KEAMANAN JARINGAN

Jaringan Komputer

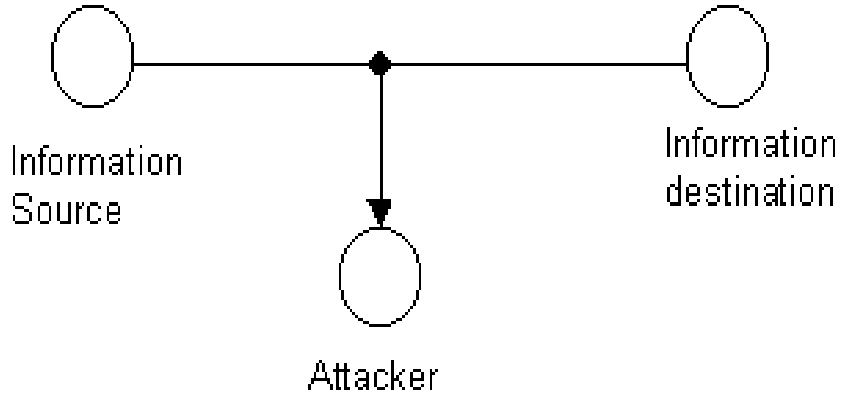
- Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar.
- Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

- Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan.

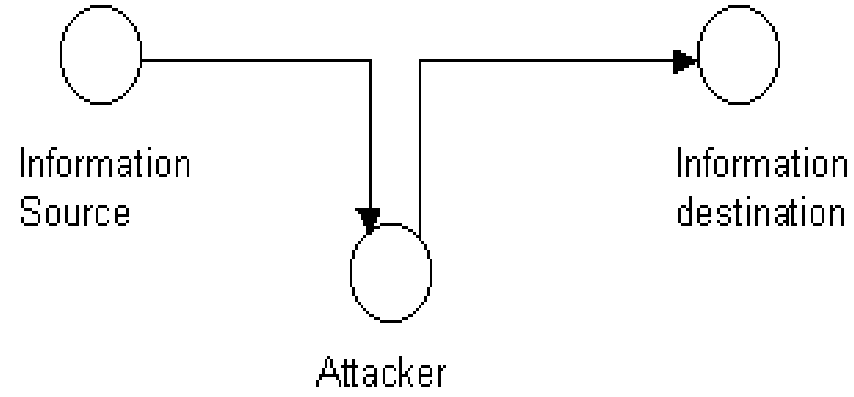
Tipe *Threat*

- Terdapat dua kategori threat yaitu

  threat pasif dan *threat* aktif.
- *Threat* pasif melakukan pemantauan dan atau perekaman data selama data ditranmisikan lewat fasilitas komunikasi. Tujuan penyerang adalah untuk mendapatkan informasi yang sedang dikirimkan.
- *Threat* aktif merupakan pengguna gelap suatu peralatan terhubung fasilitas komunikasi untuk mengubah transmisi data atau mengubah isyarat kendali atau memunculkan data atau isyarat kendali palsu.



(a) Threat pasif



(b) Threat aktif

Internet Threat Level

- Celah-celah keamanan sistem internet, dapat disusun dalam skala klasifikasi.
- Skala klasifikasi ini disebut dengan istilah skala Internet Threat Level atau skala ITL. Ancaman terendah digolongkan dalam ITL kelas 0, sedangkan ancaman tertinggi digolongkan dalam ITL kelas 9.
- Tabel berikut menjelaskan masing-masing kelas ITL.

- Kebanyakan permasalahan keamanan dapat diklasifikasikan ke dalam 3 kategori utama, tergantung pada kerumitan perilaku ancaman kepada sistem sasaran, yaitu :
  - Ancaman-ancaman lokal.
  - Ancaman-ancaman remote
  - Ancaman-ancaman dari lintas firewall

- Selanjutnya klasifikasi ini dapat dipisah dalam derajat yang lebih rinci, yaitu :
  - *Read access*
  - *Non-root write and execution access*
  - *Root write and execution access*

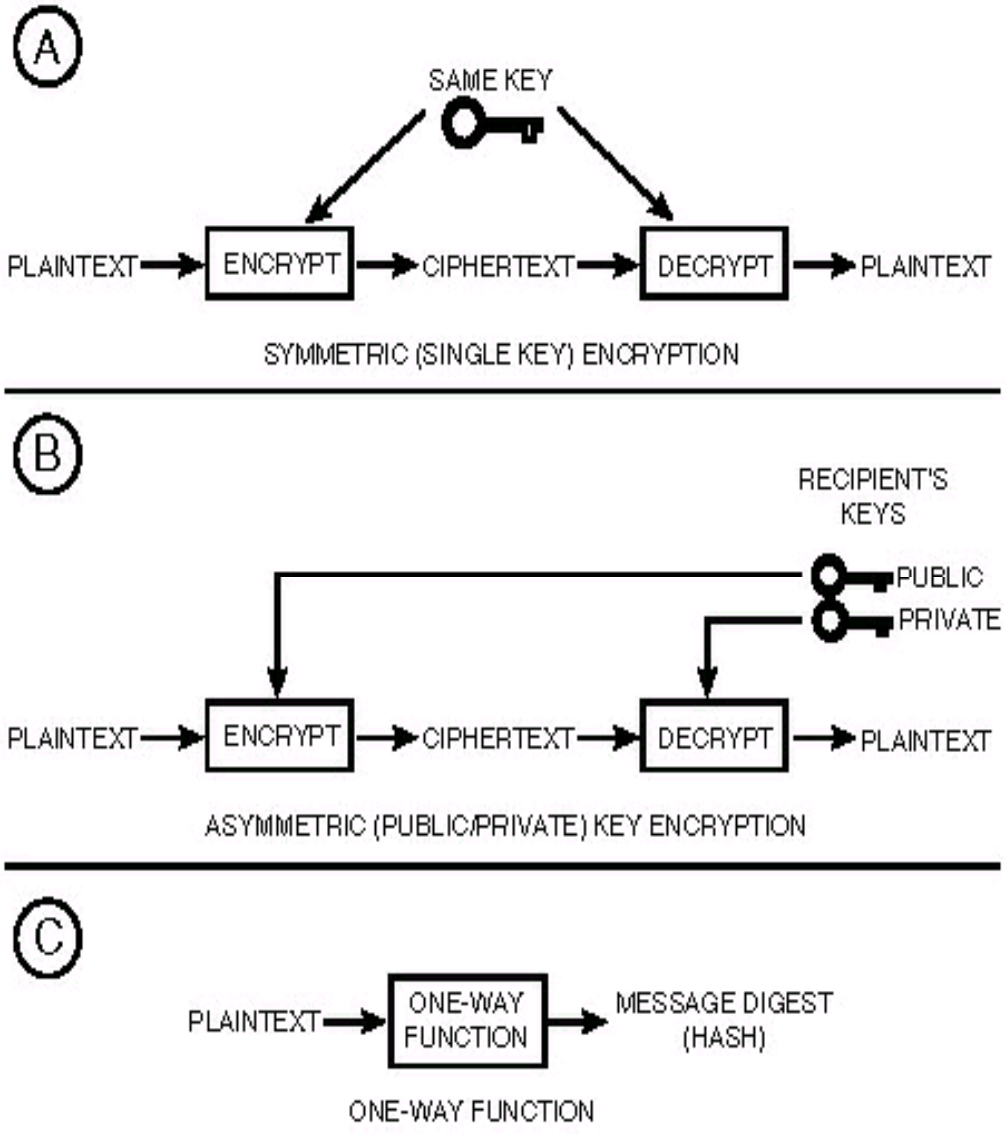
Kelas	Penjelasan
0	Denial of service attack—users are unable to access files or programs.
1	Local users can gain read access to files on the local system.
2	Local users can gain write and/or execution access to non–root-owned files on the system.
3	Local users can gain write and/or execution access to root-owned files on the system.
4	Remote users on the same network can gain read access to files on the system or transmitted over the network.
5	Remote users on the same network can gain write and/or execution access to non–root-owned files on the system or transmitted over the network.
6	Remote users on the same network can gain write and/or execution access to root-owned files on the system.
7	Remote users across a firewall can gain read access to files on the system or transmitted over the network.
8	Remote users across a firewall can gain write and/or execution access to non–root-owned files on the system or transmitted over the network.
9	Remote users across a firewall can gain write and/or execution access to root-owned files on the system.

- Seberapa besar tingkat ancaman dapat diukur dengan melihat beberapa faktor, antara lain :
  - Kegunaan sistem
  - Kerahasiaan data dalam sistem.
  - Tingkat kepetingan dari integritas data
  - Kepentingan untuk menjaga akses yang tidak boleh terputus
  - Profil pengguna
  - Hubungan antara sistem dengan sistem yang lain.

Kriptography

- Setiap orang bahwa ketika dikehendaki untuk menyimpan sesuatu secara pribadi, maka kita harus menyembunyikan agar orang lain tidak tahu. Sebagai misal ketika kita megirim surat kepada seseorang, maka kita membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan surat tersebut agar tetap tidak secara mudah dibaca orang apabila amplop dibuka, maka kita mengupayakan untuk membuat mekanisme tertentu agar isi surat tidak secara mudah dipahami.

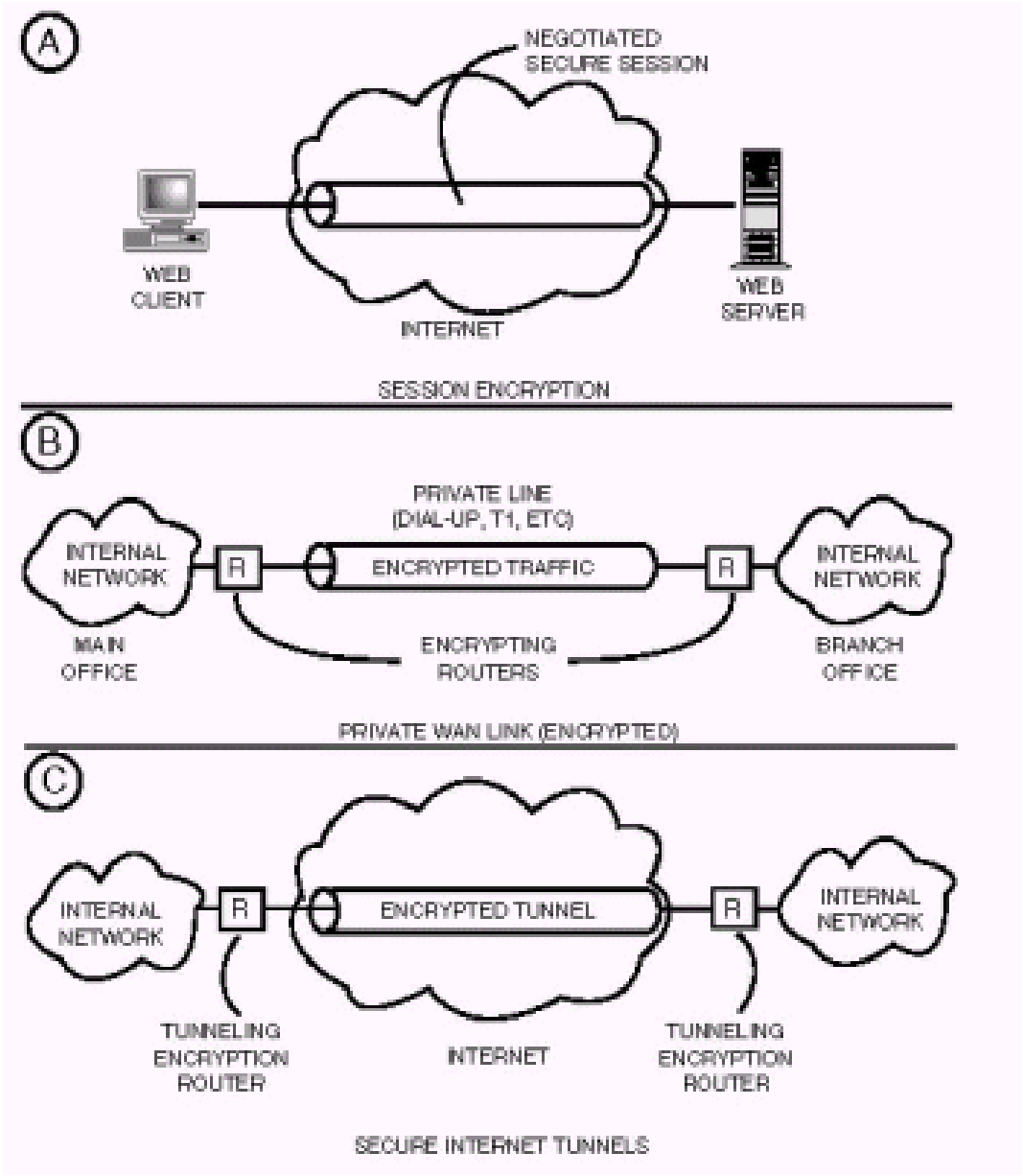
- Cara untuk membuat pesan tidak mudah terbaca adalah enkripsi. Dalam hal ini terdapat tiga kategori enkripsi antara lain :
  - Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk meng-enkripsi dan juga sekaligus men-dekripsi informasi.
  - Kunci enksripsi public, dalam hal ini dua kunci digunakan, satu untuk proses enkripsi dan yang lain untuk proses dekripsi.
  - Fungsi one-way, di mana informasi di-enkripsi untuk menciptakan “signature” dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.


A
SAME KEY
PLAINTEXT
ENCRYPT
CIPHERTEXT
DECRYPT
PLAINTEXT
SYMMETRIC (SINGLE KEY) ENCRYPTION
B
RECIPIENT'S KEYS
PUBLIC
PRIVATE
PLAINTEXT
ENCRYPT
CIPHERTEXT
DECRYPT
PLAINTEXT
ASYMMETRIC (PUBLIC/PRIVATE) KEY ENCRYPTION
C
PLAINTEXT
ONE-WAY FUNCTION
MESSAGE DIGEST (HASH)
ONE-WAY FUNCTION

- Enkripsi dibentuk dengan berdasarkan suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tak bisa dilihat.
- Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya.
- Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati yang harus secara efektif menghasilkan sebuah bentuk terenkripsi yang tidak bisa dikembalikan oleh seseorang bahkan sekalipun mereka memiliki algoritma yang sama.

- Tujuan dari sistem kriptografi adalah :
  - Confidentiality : memberikan kerahasiaan pesan dan menyimpan data dengan menyembuyikan informasi lewat teknik-teknik enkripsi.
  - Message Integrity : memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat samapai saat ia dibuka.
  - Non-repudiation : memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
  - Authentication : Memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia kan memasuki sebuah sistem.

- Dengan demikian menjadi jelas bahwa kriptografi dapat diterapkan dalam banyak bidang . Beberapa hal di antaranya :
  - Certificates (Digital IDs) .
  - Digital signatures.
  - Secure channels.


A
NEGOTIATED
SECURE SESSION
WEB
CLIENT
INTERNET
WEB
SERVER
SESSION ENCRYPTION
B
PRIVATE LINE
(DIAL-UP, T1, ETC)
INTERNAL
NETWORK
R
ENCRYPTED TRAFFIC
R
INTERNAL
NETWORK
MAIN
OFFICE
ENCRYPTING
ROUTERS
BRANCH
OFFICE
PRIVATE WAN LINK (ENCRYPTED)
C
INTERNAL
NETWORK
R
ENCRYPTED TUNNEL
R
INTERNAL
NETWORK
TUNNELING
ENCRYPTION
ROUTER
INTERNET
TUNNELING
ENCRYPTION
ROUTER
SECURE INTERNET TUNNELS

Contoh kriptography

Digital Signature

- *Watermark* dapat dianggap sebagai sidik 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.

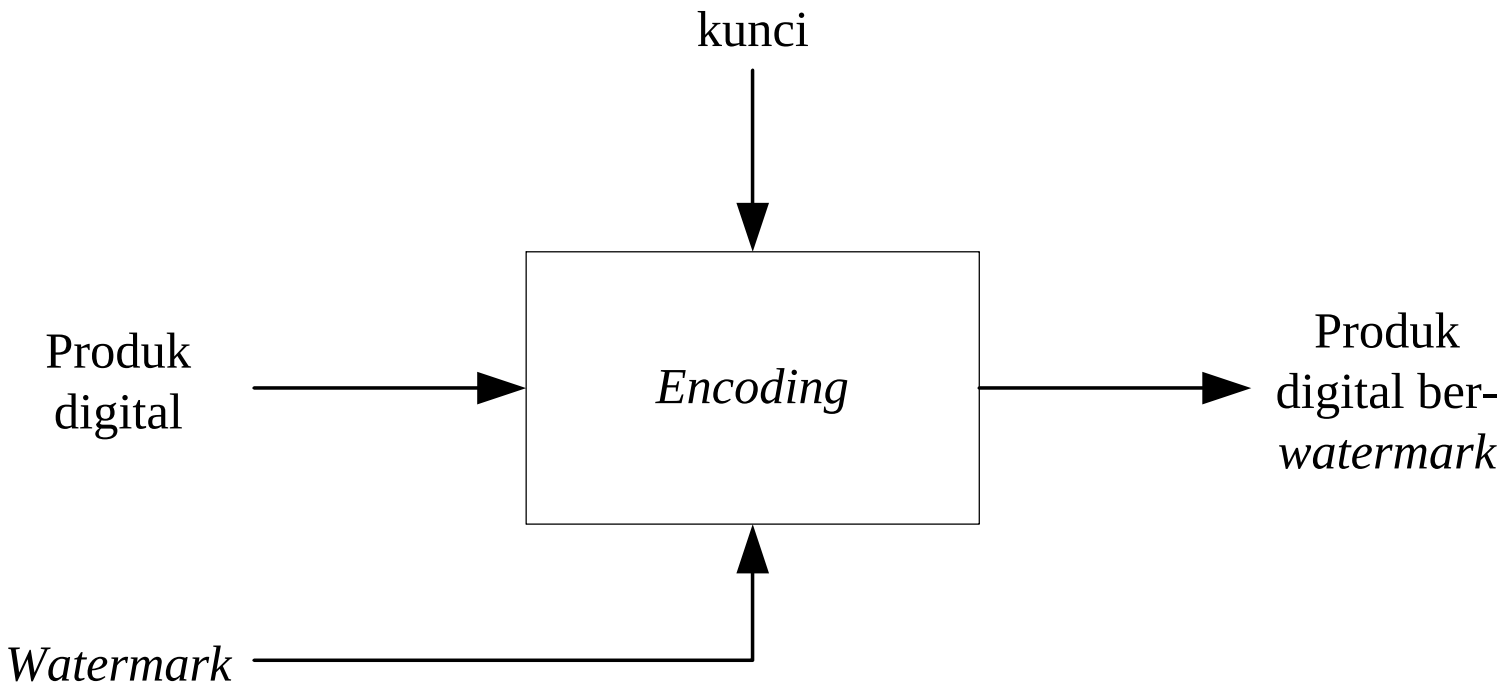
Sejarah *Watermarking*

- Abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* dengan cara menekan bentuk cetakan gambar pada kertas yang baru setengah jadi.

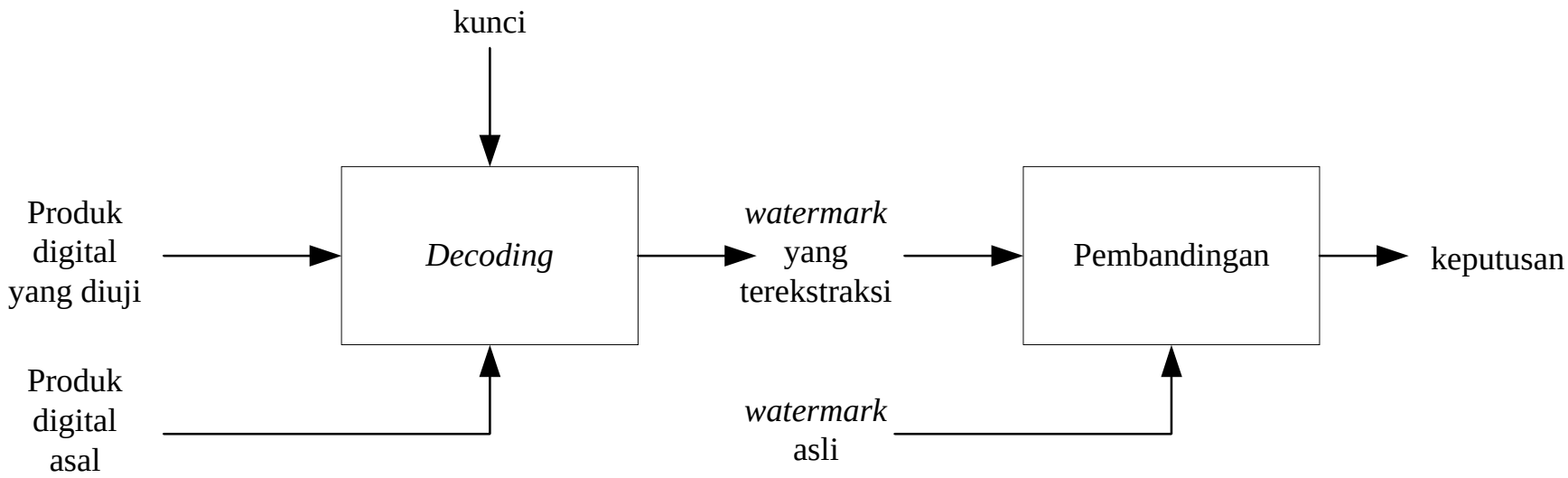
- Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas ini biasanya digunakan oleh seniman/sastrawan untuk menulis karya seni.

- Kertas yang sudah dibubuhi tanda-air dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

Penyisipan *Watermark* (*embedding*)



Verifikasi *Watermark*



- *Watermark* umumnya data audio atau gambar.

- *Watermark* berupa teks mengandung kelemahan karena kesalahan satu bit akan menghasilkan hasil teks yang berbeda pada waktu verifikasi (ektraksi).

Kegunaan *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).
- *Covert communication*: untuk sistem komunikasi di negara2 di mana kriptografi tidak dibolehkan.
- *Piracy protection*: mencegah penggandaan yang tidak berizin.

Jenis-jenis *Watermarking*

- *Image Watermarking*
- *Video Watermarking*
- *Audio Watermarking*
- *Text Watermarking*

Jenis-jenis *Watermarking*

- *Blind watermarking*

  Proses verifikasi watermark tidak membutuhkan media asal (yang belum diberri *watermark*)

- *Non-blind watermarking*

  Proses verifikasi *watermark* membutuhkan media asal

Jenis-jenis *Watermarking*

- *Fragile watermarking*

  Tujuan: untuk menjaga integritas/keorisinila data

- *Robust watermarking*

  Tujuan: untuk menyisipkan informasi kepemilikan

Jenis-jenis *Watermarking*

(khusus pada citra)

- *Visible Watermarking*
- *Invisible Watermarking*

Image Watermarking

- *Visible Watermarking*

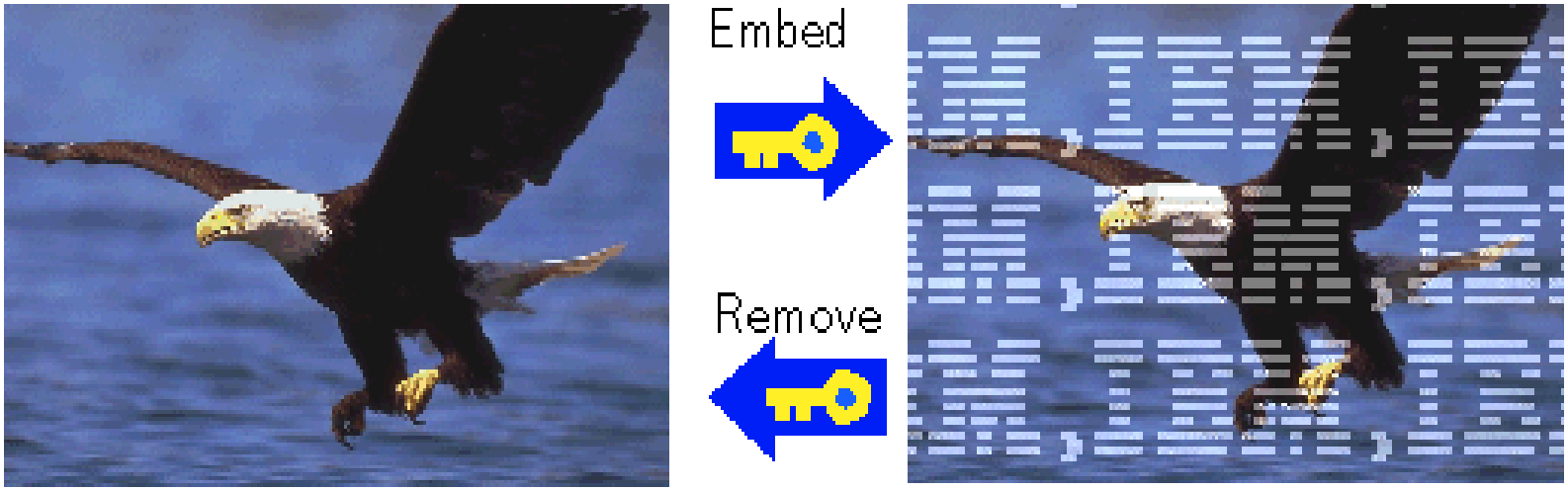
  (khusus untuk citra yang dicetak)

- *Invisible Watermarking*

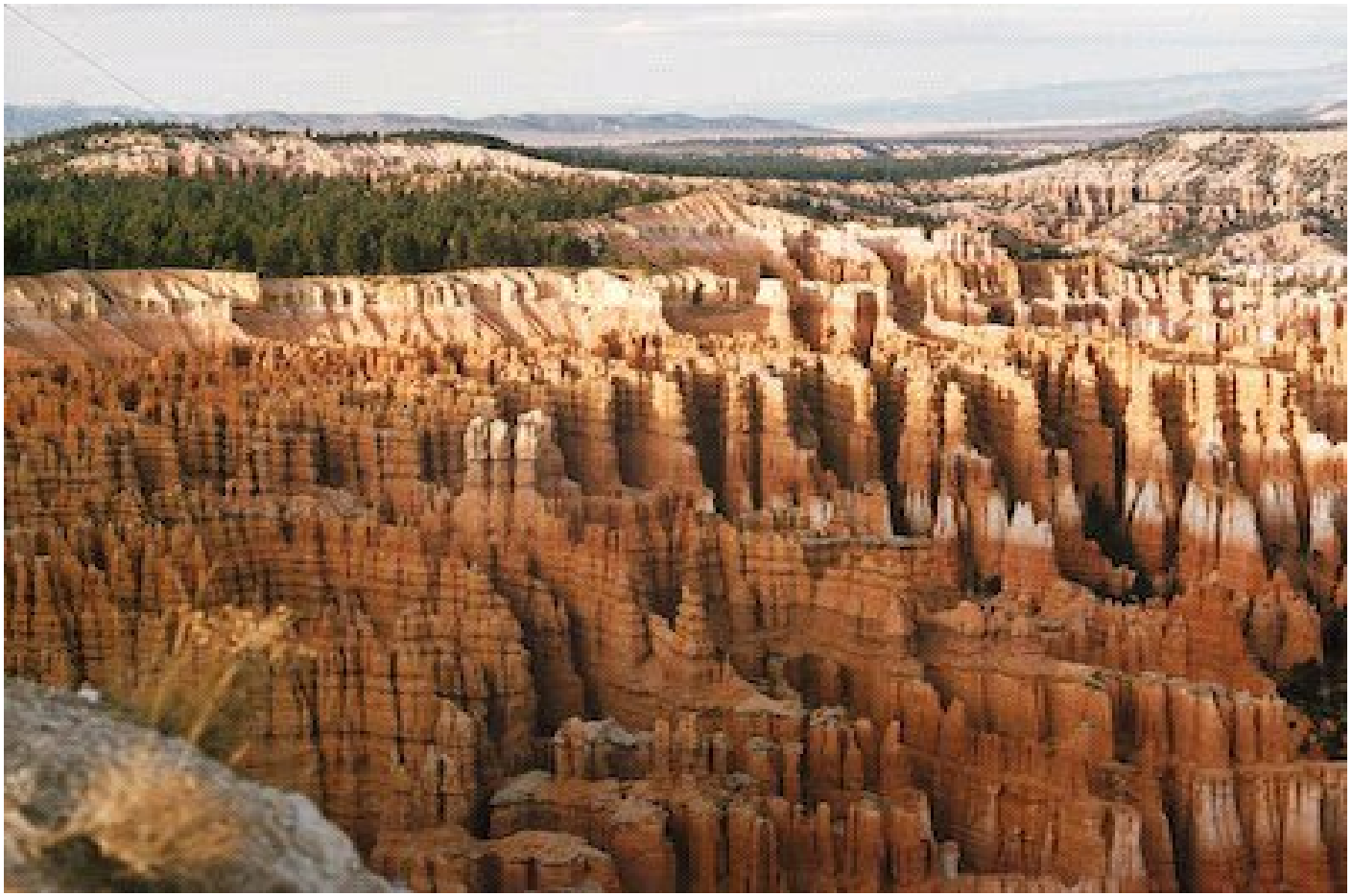
  (khusus untuk citra digital)

Visible Watermarking

Visible Watermarking



Invisible Watermarking



- Saat ini, *Microsoft* sedang meneliti untuk mengembangkan sistem *watermarking* untuk audio digital, yang akan dimasukkan ke dalam *media player Windows*.

- Data seperti informasi lisensi disisipkan ke dalam musik/lagu; *media player* tidak akan memainkan *file* audio yang memuat *watermark* yang salah.