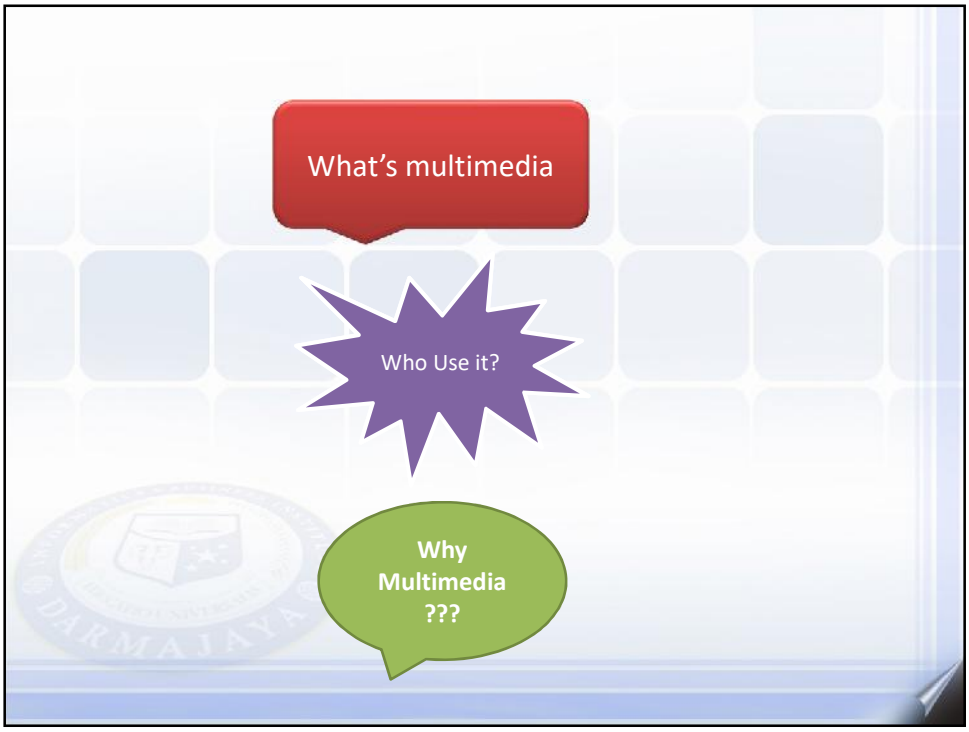
Computer and Network Security
- Security in Multimedia–
VER 2019

Outline

- Steganography
- Tipe Steganography
- Teknik Steganography
- Digital Watermarking



Security Threats On Multimedia

- Interruption
- Interception
- Modification
- Fabrication

Technology

- Cryptography
- Steganography
  - ***Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message i.e covered writing***
- Digital Watermarking

History of Steganography

- One of the earliest uses of steganography was documented in Histories. Histiaeus shaved the head of his most trusted slave and tattooed it with a message which disappeared after the hair had re-grown. The purpose of this message was to instigate a revolt against the Persians. Another slave could be used to send a reply.
- During the American Revolution, invisible ink which would glow over a flame was used by both the British and Americans to communicate secretly .
- **Saat ini : pengamanan menggunakan pendekatan digital**
  - **Baik untuk text , audio dan image**

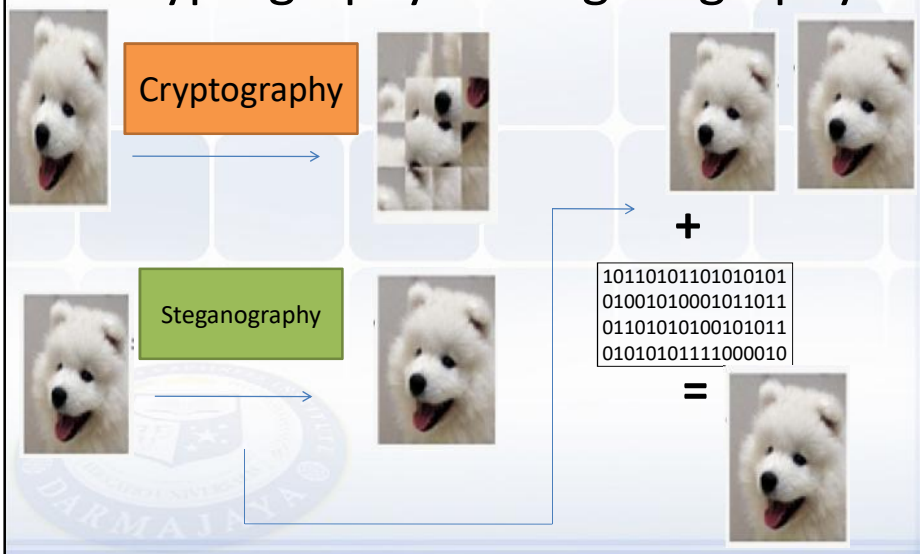
Example

"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils".

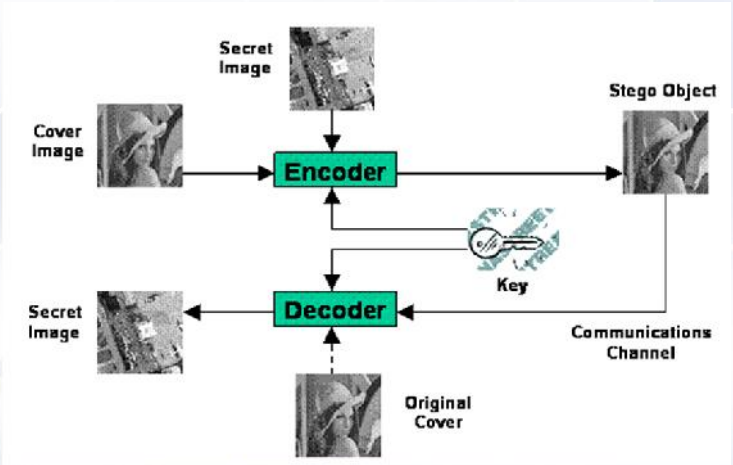
- To reveal the hidden message, pick the second letter in each word, then we get :

"Pershing sails from NY June 1"

Cryptography vs Steganography



Encoding and Decoding in Steganography



Demo Steganography

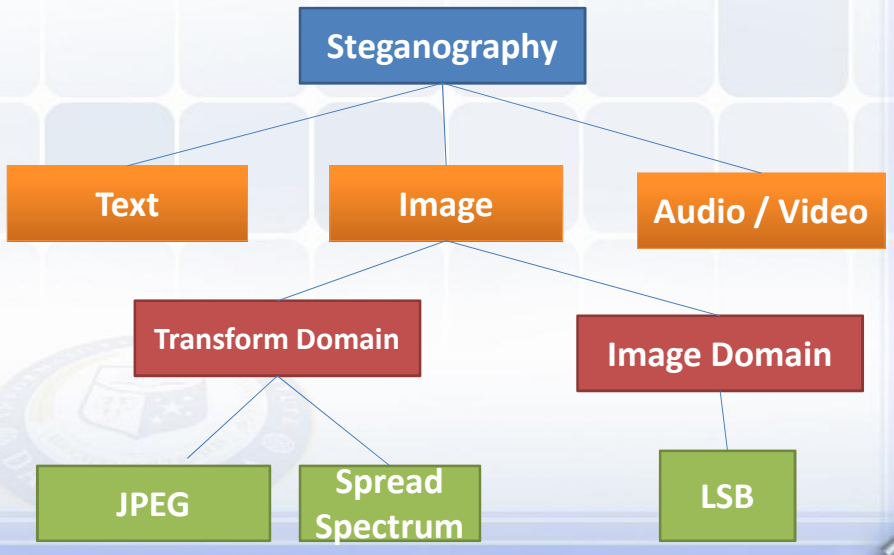
Kriteria Steganography

- **Imperceptibility**
  - Imperceptibility adalah unsur penting : pesan rahasia tidak terlihat oleh manusia.
  - Antara media asli dengan media yang telah disisipi pesan tidak boleh dapat dibedakan dengan kasat mata dan pendengaran.
  - Kualitas media penampung tidak jauh berubah dari kualitas asli.
- **Robustness**
  - Pesan rahasia yang disembunyikan harus tahan terhadap manipulasi yang dilakukan kepada media penampung, seperti perubahan kontras, rotasi, pembesaran, pemotongan.

Kriteria Steganography

- **Recovery**
  - Pesan rahasia yang disembunyikan pada suatu media harus dapat diambil kembali.
- **Security**
  - Pesan atau data rahasia yang disisipkan ke suatu media haruslah terjamin keamanannya, sehingga pihak-pihak yang tidak berkepentingan tidak dapat mengetahui keberadaan informasi yang telah disisipkan tersebut.

Steganography Technique



Least Significant Bit

- Least significant bit (LSB) encoding is the most popular and the easiest technique.
- LSB : merupakan bit yang paling kurang berarti.
- MSB : merupakan bit yang paling berarti (most significant bit).
- Contoh pada byte **1**1010010

Least Significant Bit

- When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.
- Red, Green, Blue (RGB) and gray

Least Significant Bit

- For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Least Significant Bit

- When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

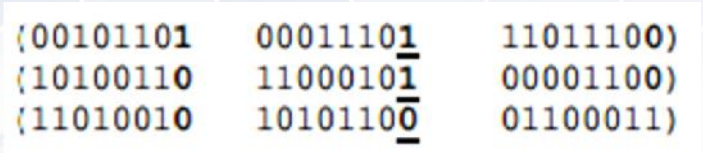
Another Example

- Given number = 200

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

Another Example

- Transfer 200 into bit =
- 11001000
- Final result :



Least Significant Bit

- In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size.
- The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden

Watermark

- Paper Watermarks
- Digunakan untuk identifikasi dan autentikasi, pada :
  - Uang kertas
  - Paspor
  - Dokumen hukum
  - dll

Digital Watermarking

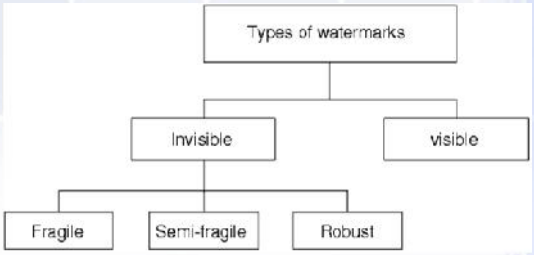
- Merupakan pola digital yang disisipkan ke dalam dokumen digital seperti text, grafis, atau multimedia.
- Membawa informasi unik tentang hak kepemilikan (copyright owner), atau kewenangan.

Digital Watermarking VS Cryptography

- Enkripsi melibatkan transformasi dokumen sehingga isi dari dokumen tidak terlihat tanpa kunci dekripsi
- Watermarking membiarkan file / gambar asli utuh dan bisa dikenali

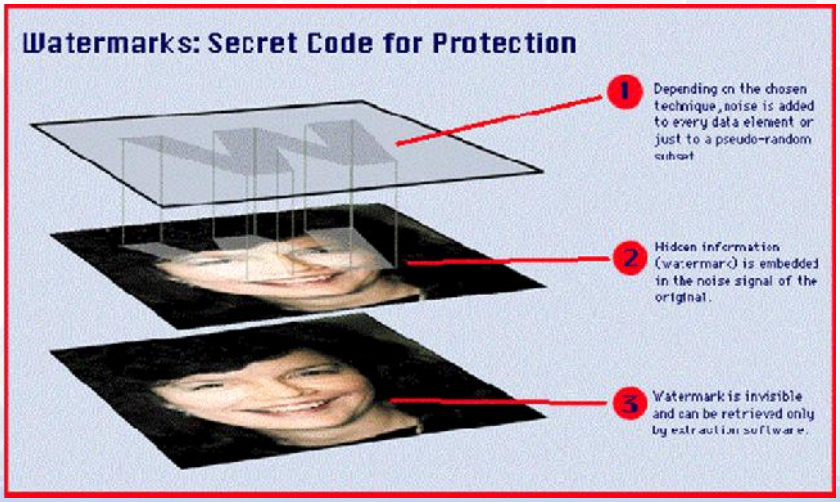
Tipe Watermark

- Visible
  - pola yang tembus pandang
- Invisible
  - Tidak terlihat, tetapi dapat dideteksi secara komputasional



Visible Watermark

Invisible Watermark



Aliansi Digital Watermarking

Represents applications and solutions for:

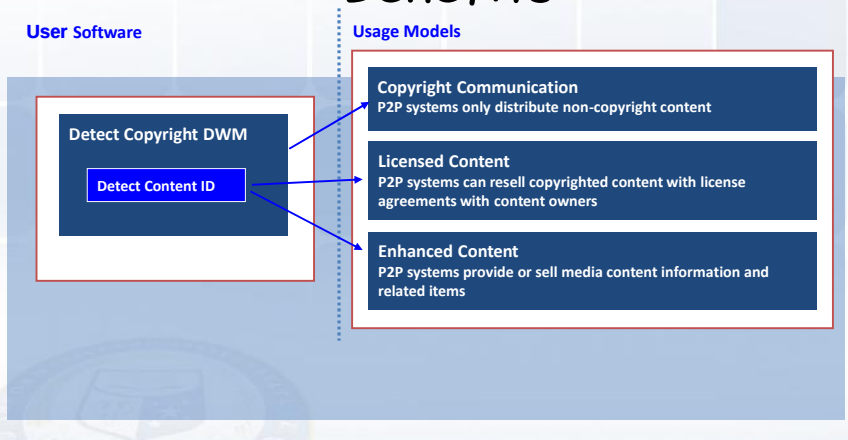
- Audio and Music Content
- Video, Movies and TV Content
- Digital Imagery
- Identity Documents
- Value Documents

Anggota Aliansi Digital Watermarking

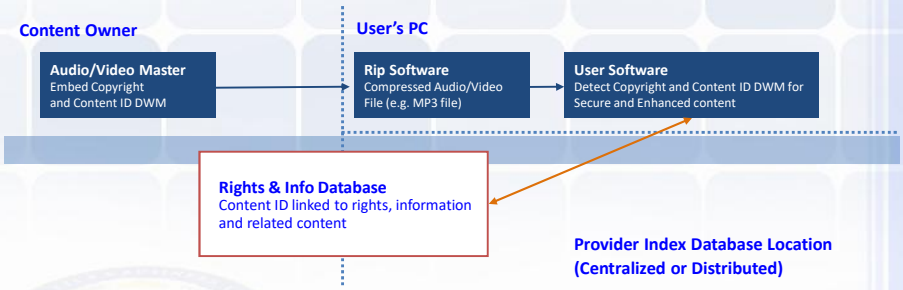
Digital Watermarking Examples

- Copyright Communication
  - Copy Protection
  - Monitoring
  - Filtering/Classification
  - Authentication/Integrity
- Product Serialization & Tracking
  - Asset/Content Management
  - Rights Management
  - Remote Triggering
  - Linking/E-Commerce

Potential Usage Models and Benefits

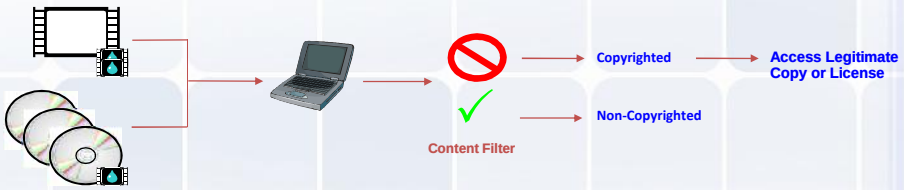


Copyright Digital Watermark Architecture



Can be used to address P2P and social network content Identification needs as well as providing identification of orphan works and access to metadata/networked information

Filtering & Classification



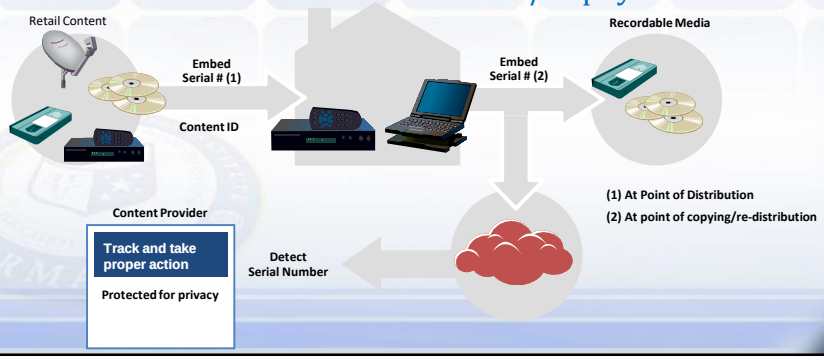
- Can support existing, established and/or new Classification Systems or content identifiers such as MPAA film ratings, ISAN or ad identification codes, etc.
- Filtering can occur at the whole content level and/or at a more granular level identifying copyrighted, sensitive and/or questionable material for the given audience
- May be key element of identifying copyrighted content to support legitimate P2P distribution

Connected Content/Linking

- Promoting & Facilitating M-Commerce
- Location based services
- Multimedia access
  - Streaming audio
  - Music
  - Multimedia
  - Bookmarking

Digital Media Serialization & Tracking

- Identifies content owners and rights while communicating copyright information
- Awareness of watermarked content by consumer creates deterrent against unauthorized copying and distribution
- Provides accurate identification of source of unauthorized content discovered on the Internet and/or physical media



End