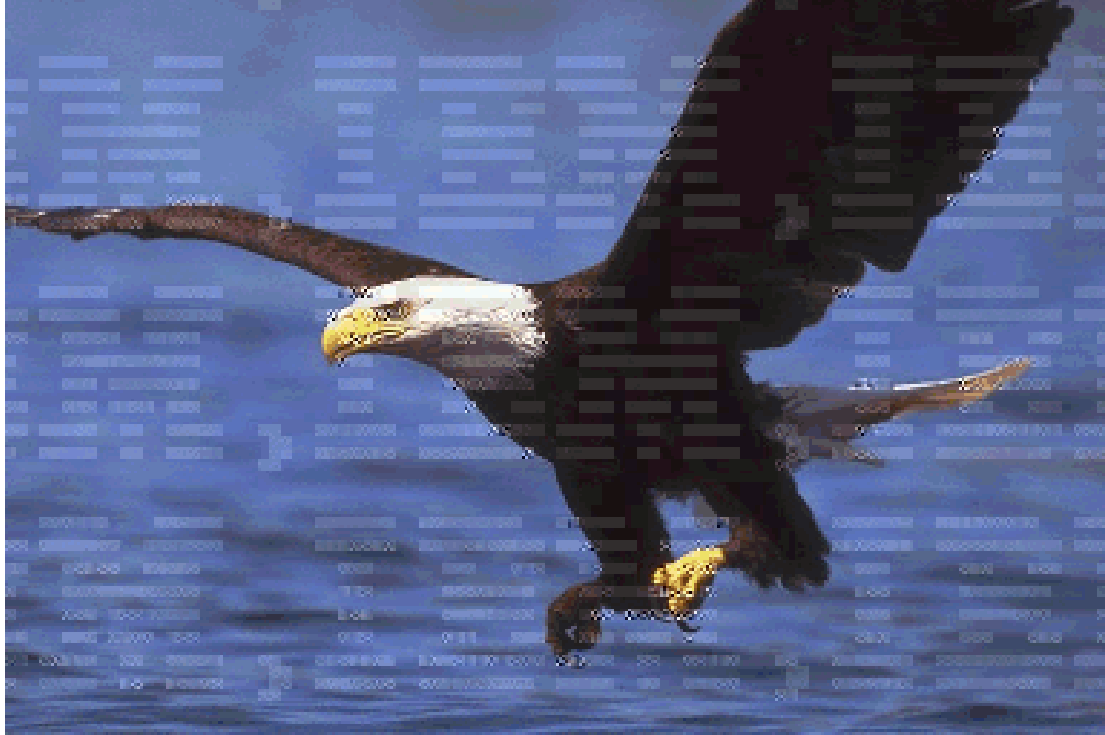
- Penyisipan *watermark* ke dalam citra menghasilkan citra ber-*watermark* (*watermarked image*)
- Terbagi menjadi 2 jenis: *visible watermarking* dan *invisible watermarking*



Invisible Watermark



Visible Watermark



Visible watermarking





Invisible watermarking

Klasifikasi (invisible) *Image Watermarking*

- ***Fragile watermarking***

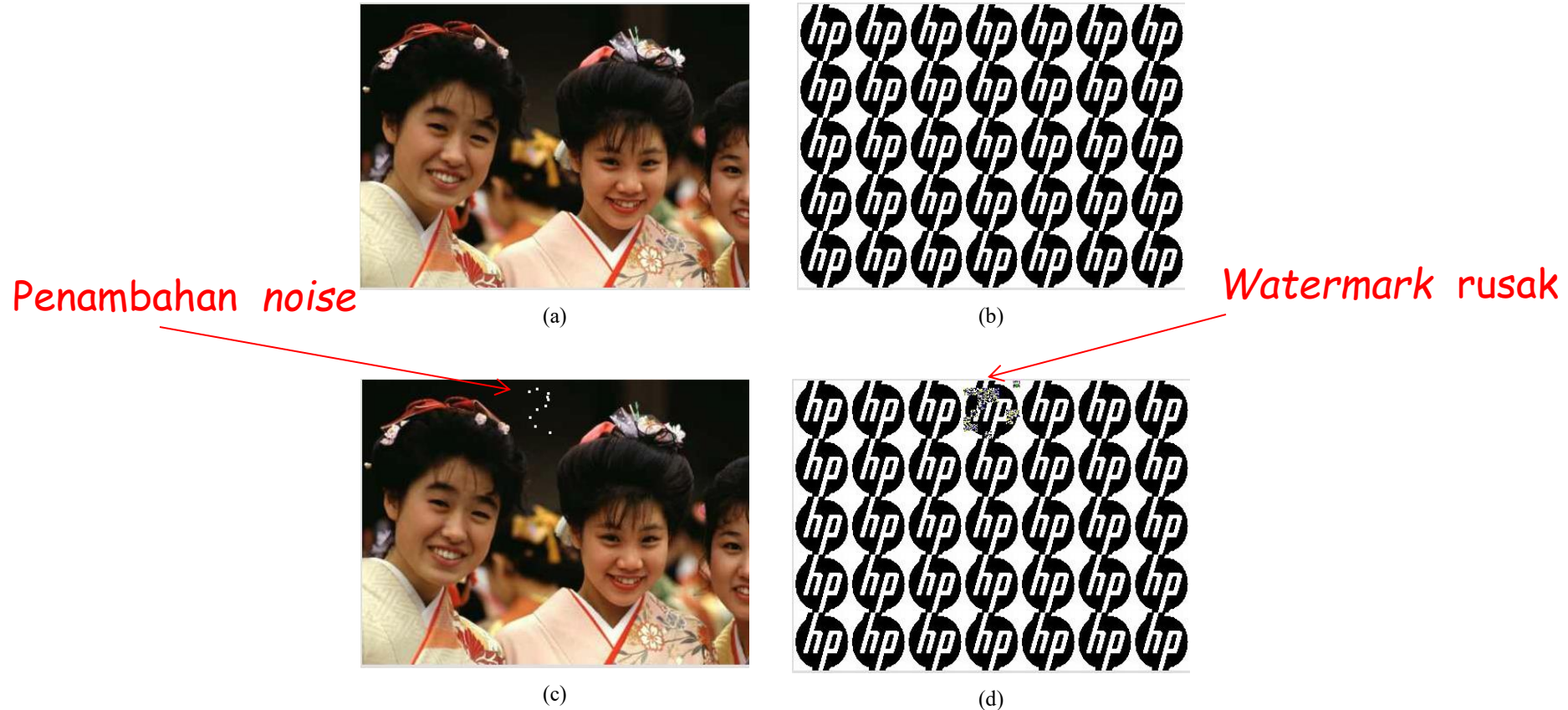
Tujuan: untuk menjaga integritas/orisinilitas citra digital.

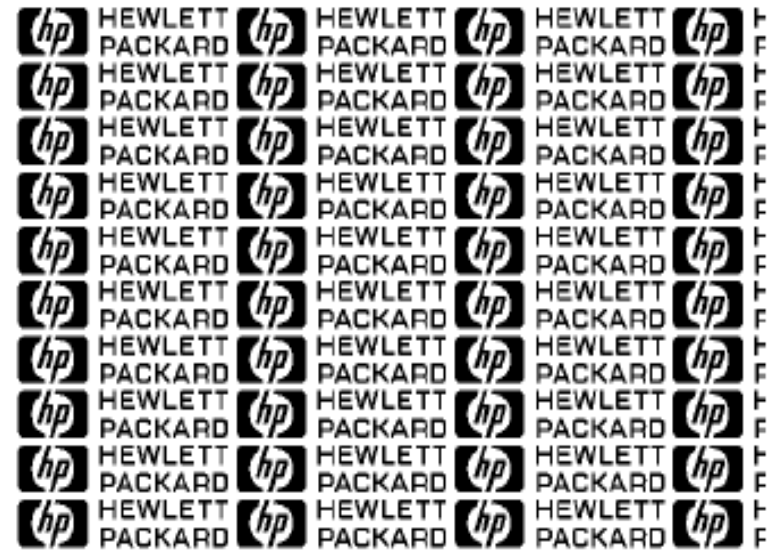
- ***Robust watermarking***

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?

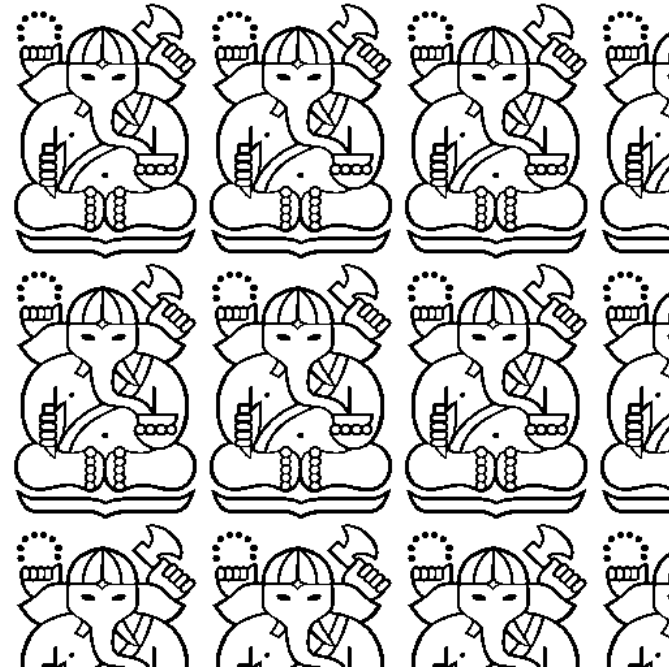
- Pertama, harus mengerti dulu konsep citra digital (sudah dijelaskan di dalam materi Steganografi)
- Kedua, mengerti metode LSB (sudah dijelaskan di dalam materi Steganografi)

Algoritma *Fragile Watermarking*

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



Citra asli

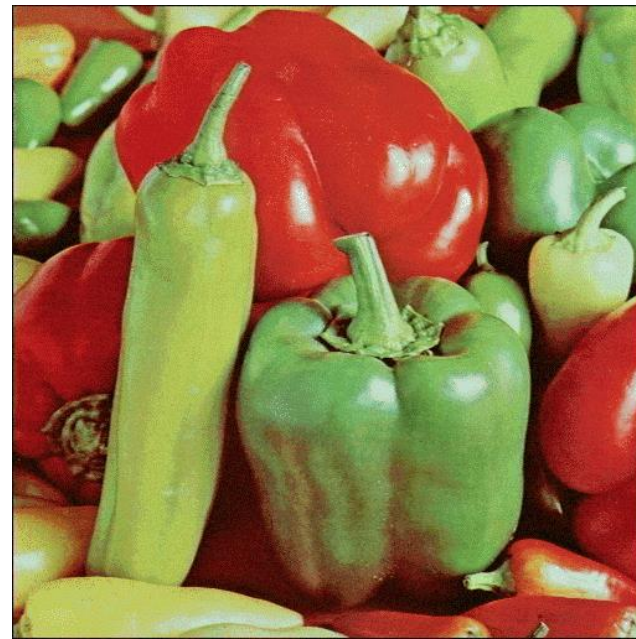


watermark

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

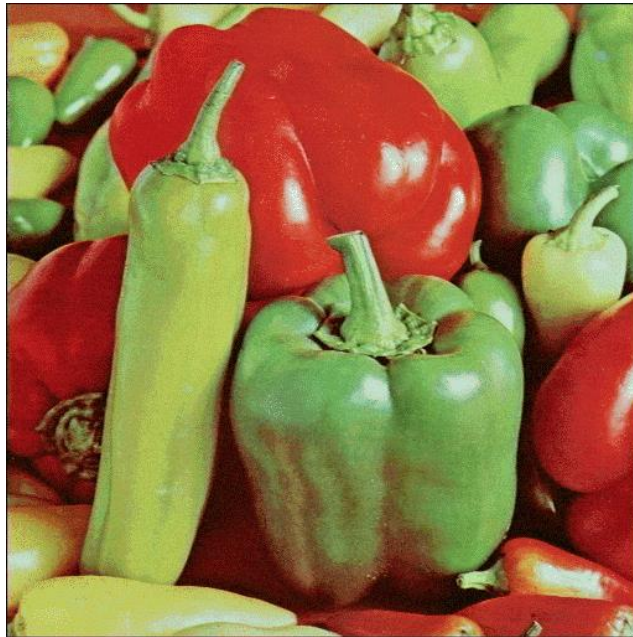


Citra asli

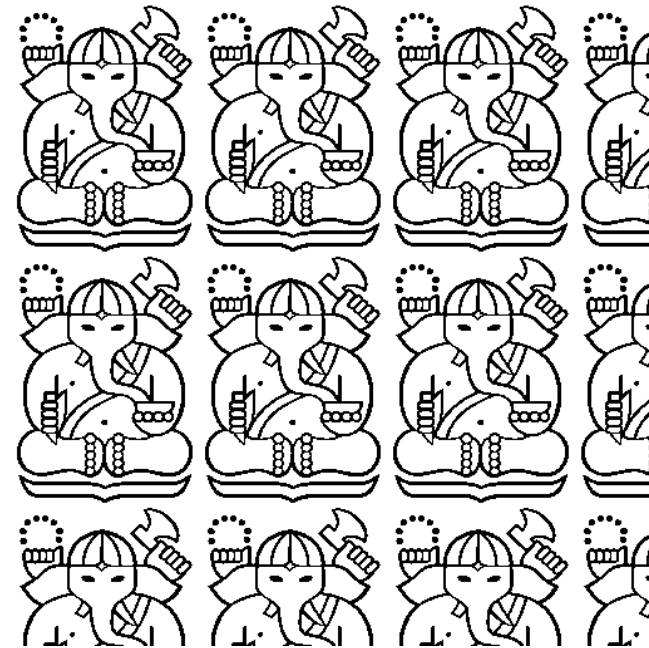


Citra ber-watermark

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



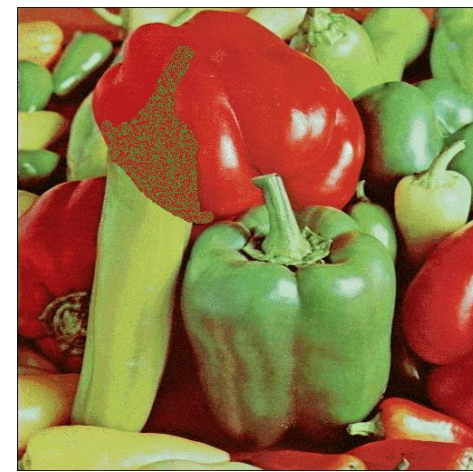
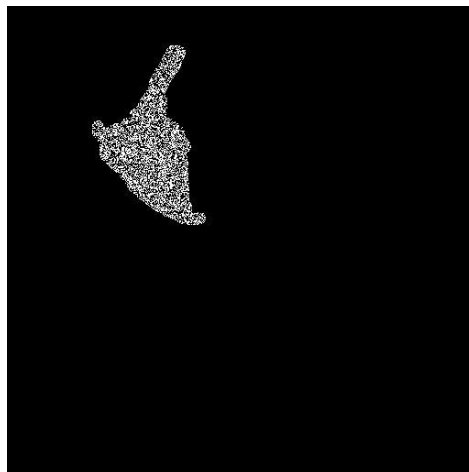
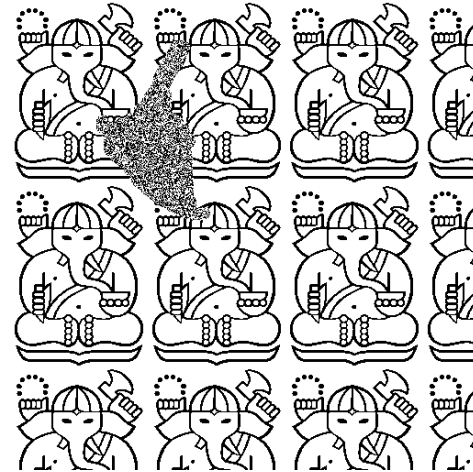
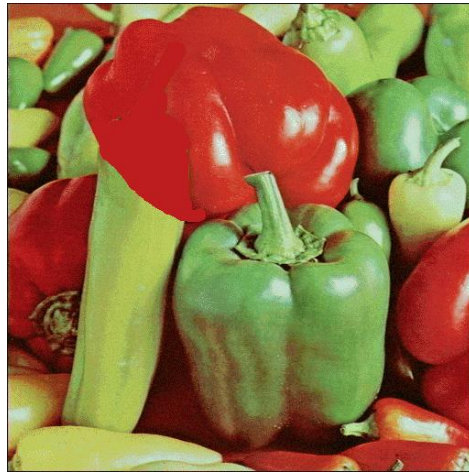
Citra ber-watermark



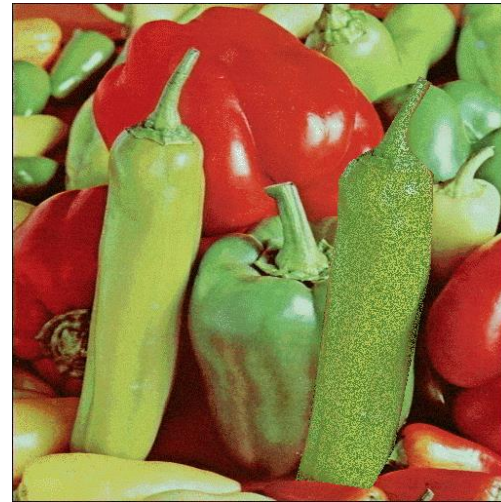
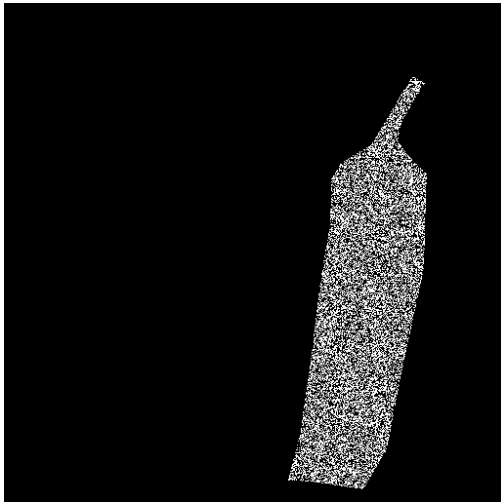
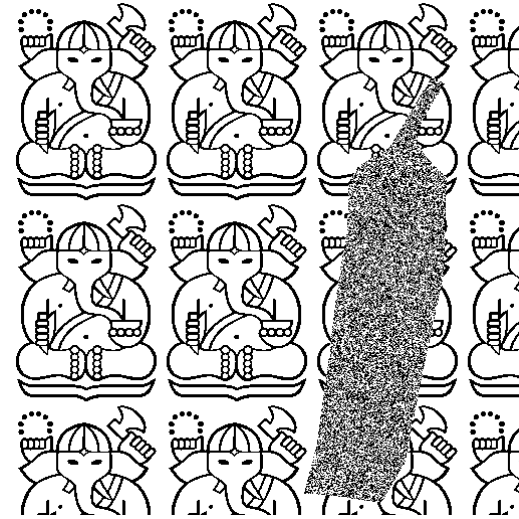
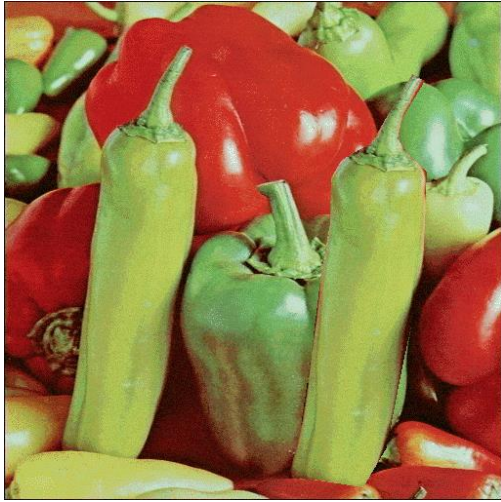
Watermark hasil ekstraksi

Test manipulasi pada citra ber-*watermark*

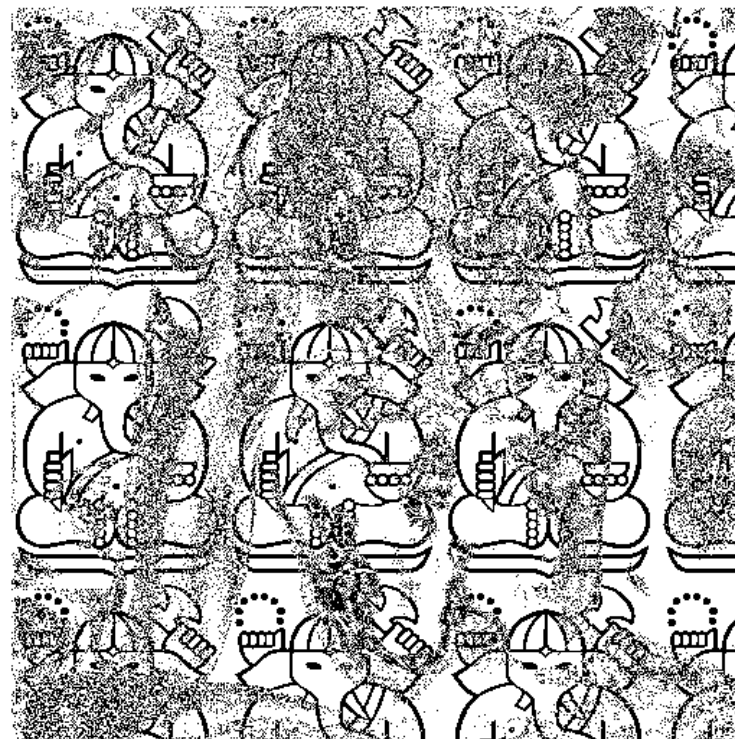
Deletion attack



Insertion attack



Brightness and contrast attack

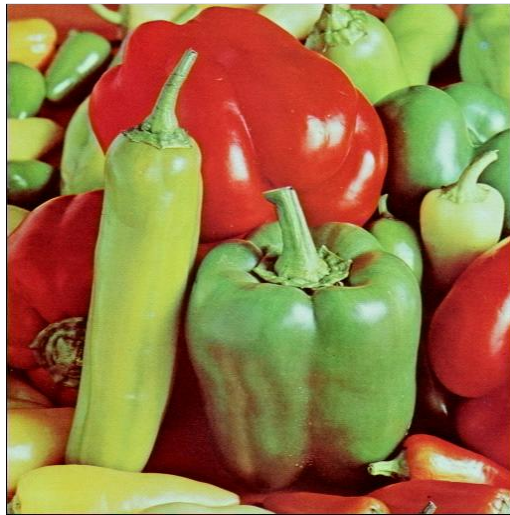


Robust Watermarking

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

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

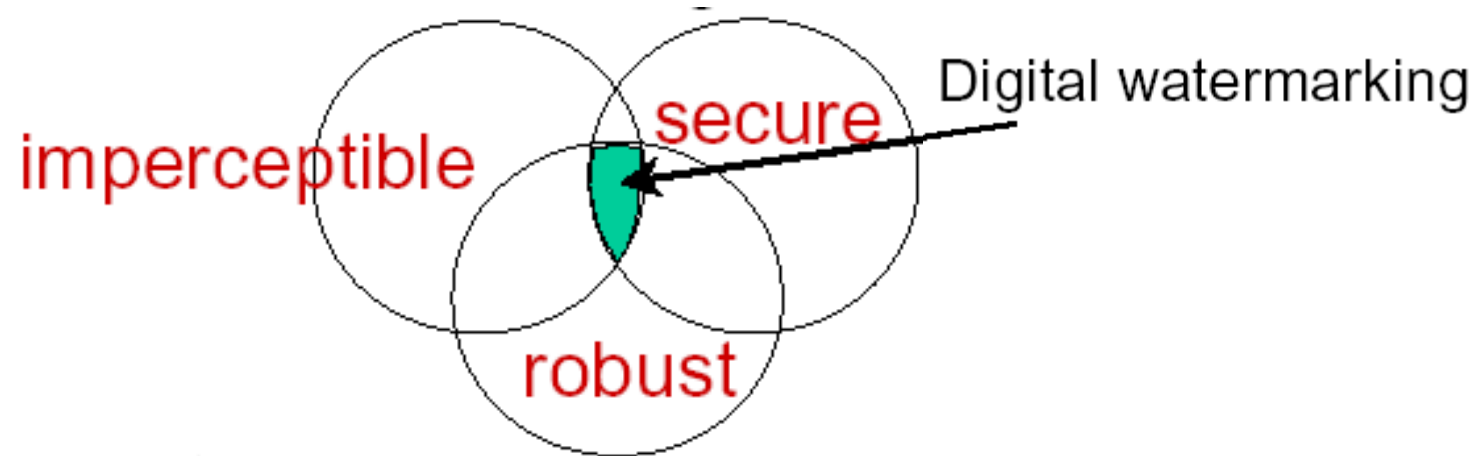
- Tujuan: perlindungan hak kepemilikan dan *copyright*



+ shantty =



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





Original image



Watermarked image



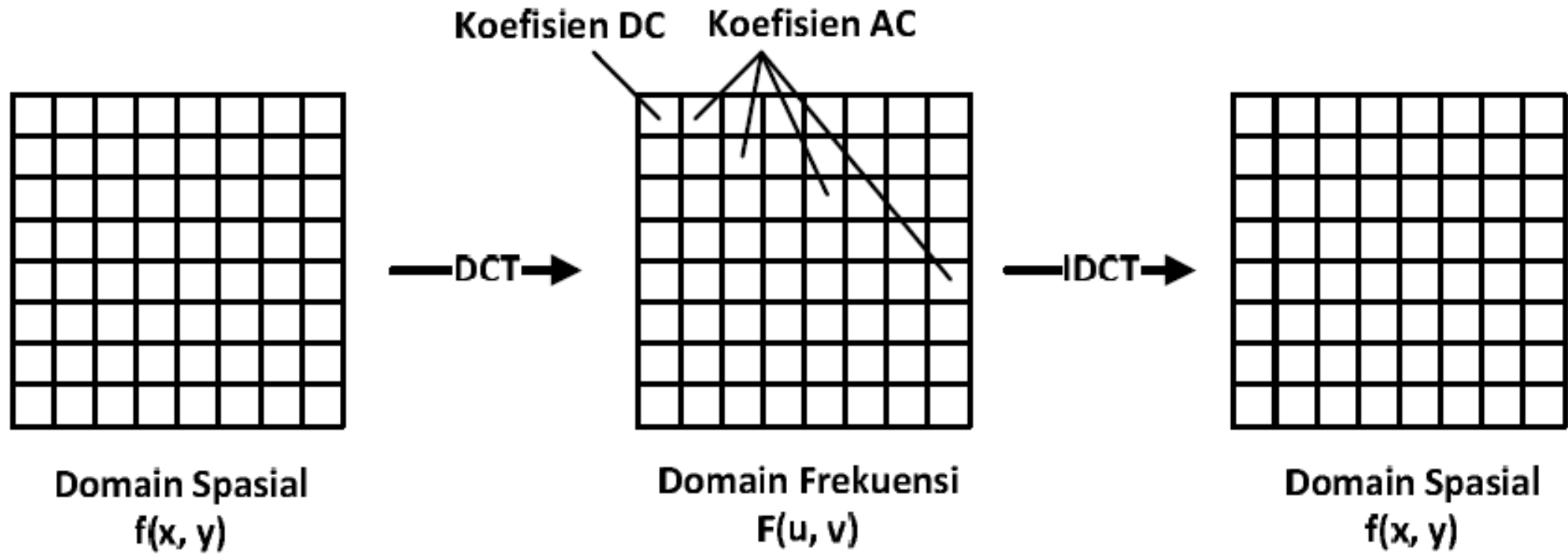
watermark



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*)



- *Discrete Cosine Transform (DCT)*

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

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

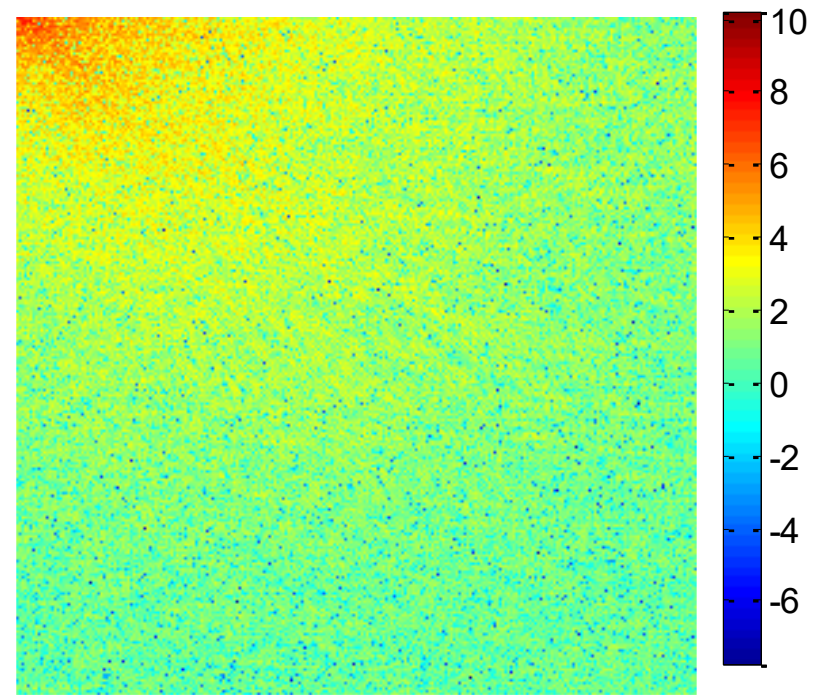
C(u,v) disebut koefisien-koefisien DCT

- *Inverse Discrete Cosine Transform (IDCT)*

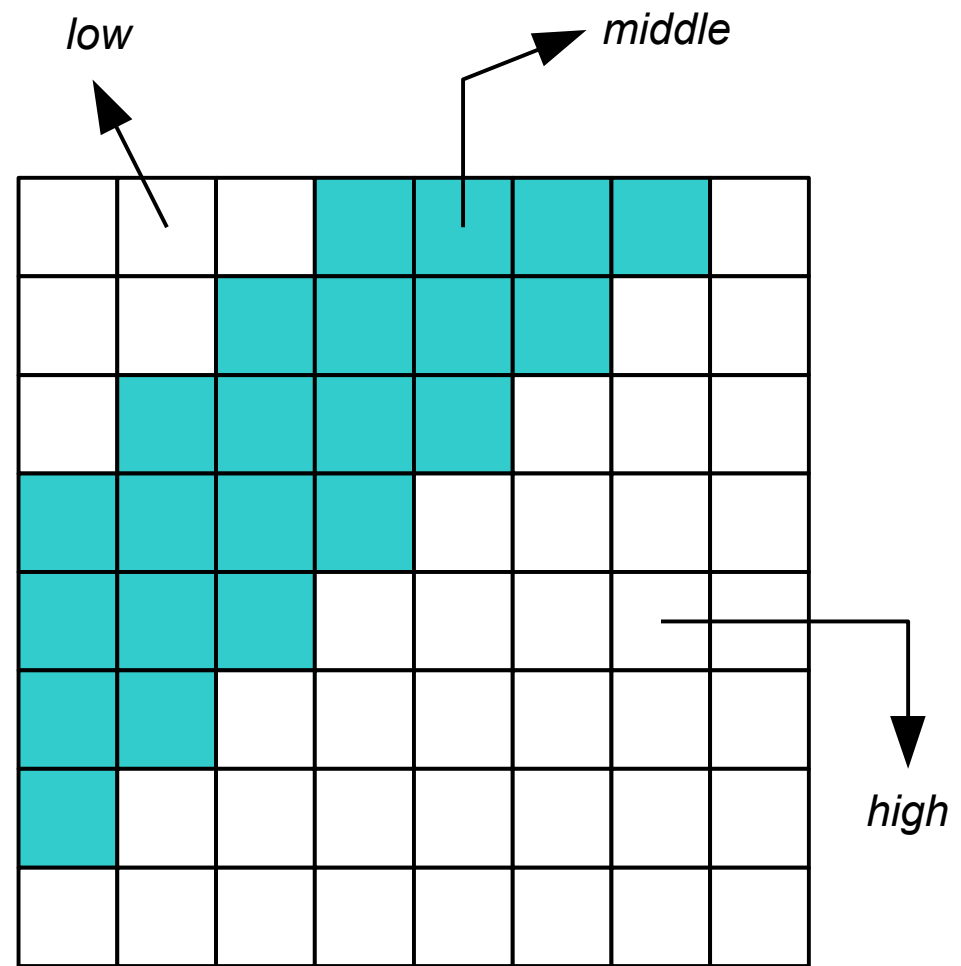
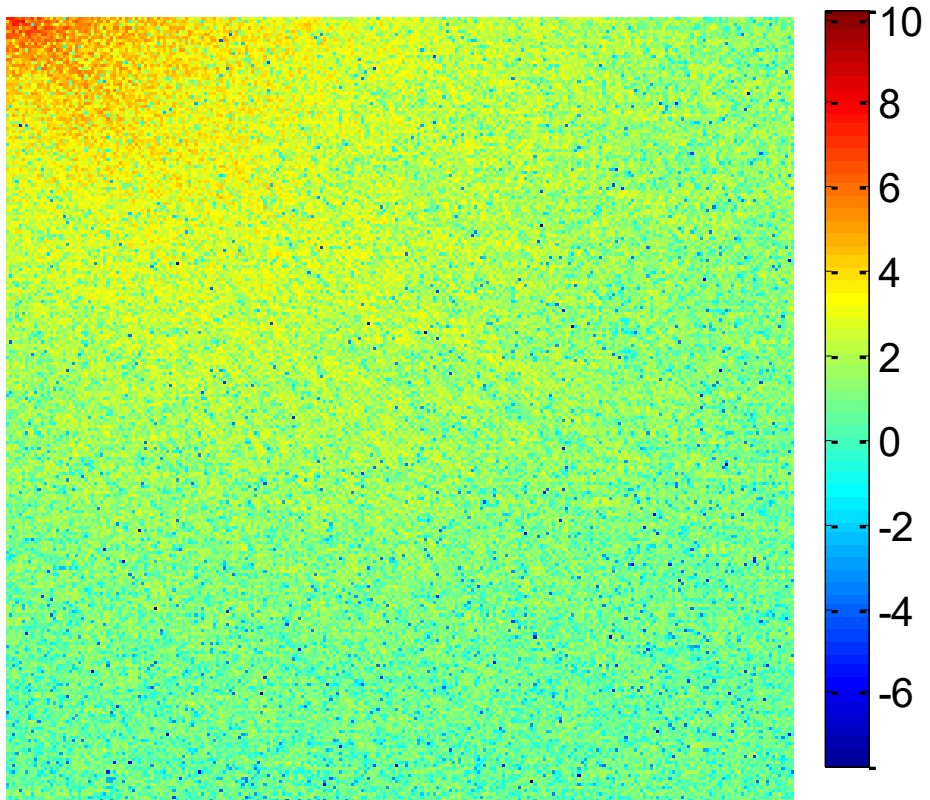
$$I(x, y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u, v) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \quad (4)$$



Citra dalam ranah spasial



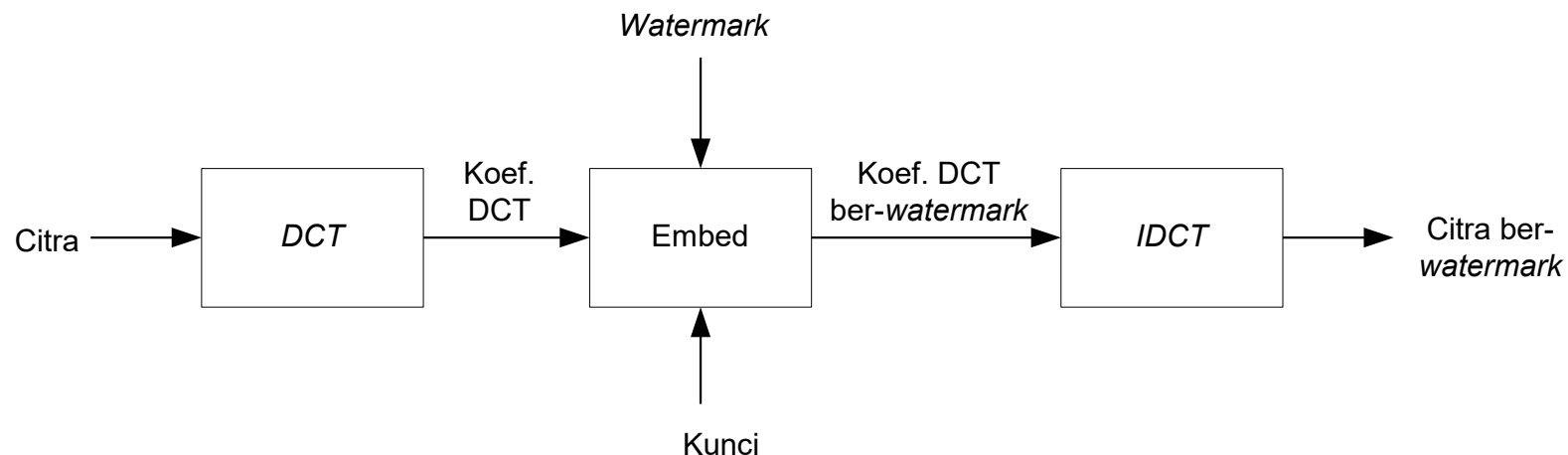
Citra dalam ranah frekuensi



- Hasil tranformasi menghasilkan nilai-nilai yang disebut koefisien-koefisien transformasi (misalnya koefisien DCT).
- Bit-bit *watermark* (w) disembunyikan pada koefisien-koefisien tranformasi (x) menggunakan berbagai metode, seperti metode LSB, *spread spectrum*, dsb.
- Jika watermark berupa bilangan riil, salah satu formulanya adalah:

$$\hat{x}_i = x_i + \alpha w_i \quad \alpha = \text{kekuatan } robustness$$

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



Wang Algorithm (1)

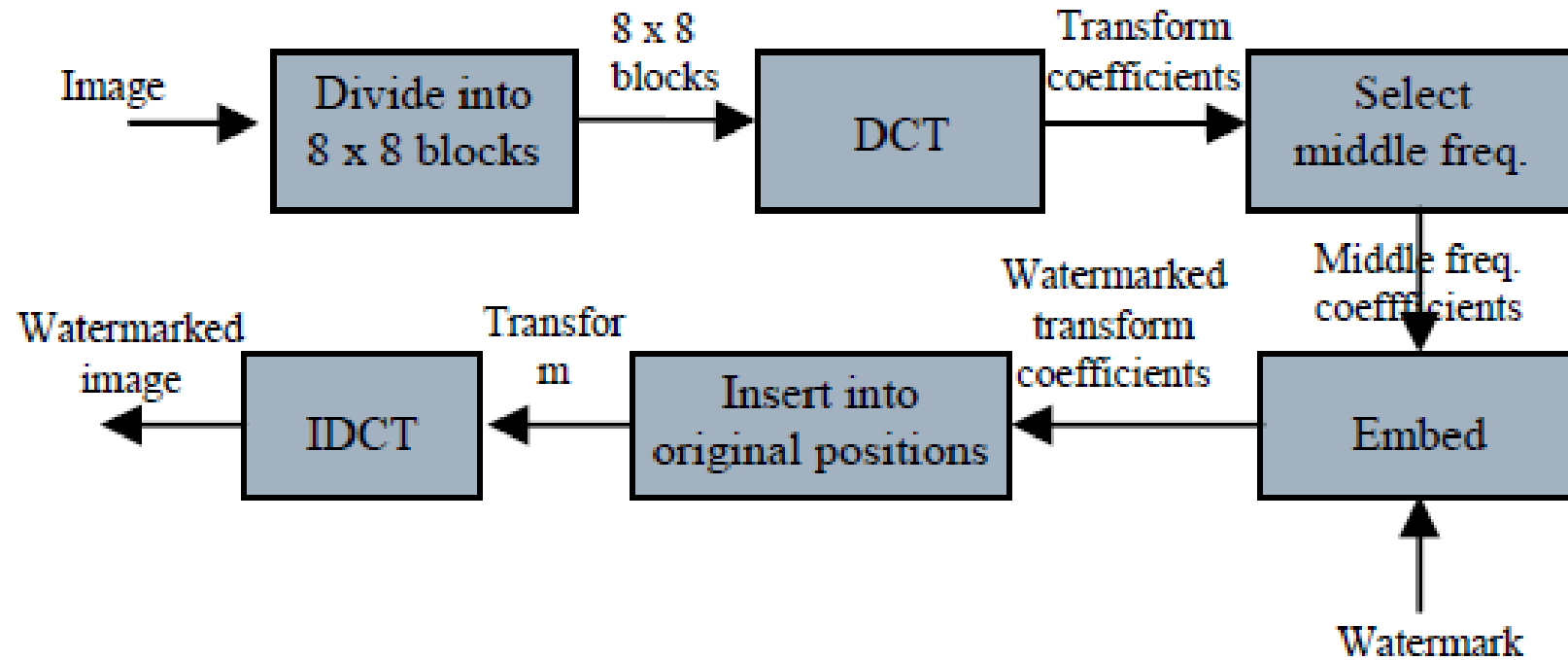


Fig. 1. Embedding process

Wang Algorithm (2)

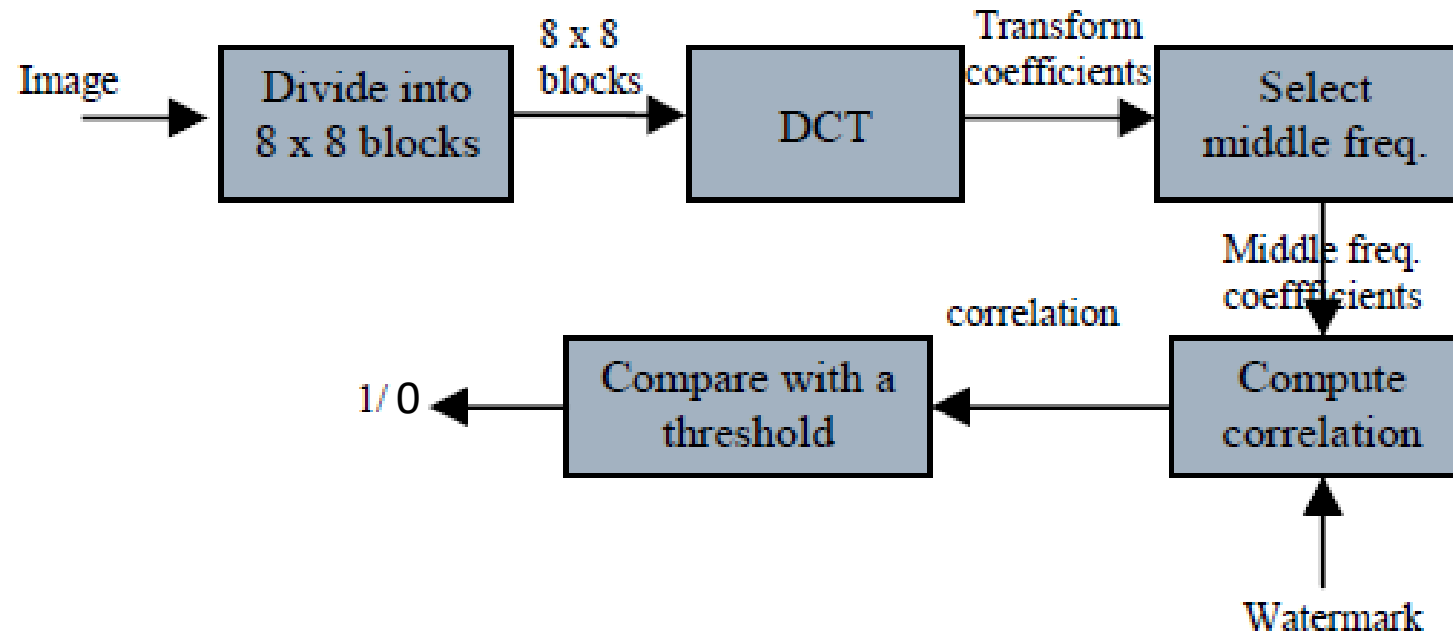


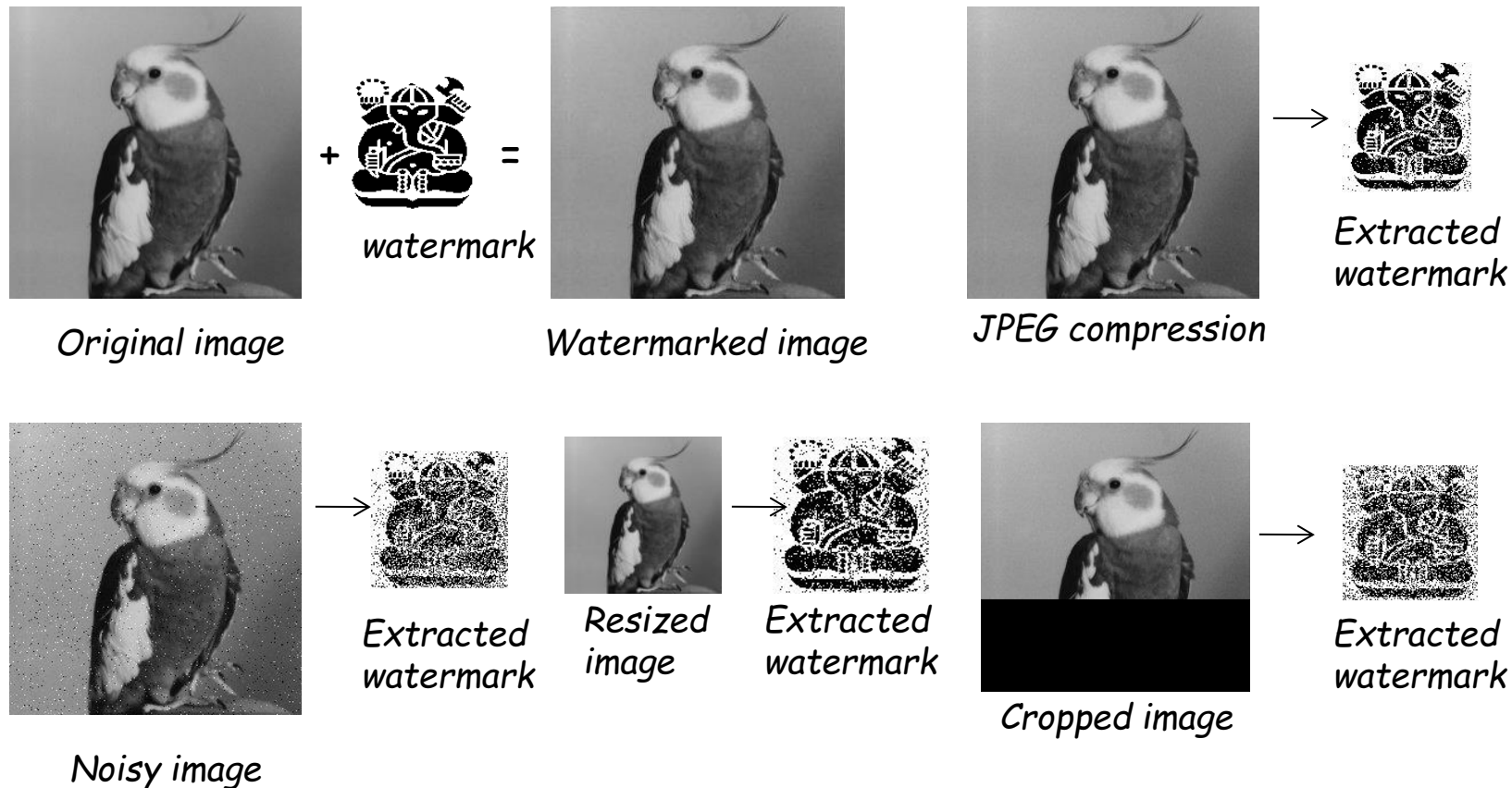
Fig. 2. Detection process

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

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

Test ketahanan *watermark* terhadap manipulasi terhadap citra.

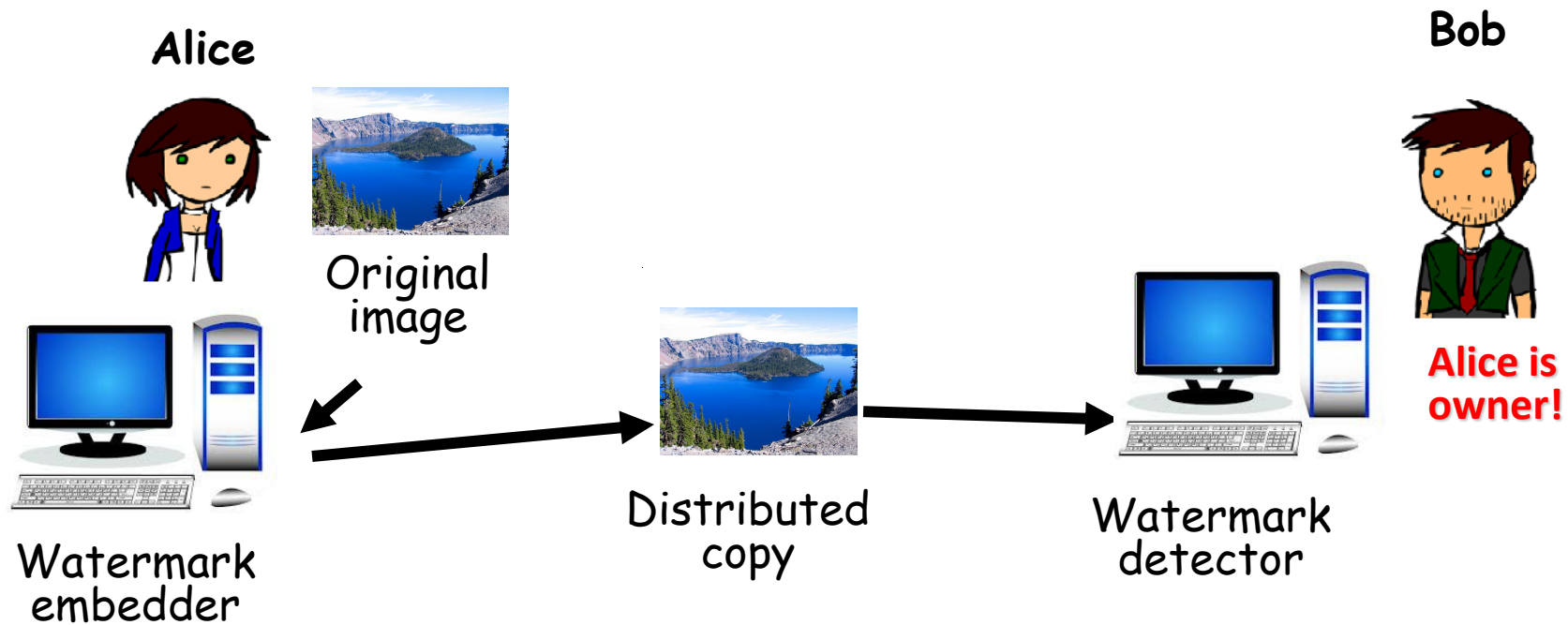
Contoh: kompresi, *cropping*, *editing*, *resizing*, dll



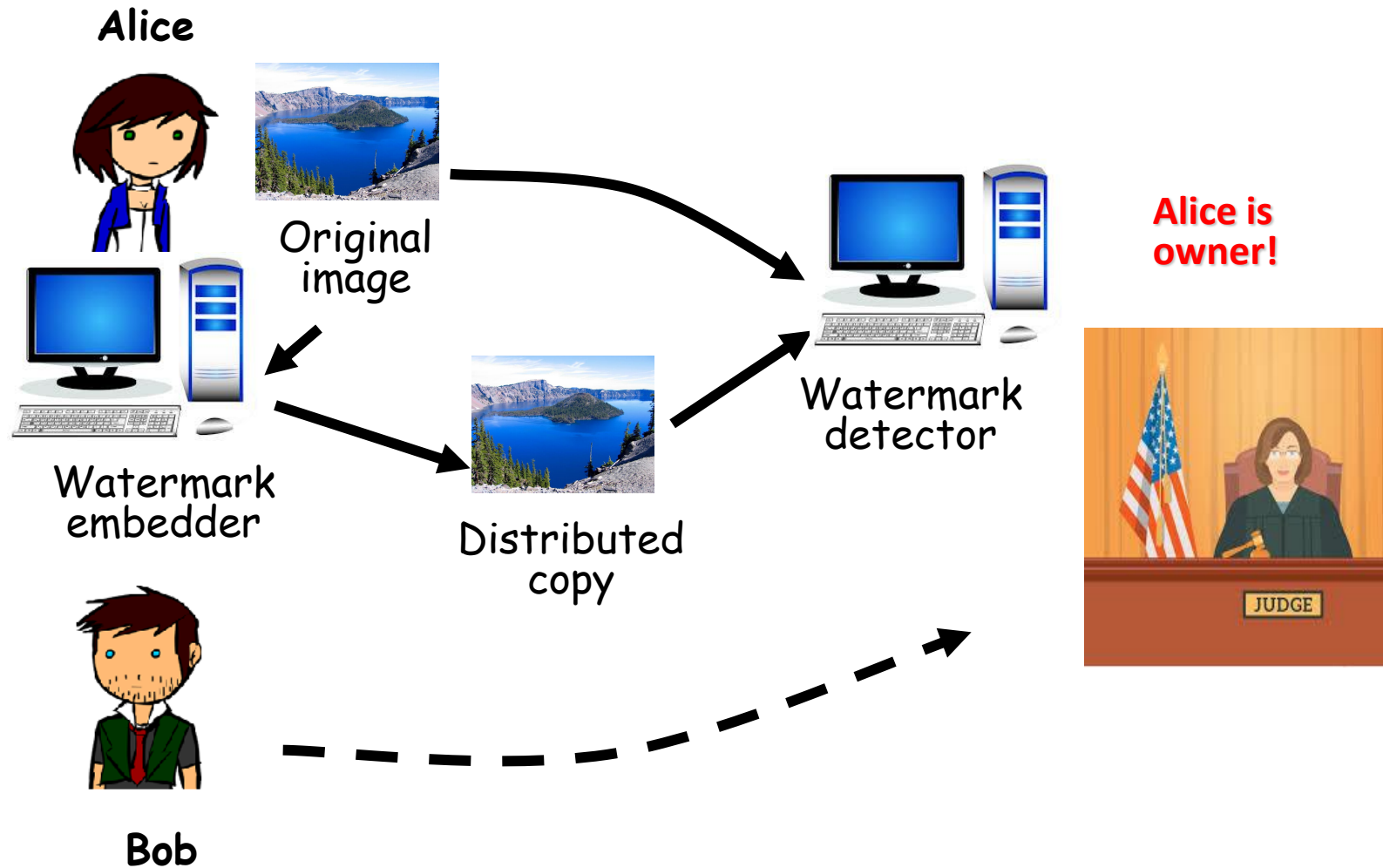
Aplikasi *Watermarking*

- 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*

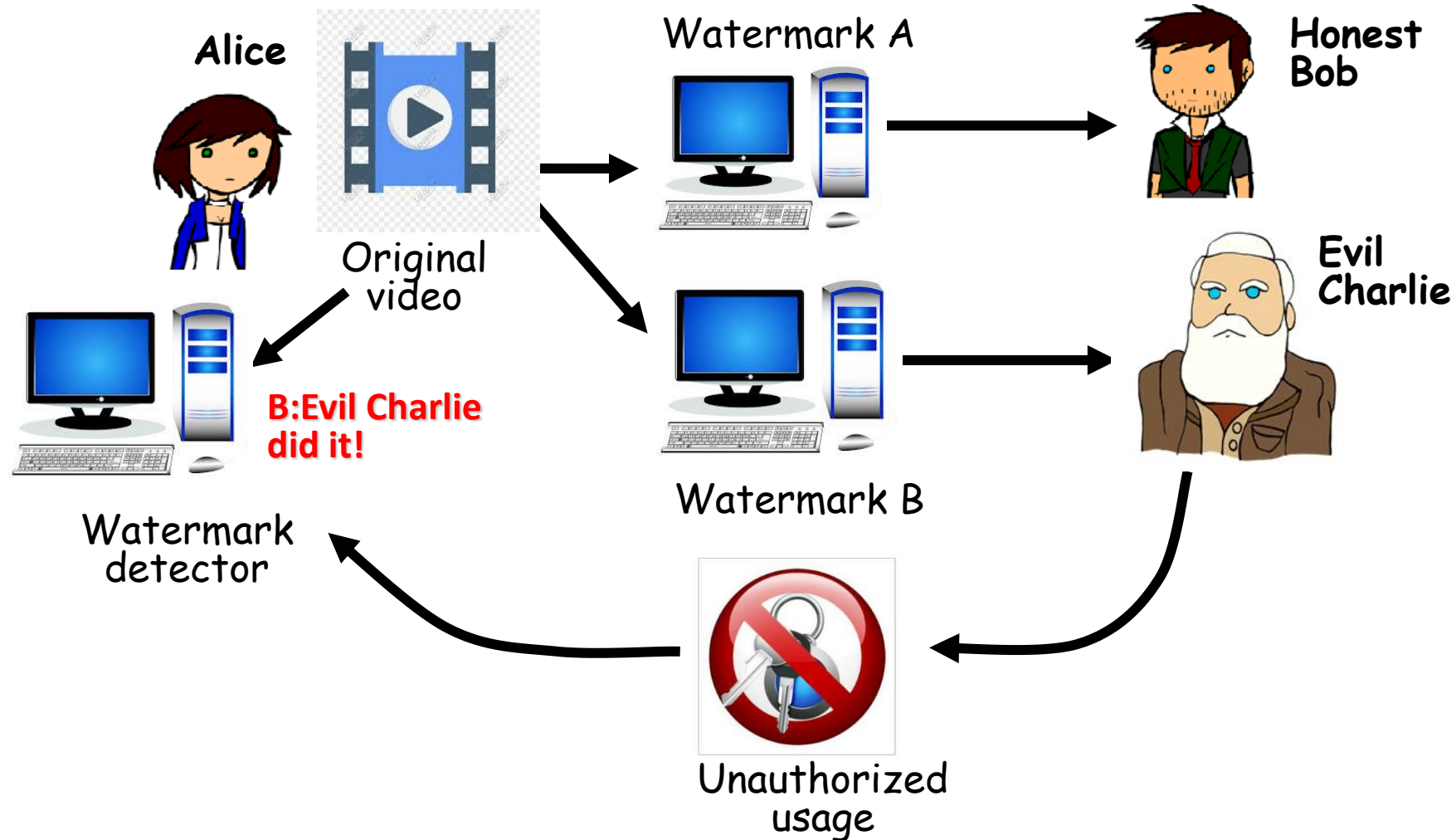
Aplikasi watermarking: *Owner identification*



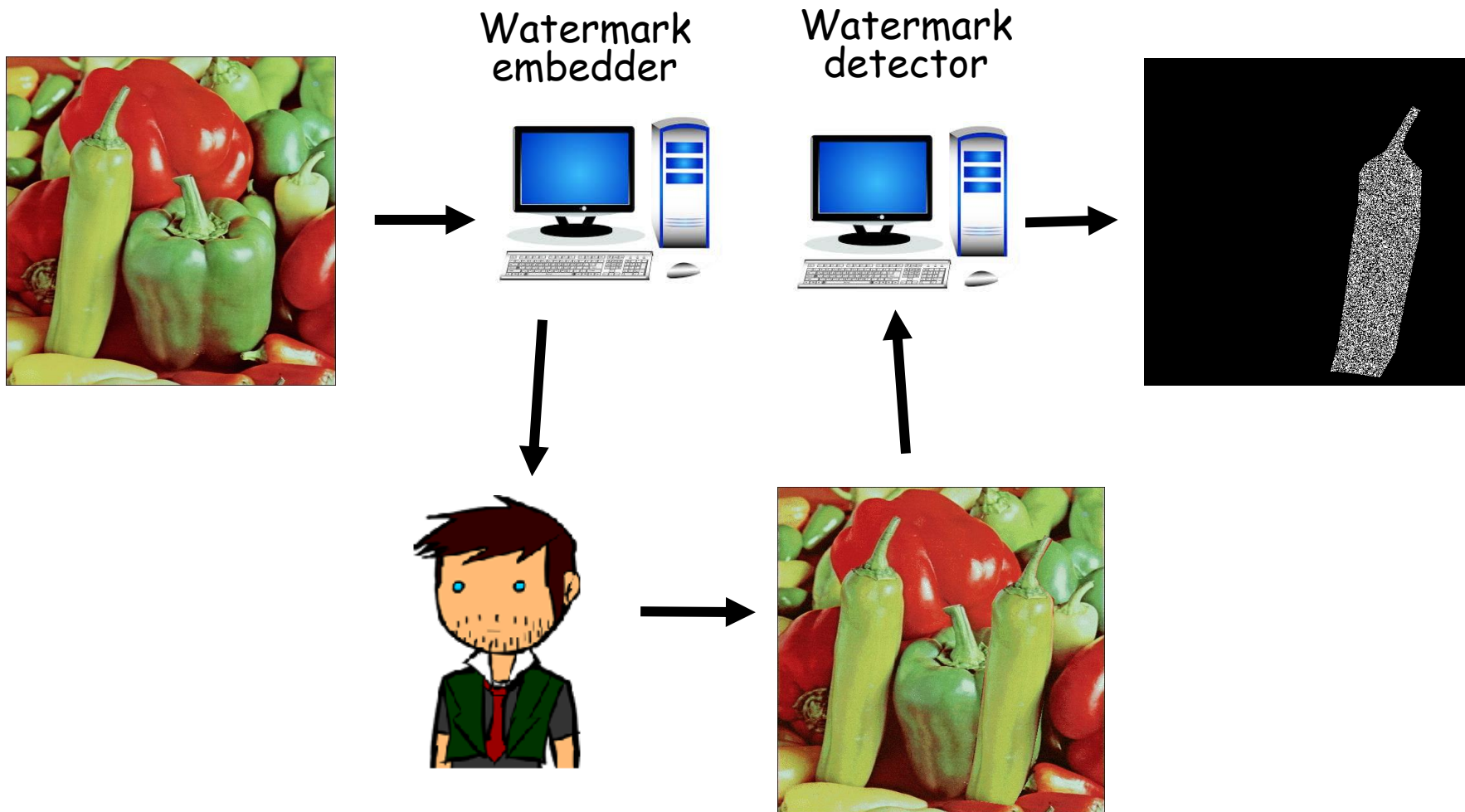
Aplikasi watermarking: *Proof of ownership*



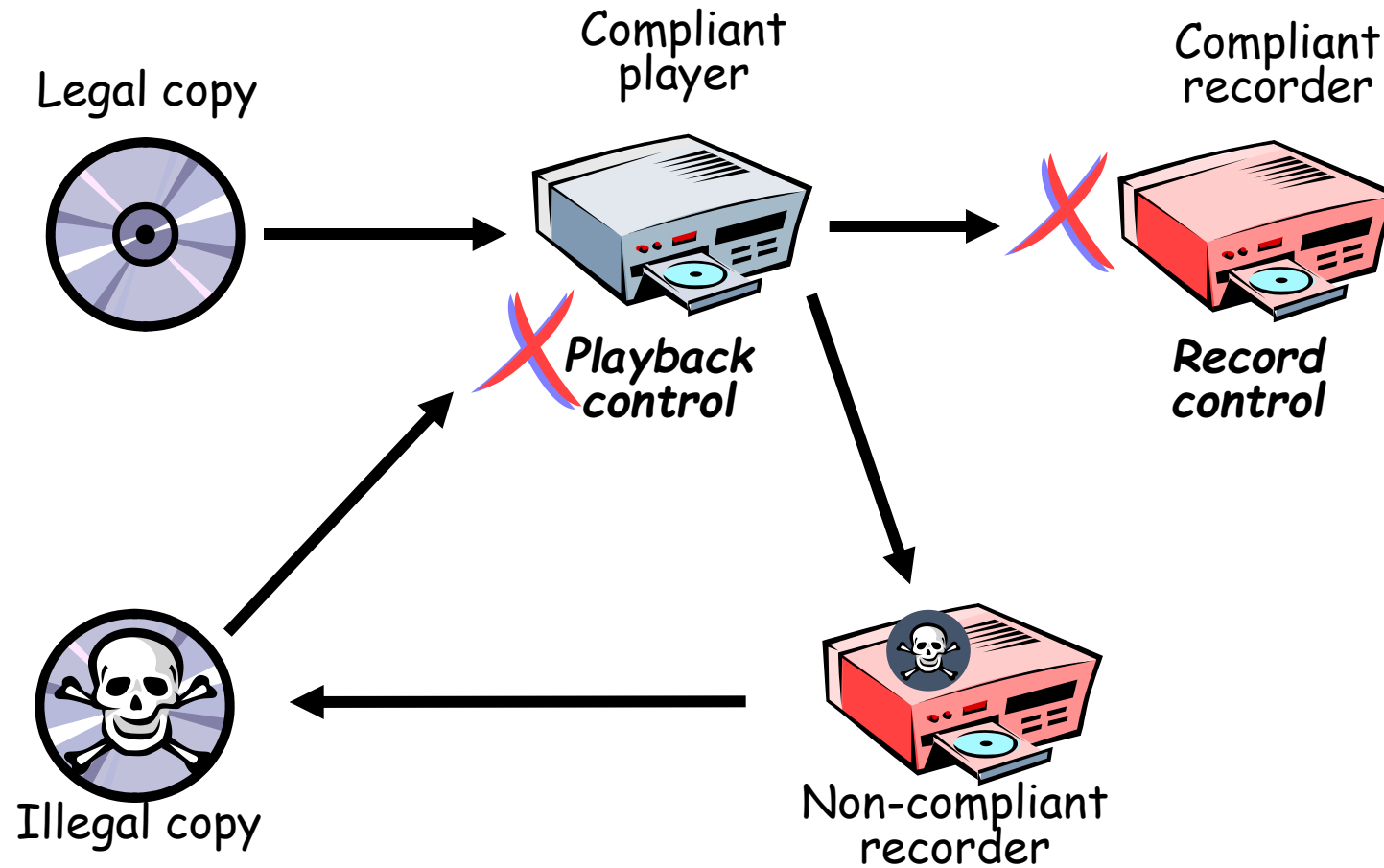
Aplikasi watermarking: *Transaction tracking/fingerprinting*



Aplikasi watermarking: *Content authentication*

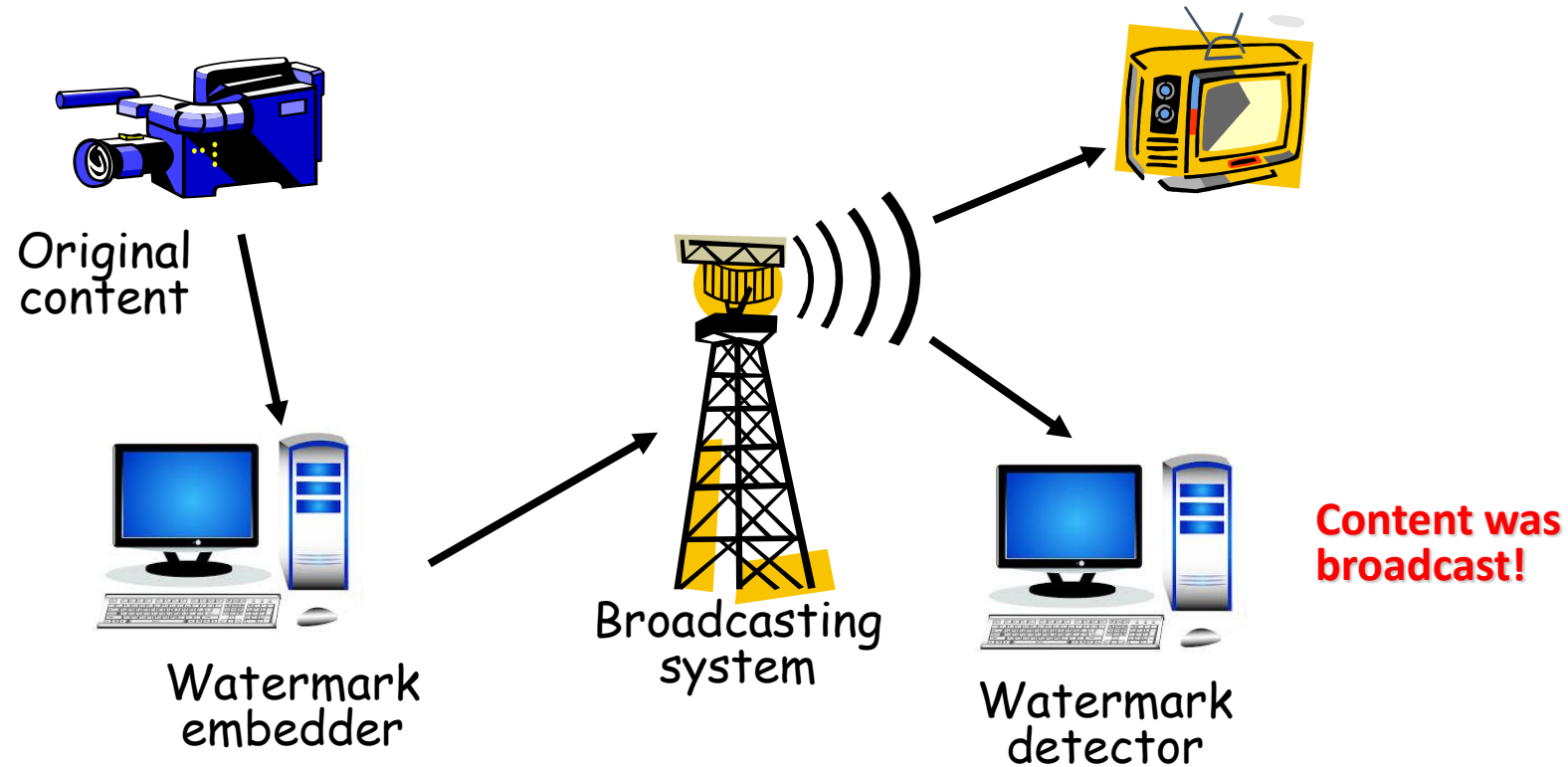


Aplikasi watermarking: *Copy control/Piracy Control*



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.

Bagaimana watermarking digunakan di dalam Netflix?

- Di Netflix, watermarking digunakan sebagai bagian dari sistem keamanan konten (*content protection*) untuk mencegah pembajakan dan melacak sumber kebocoran film atau serial.
- *Watermark* tertanam di dalam video/audio (disebut juga *invisible watermarking* atau *forensic watermarking*), bukan *watermark* yang terlihat (*visible watermark*)
- Watermark bisa dideteksi secara forensik jika terjadi pembajakan.
- Watermark tersebut mengandung identitas seperti:
 - ID akun
 - ID sesi streaming
 - Perangkat
 - Timestamp distribusi
- Jika file Netflix direkam dan diunggah ke situs bajakan, maka Netflix dapat mengekstrak watermark dari video bajakan tersebut dan dapat mengetahui dari akun siapa bocor dan kapan.



Salah satu teknik konvensional membajak film yang tayang di layar, kamera *camcorder* atau kamera *handphone* merekam film yang sedang *play* di layar

Sumber gambar: <https://medium.com/pallycon/how-netflix-protects-contents-part-2-33c1b60002a3>

Bagaimana cara penyisipan watermark ke dalam video Netflix?

- Saat user melakukan video streaming, sistem menyisipkan watermark unik secara real-time pada setiap segmen video.
- Watermark yang disisipkan bisa lebih dari satu untuk masing-masing segmen
- Misalnya, segmen 1 punya dua versi (A dan B), segmen 2 punya dua versi, dst
- Setiap user akan menerima kombinasi unik: A – B – B – A – A – B – ...
- Kombinasi itu = identitas user.
- Watermark biasanya disisipkan dalam domain DCT (Discrete Cosine Transform) dengan penerapan kompresi video (H.264 / H.265)
- Baca lebih lengkap di: <https://medium.com/pallycon/how-netflix-protects-contents-part-2-33c1b60002a3>

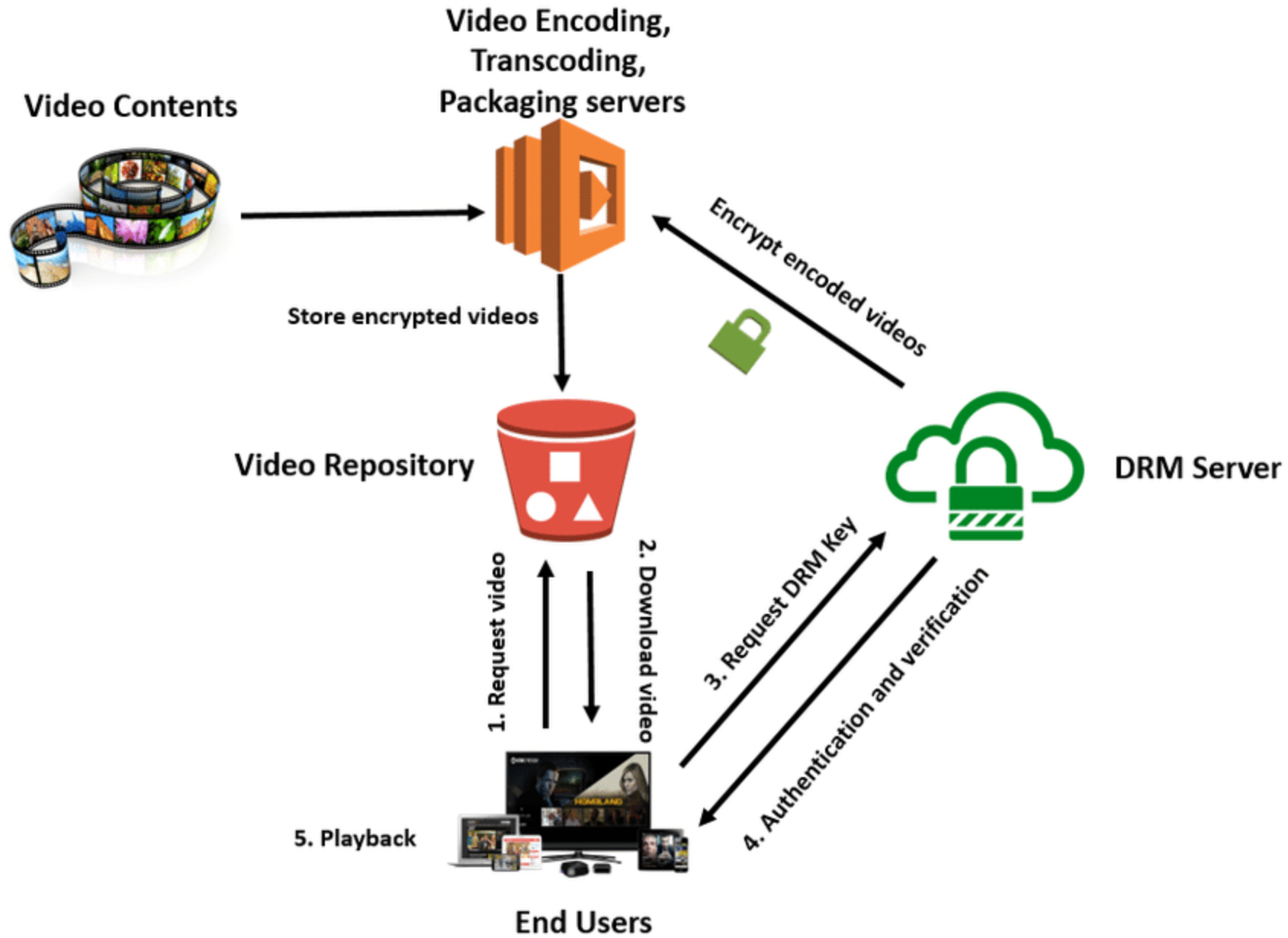
Digital Right Management (DRM)

- DRM (*Digital Rights Management*) adalah teknologi untuk mengontrol akses dan penggunaan konten digital seperti film, musik, e-book, dan software agar hanya bisa digunakan sesuai izin pemilik hak cipta.
- DRM = sistem pengamanan berbasis enkripsi + kontrol lisensi
- DRM digunakan untuk:
 - Mencegah pembajakan
 - Membatasi siapa yang boleh mengakses konten
 - Membatasi perangkat yang boleh memutar konten
 - Mengatur durasi akses (misalnya sewa 48 jam)

Cara Kerja DRM

Secara umum prosesnya seperti ini:

- **Konten dienkrupsi**
Video atau file tidak disimpan dalam bentuk asli, tapi sudah terenkrupsi.
- **User login & verifikasi lisensi**
Saat menekan tombol play:
 - Aplikasi meminta lisensi ke server DRM.
 - Server memverifikasi akun & hak akses.
- **Kunci dekripsi dikirim secara aman**
Jika valid, sistem mengirimkan *decryption key*.
- **Konten didekripsi di perangkat**
Biasanya dilakukan dalam *secure environment (Trusted Execution Environment)*.



- Beberapa DRM populer:
 - Widevine → digunakan oleh Netflix, YouTube
 - PlayReady → banyak dipakai Windows ecosystem
 - FairPlay → digunakan Apple
- Di platform seperti Netflix, video tidak pernah dikirim dalam bentuk mentah. Semua stream terenkripsi. Hanya perangkat yang lolos verifikasi DRM yang bisa memutar.
- Kalau file video diunduh langsung dari server tanpa lisensi:
 - file tetap tidak bisa diputar karena terenkripsi.

- Watermarking di Netflix bekerjasama dengan sistem DRM (*Digital Right Management*) seperti *Widevine* (Google), *PlayReady* (Microsoft), *FairPlay* (Apple)

- Perbedaan DRM dan watermarking,

DRM

- mencegah akses illegal
- berbasis enkripsi
- aktif saat streaming

Watermarking

- melacak sumber kebocoran/pembajakan
- berbasis penyisipan identitas
- watermark tetap ada walau video direkam

- Kenapa tidak cukup proteksi konten hanya dengan DRM? Karena DRM bisa dibypass, orang masih bisa merekam video pakai kamera. Saat perekaman terjadi, DRM tidak bisa lagi melindungi, tapi watermark masih bisa mengidentifikasi sumber kebocoran. Inilah alasan *forensic watermarking* sangat penting.



DRM **(Digital Rights Management)**

Encryption + Usage management
Prevents illegal use



**Complement
each other**



Forensic Watermarking

Inserts invisible user information
Tracks illegal distribution

TERIMA KASIH