

#21 WA TERMARK



Syahrul Imardi, MT

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Watermarking “Digital”





P21

MATAKULIAH KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

P21 : Watermarking “Digital”



Pengantar

Citra (*image*) atau Gambar

"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 mengandakan 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

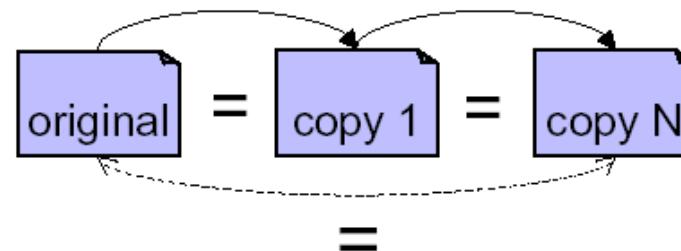
Foto mana yang asli?



(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*



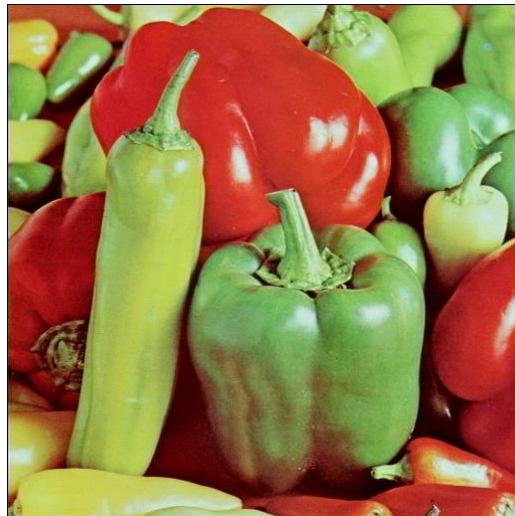
Tidak ada perlindungan terhadap citra digital!!!!

Solusi untuk masalah perlindungan citra di atas adalah:

Image Watermarking!!!!!

Image Watermarking

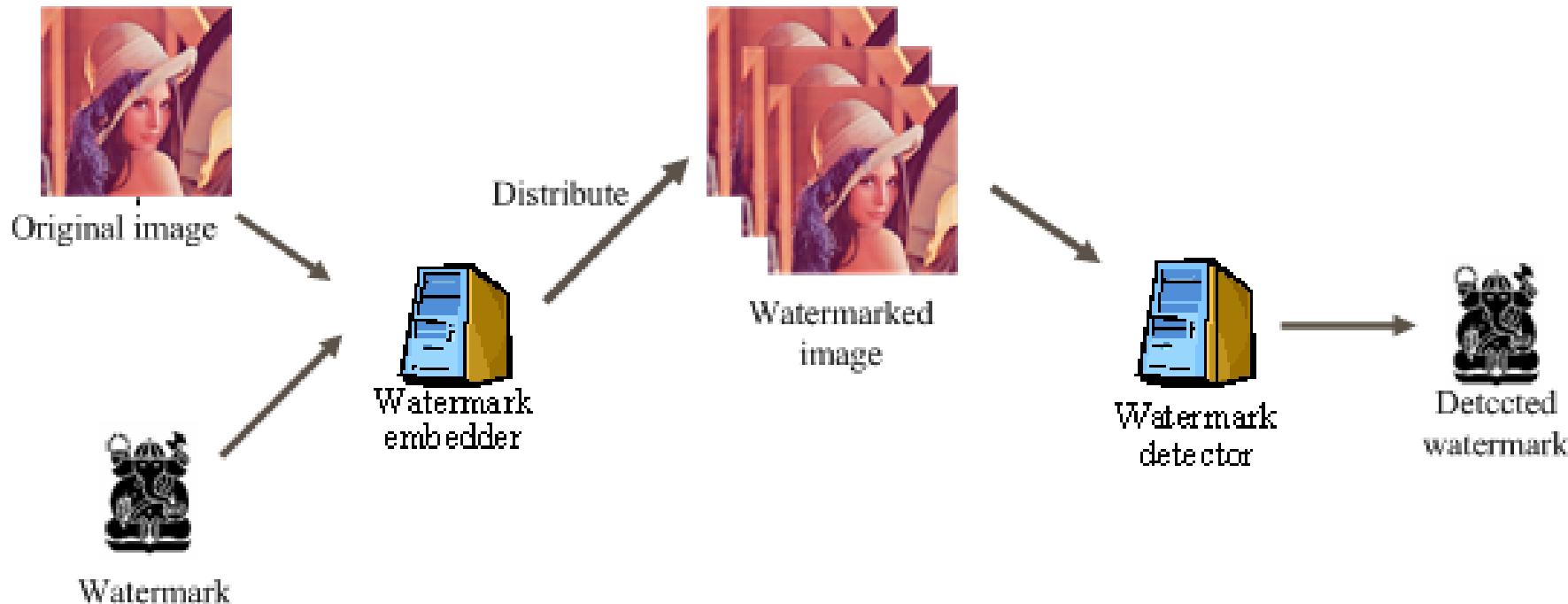
- *Image Watermarking*: teknik menyisipkan informasi yang mengacu pada pemilik gambar (disebut *watermark*) untuk tujuan melindungi kepemilikan, *copyright* atau menjaga keaslian konten
- *Watermark*: teks, gambar logo, audio, data biner (+1/-1), barisan bilangan riil
- Penyisipan *watermark* ke dalam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

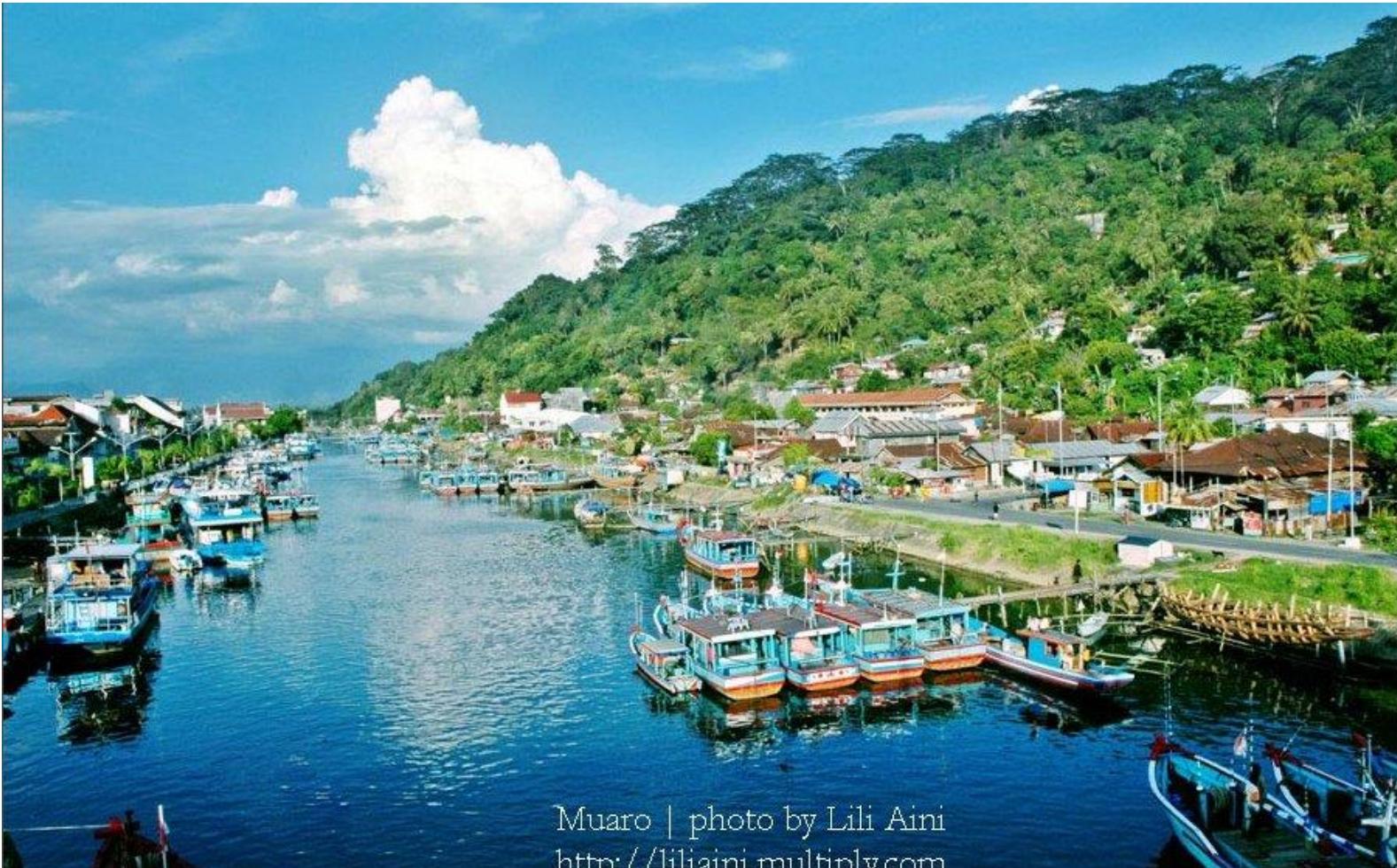
- Label *copyright* ditempelkan pada gambar.
- Kelemahan: tidak efektif melindungi *copyright* sebab label bisa dipotong atau dibuang dengan program pengolahan citra komersil (ex: *Adobe Photoshop*).



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 dibubuh tanda-air dijadikan identifikasi bahwa karya seni di atasnya adalah asli.
- Bangsa Cina melakukan hal yang sama pada pencetakan kertas

三、美術合作成果期

3.1 美術巡展板單之美術類電子教材軟體工具導讀

随着多媒体技术及网络的发展，图像已经形成了视觉上的革命，虚拟现实与电子书，许多闪光灯及黑白相片的外表，有些文字竟带有自然美的映像功能（最著名的要数毕加索），映像者等不同的效果，但是似乎有注意到是莫奈的，树叶漂浮在绿色背景上所画的风格方法。最后加入爱丽丝梦游仙境图像是，很多观众最喜欢观看，所以这本书被称作是爱丽丝梦游仙境大冒险，从这些就能知道他所画的都是什么，此外对於外孙们来说是一本充满想象色彩的书籍，适合人们阅读并享受快乐，最主要的是教育意义很大。

首先这个软件叫做易看秀，它有提供许多种工具，主要分为三个部分看板设计，图片编辑和音乐制作。还有一个叫做WWW的，就是让自己的网页（Blog）能够通过互联网上发布出去，能够让更多的朋友看到你的作品，而且还能通过电子邮件的形式发送到读者手中，是随处可见的材料制作，并且有美丽的模板可供选择。本系统将支持多国语言（目前有简体中文和英文两种），并且支持多种类型的文件转换和编辑的功能。

一般所说的电子书，是指有声读物或电子出版物的统称，包括电子书和有声读物两大类，也就是说必须有声音的扫描，所以也就有了计算机（电脑）系统，然后将文字输入到扫描仪中进行识别，从而将文本读出来，变成语音输出。对于有声读物，李克勤是绝对的爱好者，李泽厚也是他的爱好者，另外还有王菲，王力宏，周杰伦，张学友，等等都是他的爱好者。就如同学李晓东家里面有一台，所以经常用到他的工具，赵英利和我提过许多关于文字处理工具，赵英利告诉我学生可用得非常好的。

本书除了语音合成器以外，其他形式会话系统和数据压缩（JPEG）都有涉及，利用 Java 技术实现在线语音合成系统，主要是利用语音合成引擎的后台处理，主要采用的语音识别率不高，只能达到 90%左右，以上的人识别度及识别率都很好，主要音质卡的综合语音合成引擎，是将语音合成引擎结合（除了语音识别之外，主要识别率是语音识别率，而且语音合成质量也很高）。

Klasifikasi Watermarking

1. *Paper watermarking*

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

“Cannot be photocopied or scanned effectively”

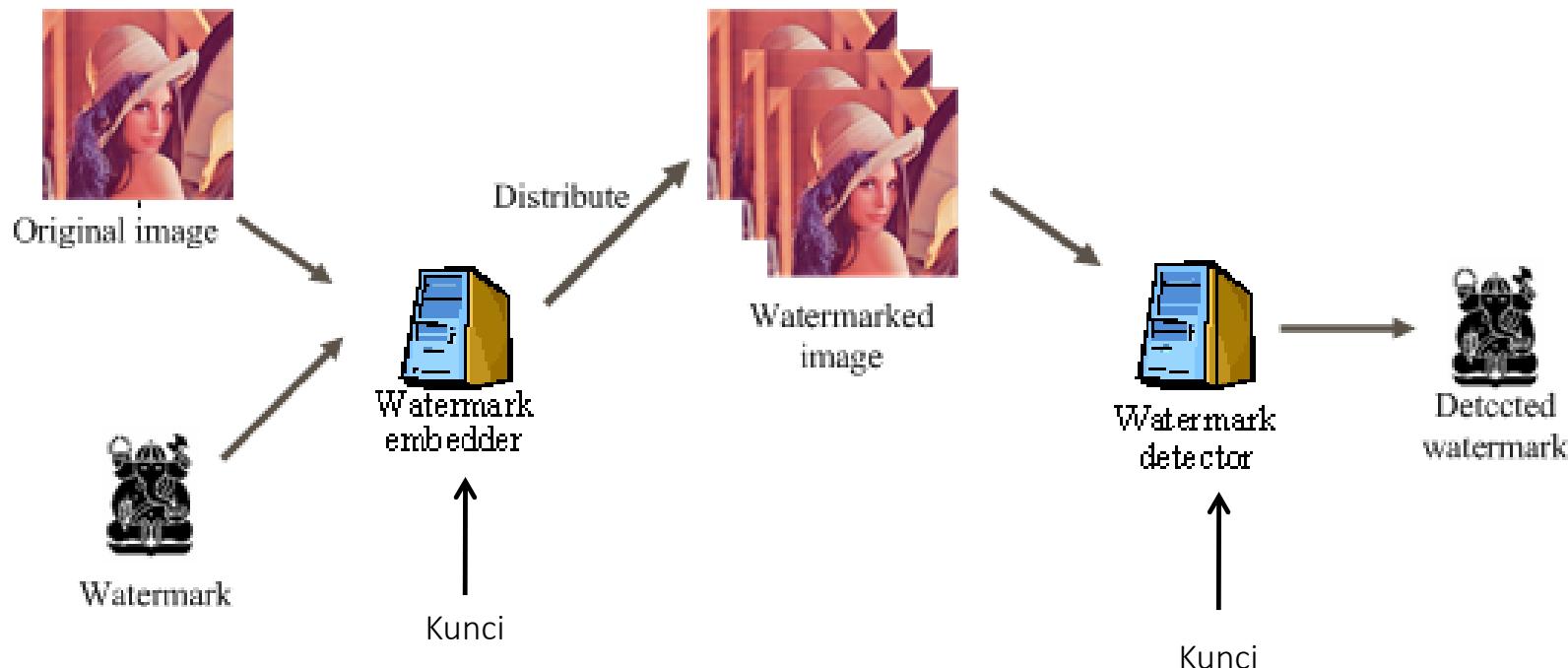
Tujuan: Identifikasi keaslian (otentikasi)

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*) yang tidak dapat dibedakan dengan citra aslinya.



Klasifikasi *Image Watermarking*

- ***Fragile watermarking***

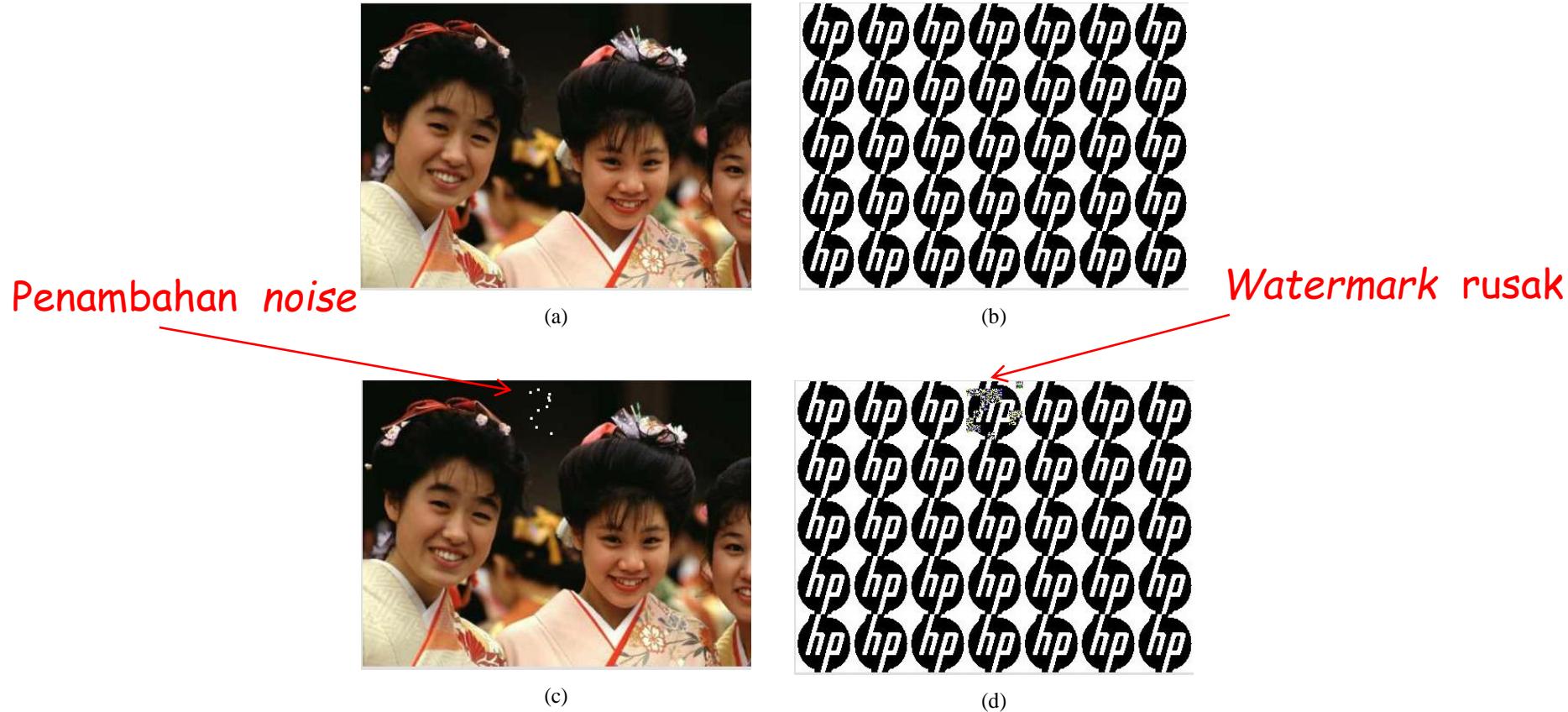
Tujuan: untuk menjaga integritas/orisinilitas citra digital.

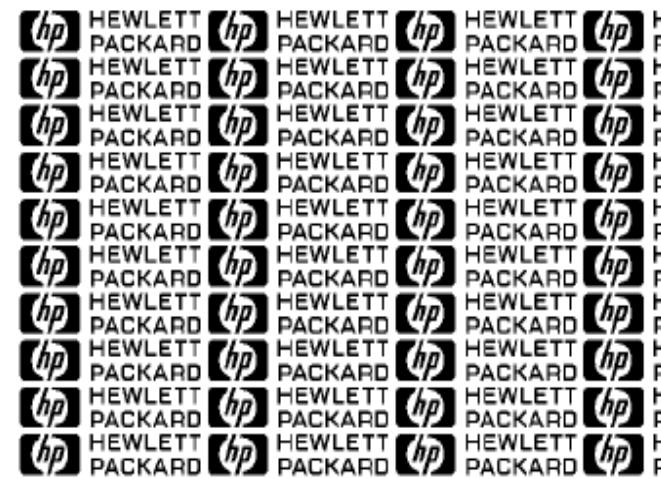
- ***Robust watermarking***

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?

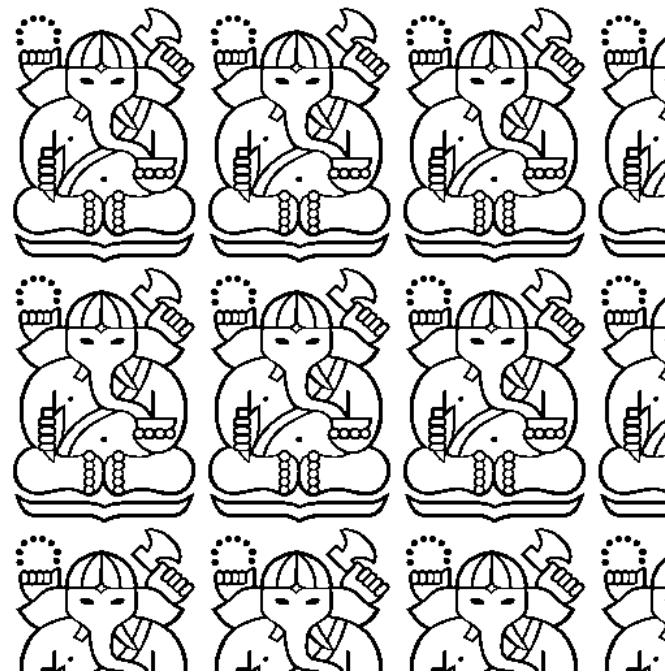
- Pertama, harus mengerti dulu konsep citra digital (sudah dijelaskan di dalam materi Steganografi)
- Kedua, mengerti metode LSB (sudah dijelaskan di dalam materi Steganografi)

Algoritma *Fragile Watermarking*

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



Citra asli

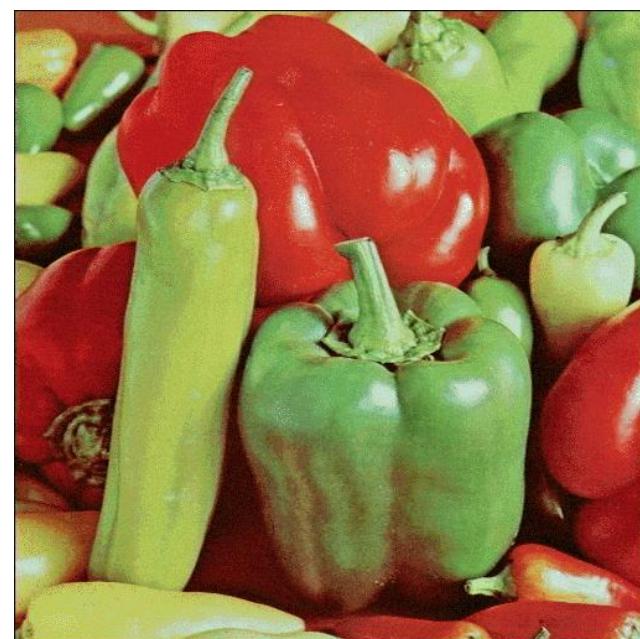


watermark

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

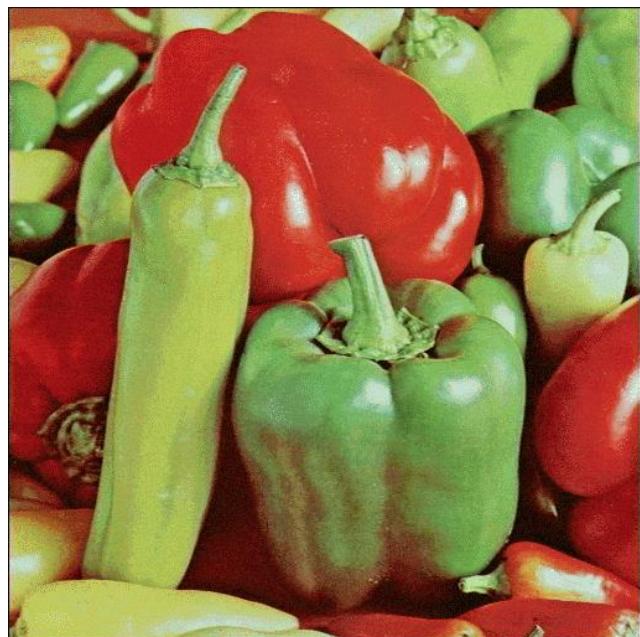


Citra asli

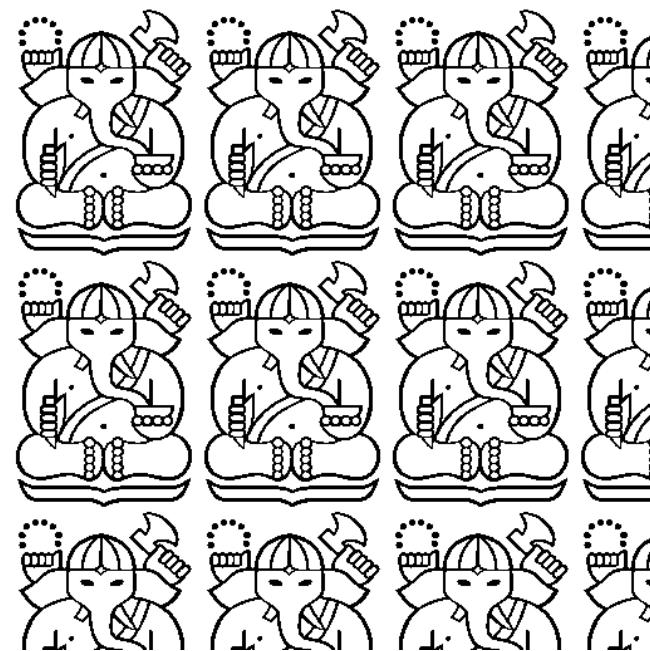


Citra ber-watermark

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



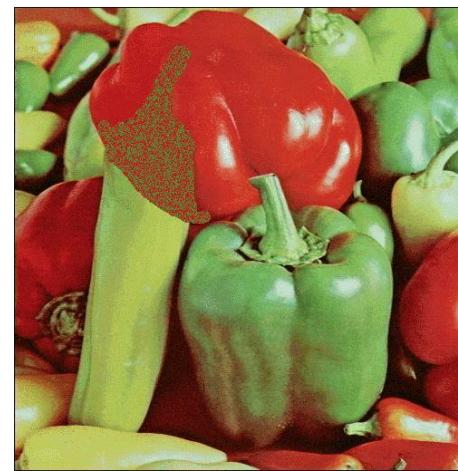
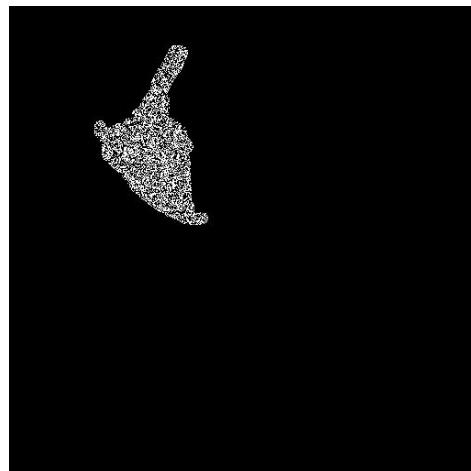
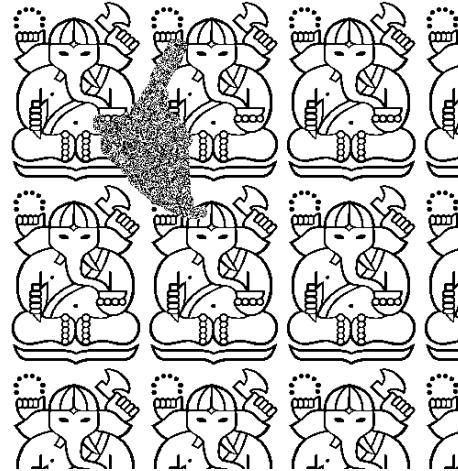
Citra ber-watermark



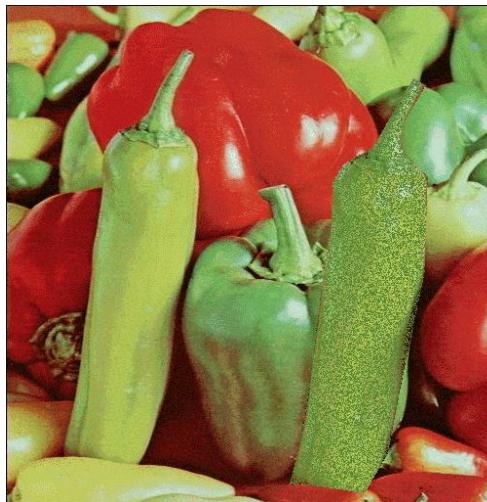
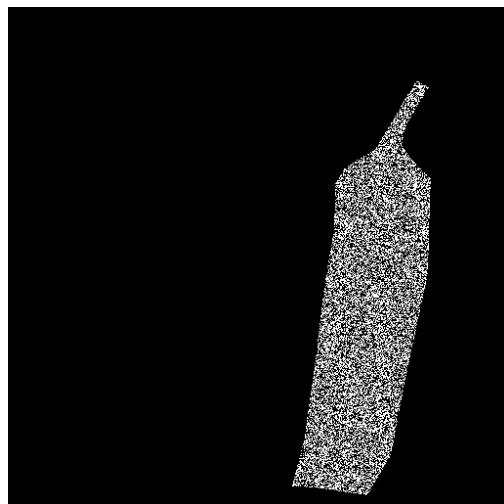
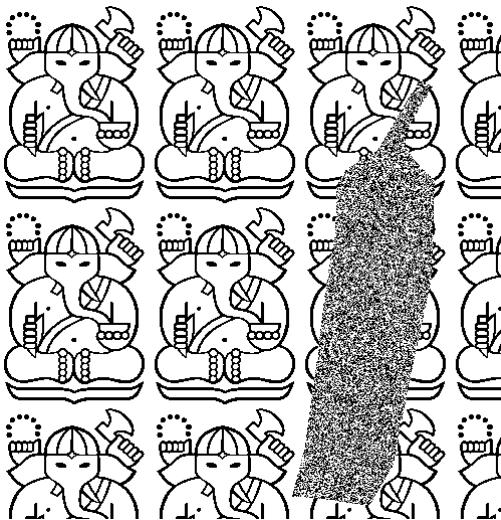
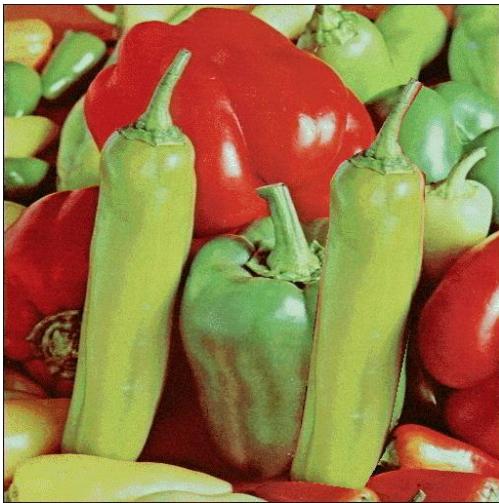
Watermark hasil ekstraksi

Test manipulasi pada citra ber-watermark

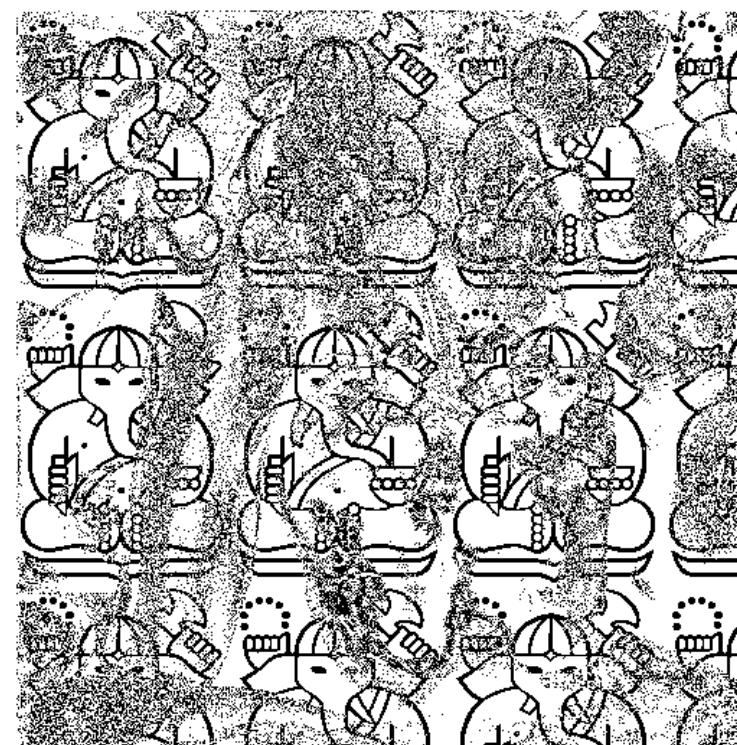
Deletion attack



Insertion attack

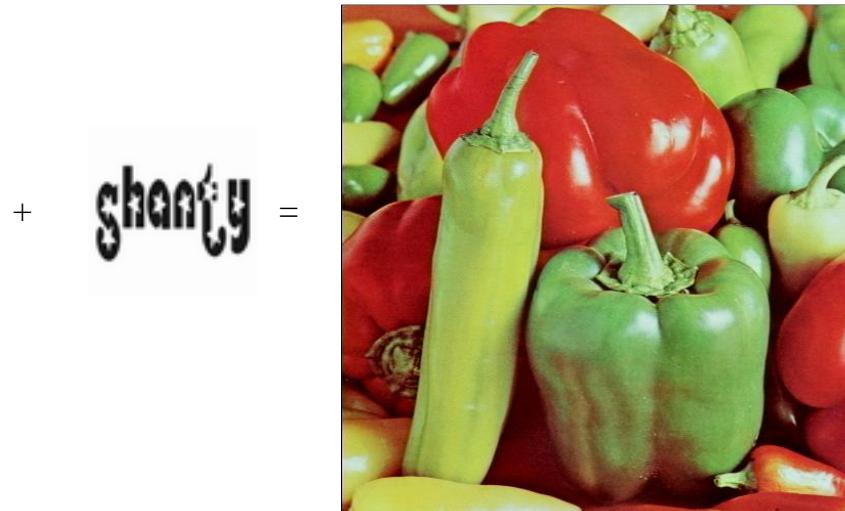
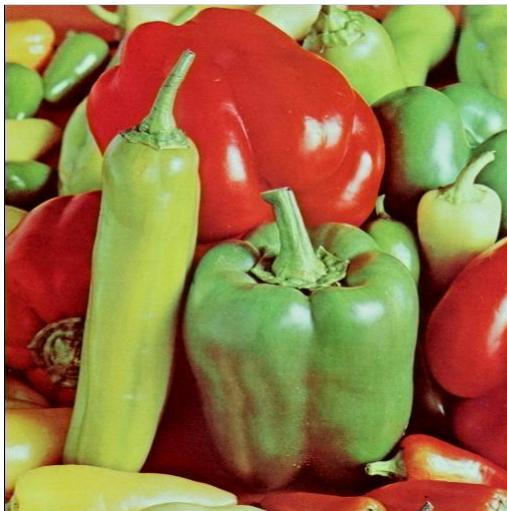


Brightness and contrast attack

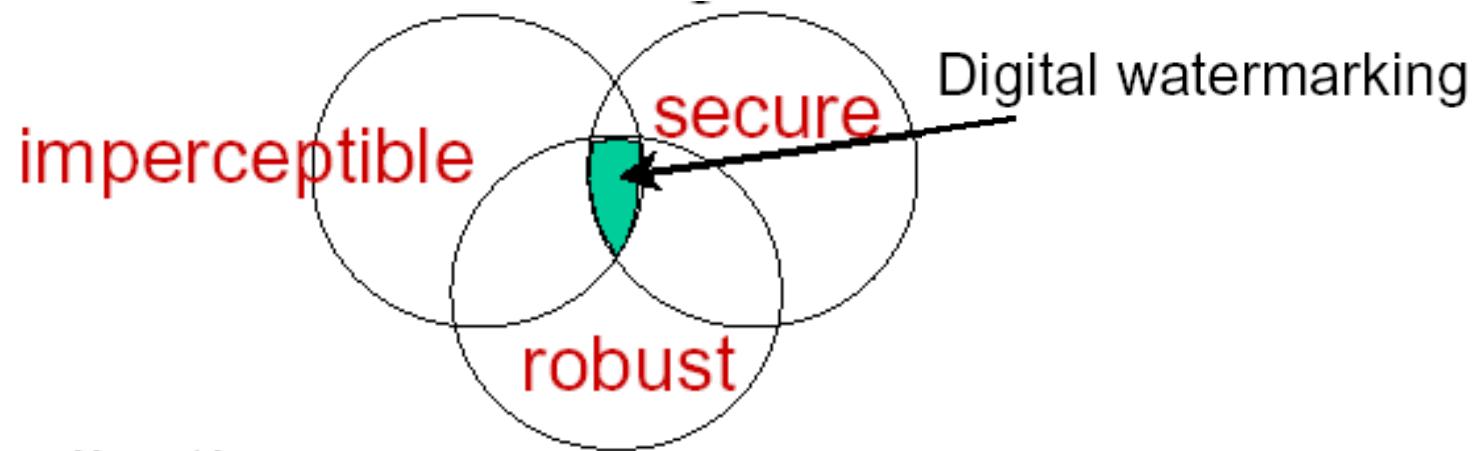


Robust Watermarking

- 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*

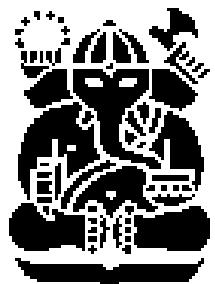




Original image



Watermarked image



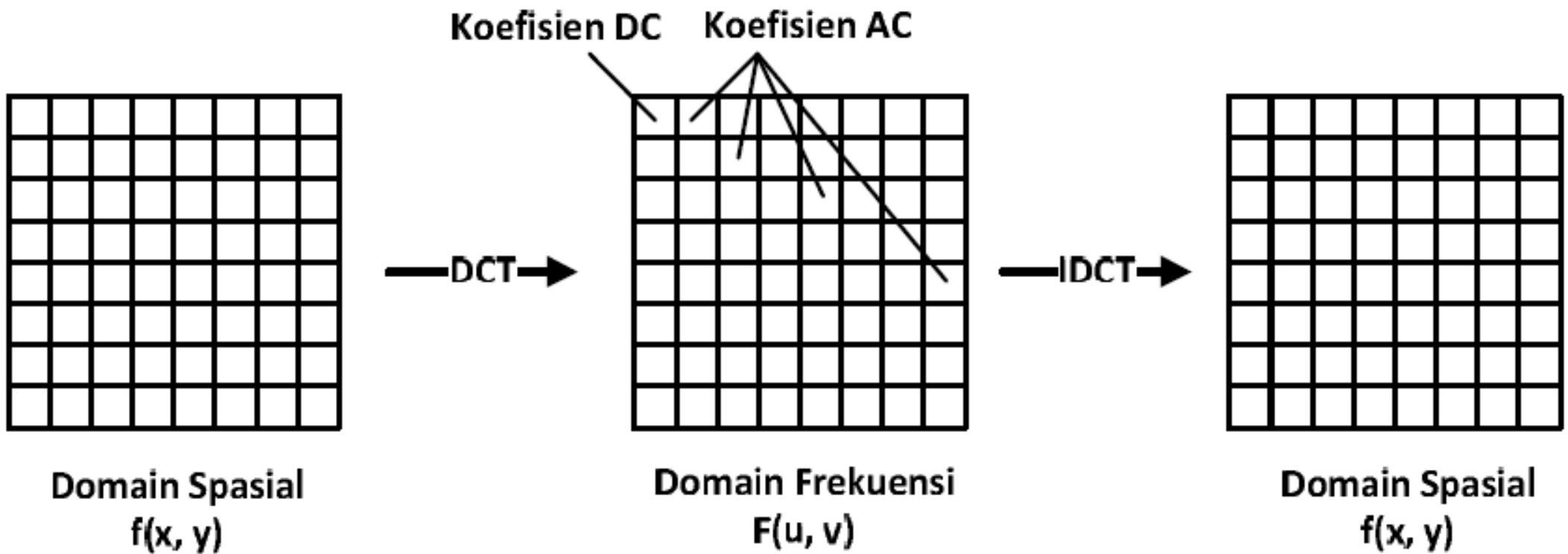
watermark



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*)



- *Discrete Cosine Transform (DCT)*

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

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

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

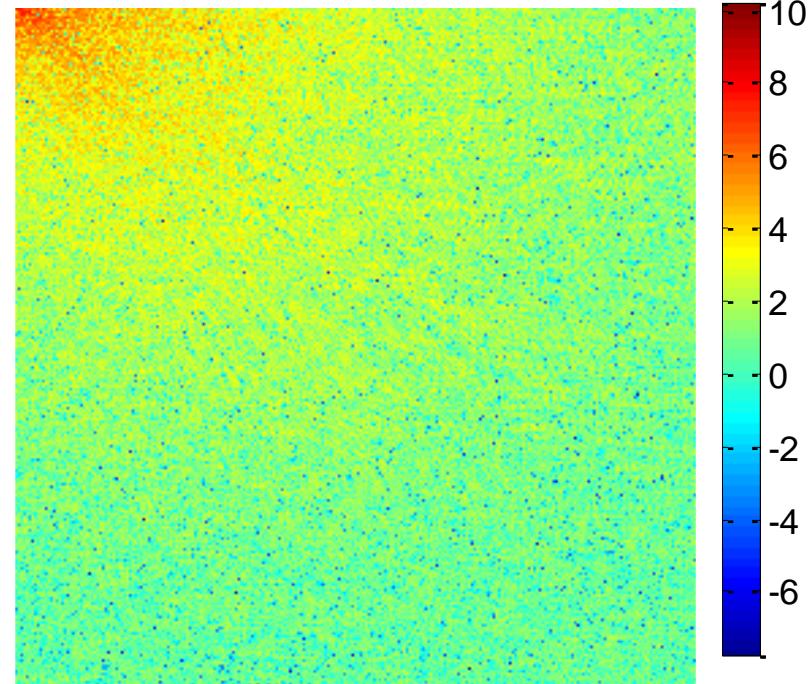
C(u,v) disebut koefisien-koefisien DCT

- *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

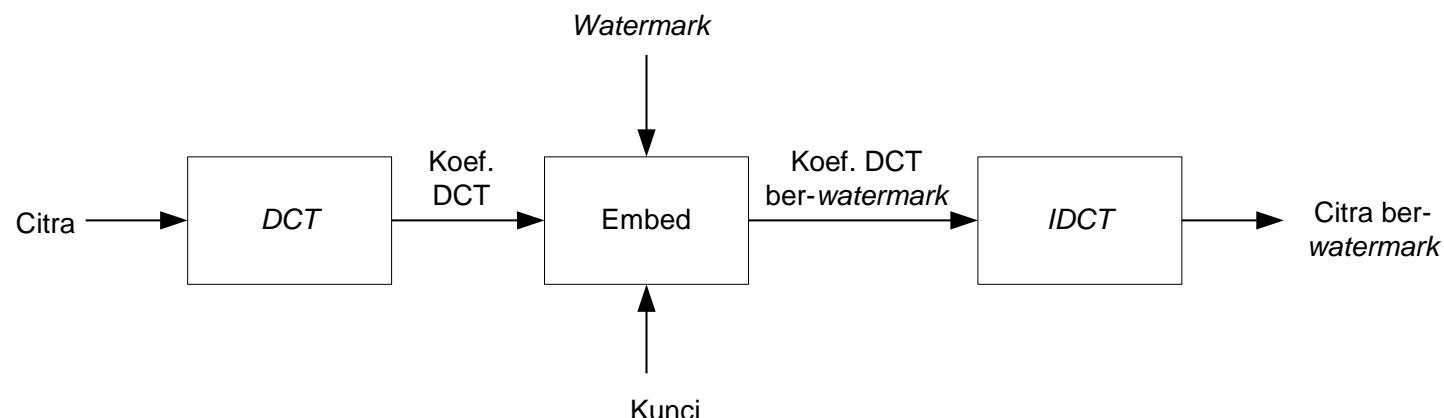


Citra dalam ranah frekuensi

- Hasil transformasi menghasilkan nilai-nilai yang disebut koefisien-koefisien transformasi (misalnya koefisien DCT).
- Bit-bit *watermark* (w) disembunyikan pada koefisien-koefisien transformasi (v) tersebut dengan suatu formula:

$$\hat{v}_i = v_i + w_i$$

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



Test ketahanan *watermark* terhadap manipulasi terhadap citra.

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



Original image



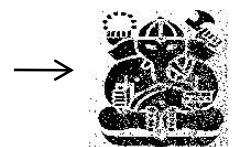
watermark



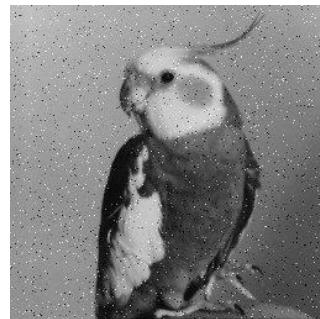
Watermarked image



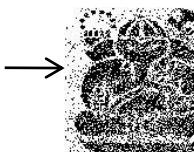
JPEG compression



Extracted watermark



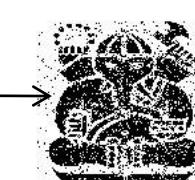
Noisy image



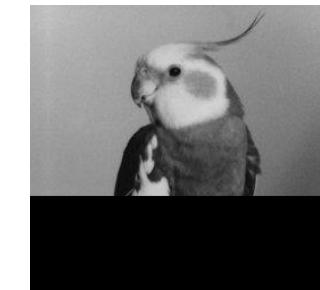
Extracted watermark



Resized image



Extracted watermark



Cropped image

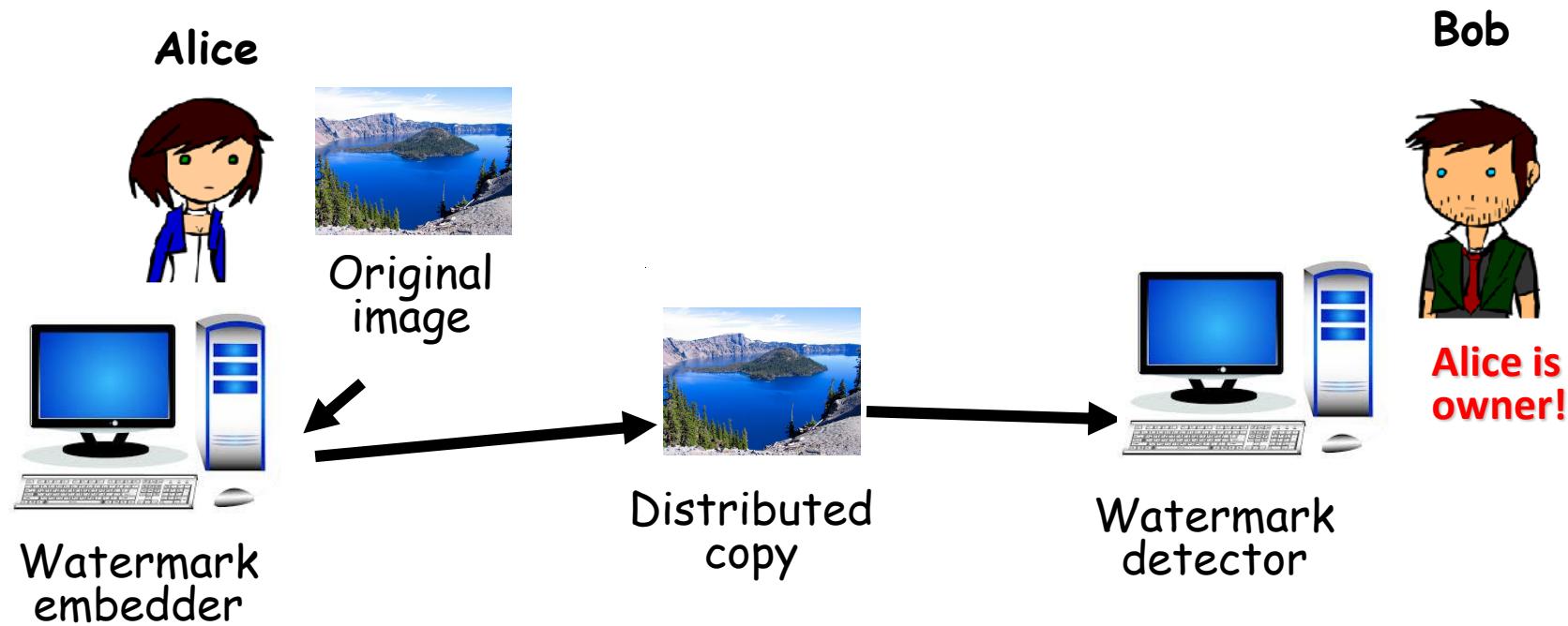


Extracted watermark

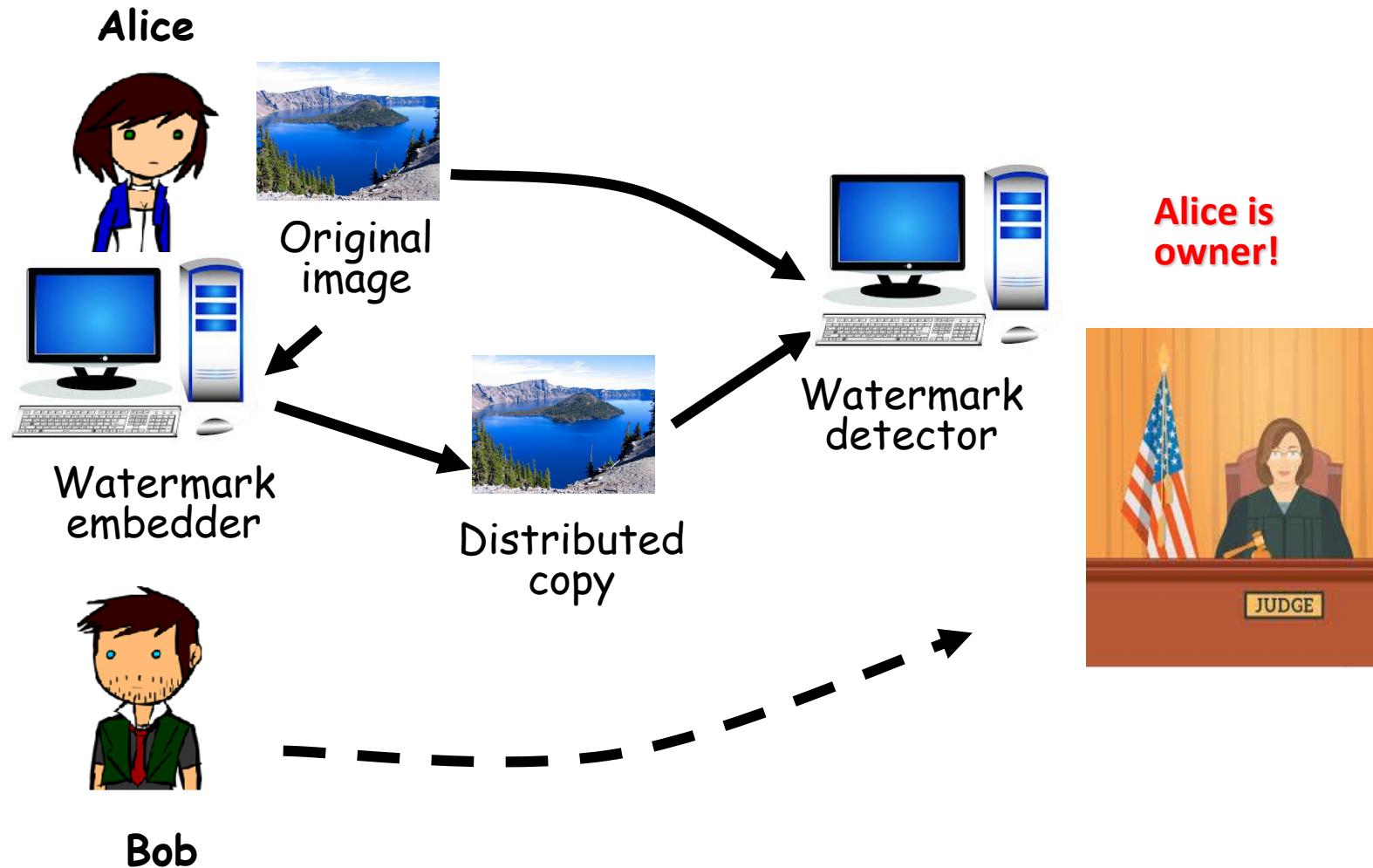
Aplikasi *Watermarking*

- 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*

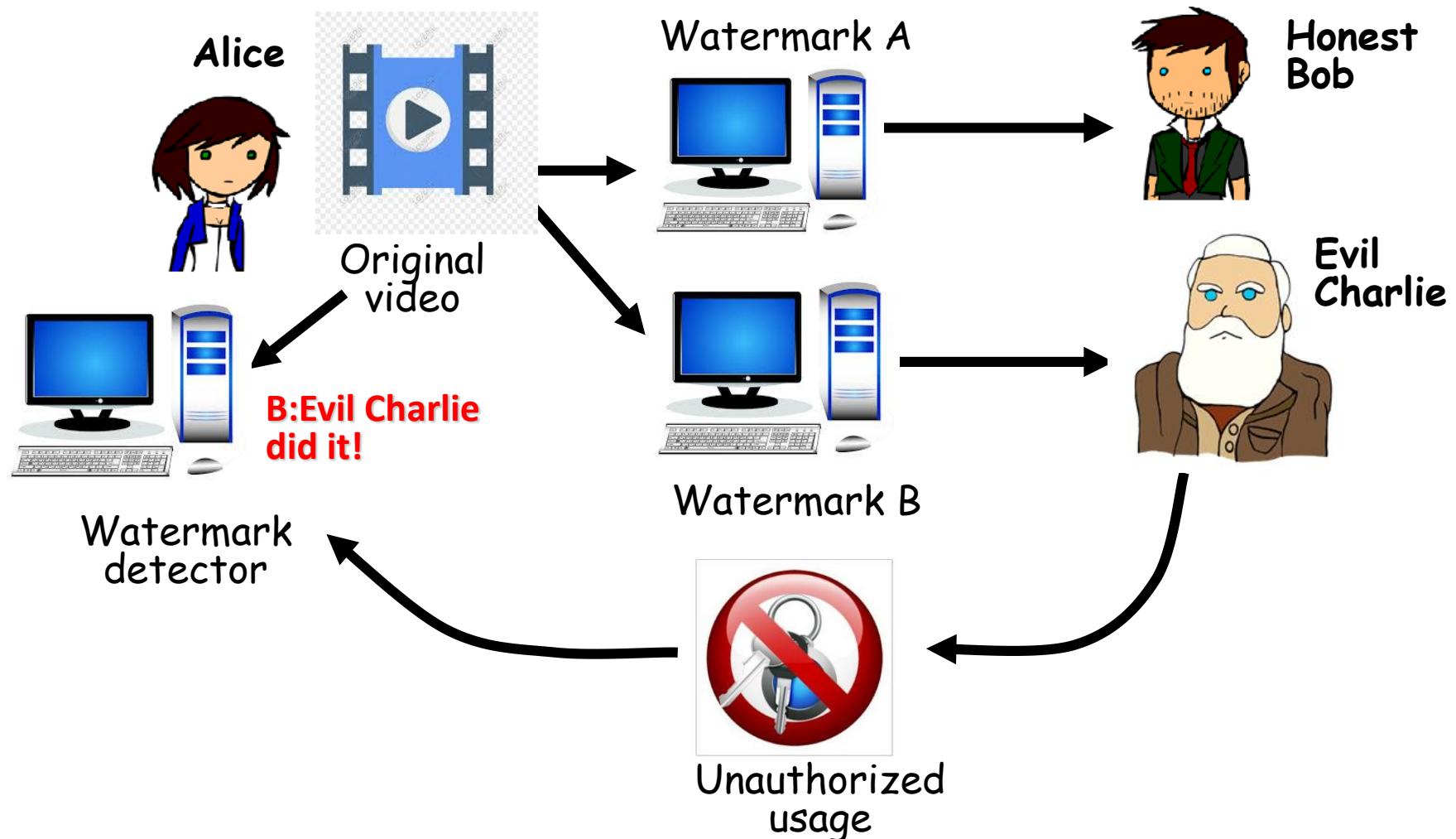
Aplikasi watermarking: *Owner identification*



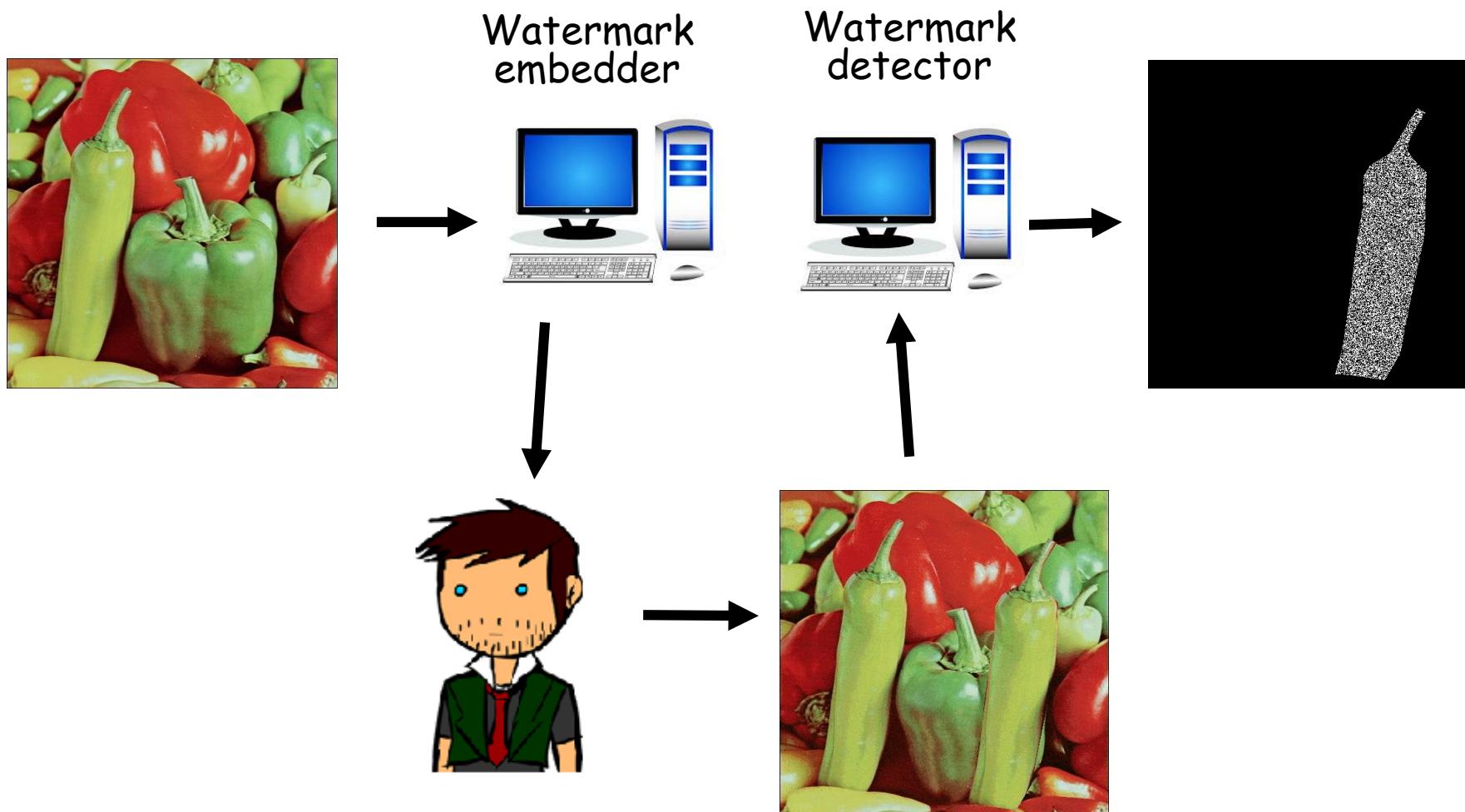
Aplikasi watermarking: *Proof of ownership*



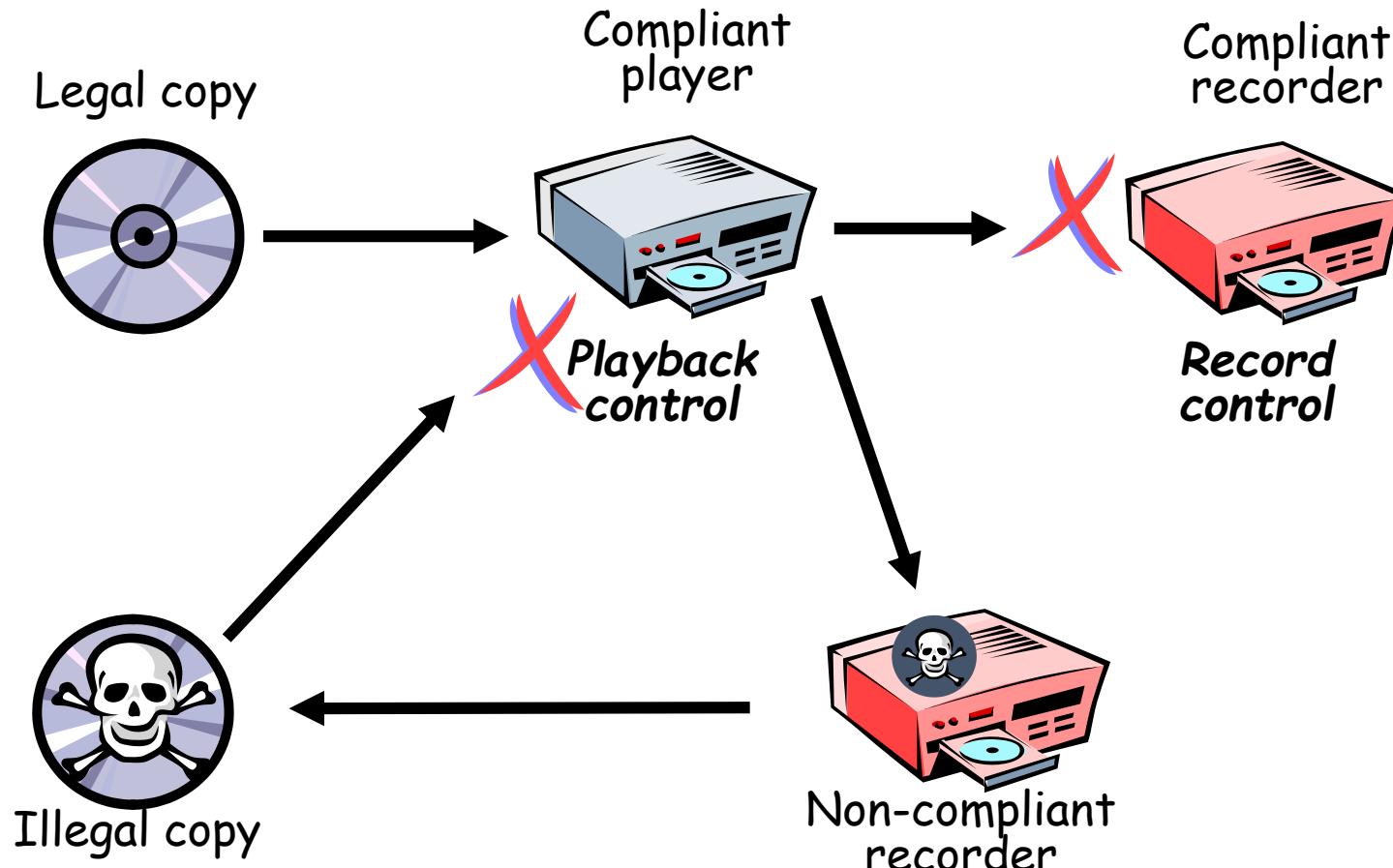
Aplikasi watermarking: *Transaction tracking/fingerprinting*



Aplikasi watermarking: *Content authentication*

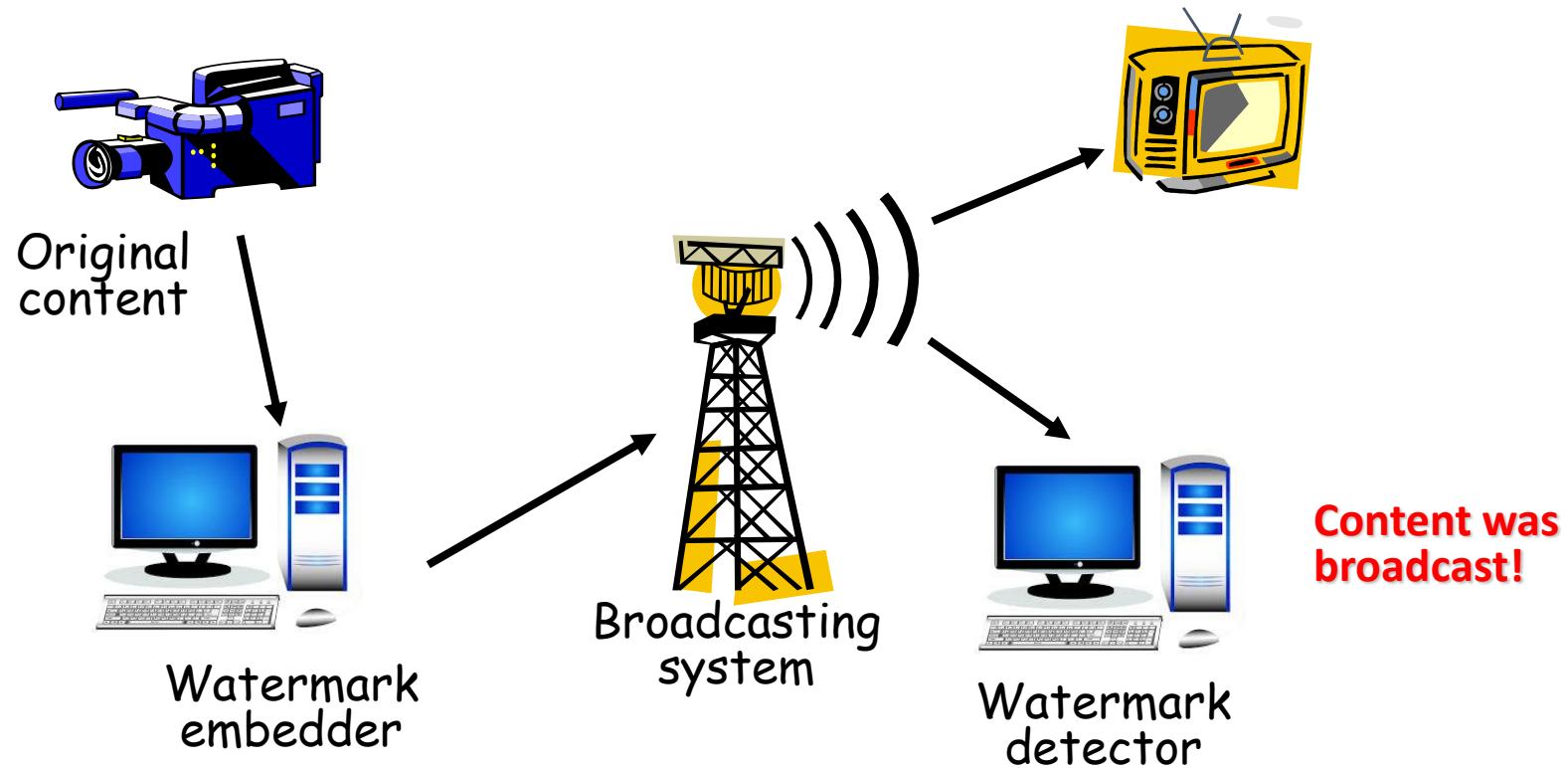


Aplikasi watermarking: *Copy control/Piracy Control*



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.

Referensi utama :

- >> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.
- >> Nancy R. Mead, Carol Woody - Cyber Security Engineering_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)
- >> James Helfrich - Security for Software Engineers-CRC Press (2019)
- >> Pete Loshin - Simple Steps to Data Encryption_ A Practical Guide to Secure Computing-Syngress (2013)
- >> Tevfik Bultan,Fang Yu,Muath Alkhalaif,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017)



Ada pertanyaan?

