# STEGANOGRAFI

Subianto | AMIK JTC SEMARANG

# PENGERTIAN

- Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.

- Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan.

- Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya “tersembunyi atau terselubung”, dan graphein, “menulis”.

- **Contoh :**

  **G**erakan **o**rang-**o**rang **d**ari **y**ordania **e**nggan **a**mbil **r**esiko.

  Dari contoh diatas huruf awal setiap kata bila di rangkai akan membentuk pesan rahasia :
  **Good year**

# Sejarah

- Penguasa yunani (Herodutus)

Mengirim pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Caranya, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepada budak.  Setelah rambut budak tumbuh cukup banyak, budak dikirim ke tempat tujuan pesan untuk membawa pesan rahasia di kepalanya. Di tempat penerima pesan kepala budak dibotaki kembali untuk membaca pesan yang tersembunyi di balik rambutnya. Pesan tersebut berisi peringatan tentang invasi dari Bangsa Persia.

- Bangsa Romawi

  Menggunakan tinta tak-tapak (invisible ink) untuk menulis pesan. Tinta tesebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

- Perang Dunia II

  Perang Dunia II Agen-agen spionase menggunkan steganografi untuk mengirim pesan. Caranya dengan menggunakan titik-titik yang sangat kecil sehingga keberadaannya tidak dapat dibedakan pada tulisan biasa yang diketik.

# Kekinian

- Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (file) komputer.

- Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

# Konsep dan Terminologi

- ***Hiddentext atau embedded message***
  Pesan yang disembunyikan.
- ***Covertext atau cover-object***
  Pesan yang digunakan untuk menyembunyikan embedded message.
- ***Stegotext atau stego-object***
  Pesan yang sudah berisi embedded message

# Kriteria yang harus dipenuhi

- ***Imperceptibility***
  Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi.
- ***Fidelity***
  Mutu media penampungan tidak berubah banyak akibat penyisipan.
- ***Recovery***
  Pesan yang disembunyikan harus dapat di ungkapkan kembali.

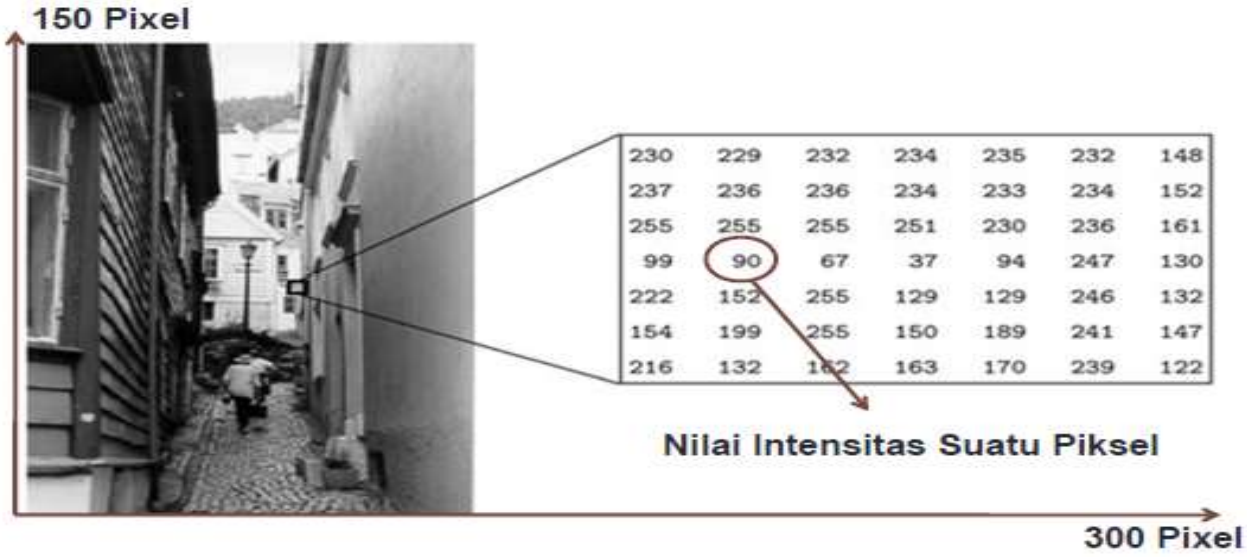
# Teknik Penyembunyian Pesan

Teknik penyisipan pesan data kedalam covertext dapat dilakukan dalam dua macam ranah :

1. Ranah spasial (waktu)(spasial/ timedomain)
   Teknik ini memodifikasi langsung nilai byte dari covertext (nilai byte dapat merepresentasikan intensitas/warna pixel atau amplitudo) contoh metode yang tergolong kedalam teknik renah spasial adalah metode LSB
2. Ranah transform (transform domain)
   Teknik ini memodifikasi langsung hasil transformasi frekuensi sinyal. Contoh yang tergolong ke dalam teknik ranah frekuensi adalah spreed spectrum.

# Metode LSB

- Metode Least Significant Bit merupakan teknik substitusi pada steganografi.
- Biasanya, arsip 24- bit atau 28-bit digunakan untuk menyimpan citra digital.
- Represnetasi warna dari pixel-pixel bisa diperoleh dari warna-warna primer, yaitu merah, hijau, dan biru. Citra 24-bit menggunakan 3 bytes untuk masing-masing pixel, dimana setiap warna primer dipresentasikandengan ukuran 1 byte.
- Penggunaan citra 24-bit memungkinkan setiap pixel dipresentasikan dengan nilai warna sebanyak 16.777.216 macam.
- Dua bit dari saluran warna tersebut bisa bisa digunakan untuk menyembunyikan data, yang akan mengubah jenis warna pixel-nya menjadi 64-bit warna.
- Namun, hal itu akan mengakibatkan sedikit perbedaan yang bisa dideteksi secara kasat mata oleh manusia.
- Metode sederhana itu disebut Least Significant Bit (LSB).


150 Pixel
230 229 232 234 235 232 148
237 236 236 234 233 234 152
255 255 255 251 230 236 161
99 90 67 37 94 247 130
222 152 255 129 129 246 132
154 199 255 150 189 241 147
216 132 162 163 170 239 122
Nilai Intensitas Suatu Piksel
300 Pixel

# Contoh Steganografi Pada Gambar

Gambar

Nilai Intensitas Piksel Dalam Desimal

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 243 | 143 | 67 | 86 | 102 | 224 | 231 | 79 | 166 |
| 171 | 13 | 17 | 20 | 22 | 21 | 21 | 251 | 9 |
| 115 | 41 | 177 | 56 | 148 | 113 | 22 | 208 | 164 |

*Covertext*

Pesan yang akan disembunyikan / *Hiddentext* adalah "HAM"

# Konversi Warna dan Pesan Kedalam Desimal

**Nilai Intensitas Piksel Dalam Desimal**

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 243 | 143 | 67 | 86 | 102 | 224 | 231 | 79 | 166 |
| 171 | 13 | 17 | 20 | 22 | 21 | 21 | 251 | 9 |
| 115 | 41 | 177 | 56 | 148 | 113 | 22 | 208 | 164 |

***Covertext***

**Pesan yang akan disembunyikan adalah :**
**"HAM"**
**Hasil Konversi ke Desimal :**
**72 65 77**

# Konversi Warna dan Pesan Kedalam Biner

Nilai Intensitas Piksel Dalam Biner

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 11110011 | 10001111 | 01000011 | 01010110 | 01100110 | 11100000 | 11100111 | 01001111 | 10100110 |
| 10101011 | 00001101 | 00010001 | 00010100 | 00010110 | 00010101 | 00010101 | 11111011 | 00001001 |
| 01110011 | 00101001 | 10110001 | 00111000 | 10010100 | 01110001 | 00010110 | 11010000 | 10100100 |

**Pesan yang akan disembunyikan / *Hiddentext* adalah :**
**"HAM"**
**Hasil Konversi ke Binner:**
**01001000 01000001 01001101**

## Nilai Intensitas Piksel Dalam Biner

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 11110010 | 10001111 | 01000010 | 01010110 | 01100111 | 11100000 | 11100110 | 01001110 | 10100110 |
| 10101011 | 00001100 | 00010000 | 00010100 | 00010110 | 00010100 | 00010101 | 11111010 | 00001001 |
| 01110010 | 00101000 | 10110001 | 00111001 | 10010100 | 01110001 | 00010110 | 11010000 | 10100100 |

# Konversi Nilai Warna Pada Gambar

## Nilai Intensitas Piksel Dalam Biner

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 11110010 | 10001111 | 01000010 | 01010110 | 01100111 | 11100000 | 11100110 | 01001110 | 10100110 |
| 10101011 | 00001100 | 00010000 | 00010100 | 00010110 | 00010100 | 00010101 | 11111010 | 00001001 |
| 01110010 | 00101000 | 10110001 | 00111001 | 10010100 | 01110001 | 00010110 | 11010000 | 10100100 |

## Nilai Intensitas Piksel Dalam Desimal

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 242 | 143 | 66 | 86 | 103 | 224 | 230 | 78 | 166 |
| 171 | 12 | 16 | 20 | 22 | 20 | 21 | 250 | 9 |
| 114 | 40 | 177 | 57 | 148 | 113 | 22 | 208 | 164 |

COVERTEXT

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 243 | 143 | 67 | 86 | 102 | 224 | 231 | 79 | 166 |
| 171 | 13 | 17 | 20 | 22 | 21 | 21 | 251 | 9 |
| 115 | 41 | 177 | 56 | 148 | 113 | 22 | 208 | 164 |

STEGOTEXT

| R | G | B | R | G | B | R | G | B |
|---|---|---|---|---|---|---|---|---|
| 242 | 143 | 66 | 86 | 103 | 224 | 230 | 78 | 166 |
| 171 | 12 | 16 | 20 | 22 | 20 | 21 | 250 | 9 |
| 114 | 40 | 177 | 57 | 148 | 113 | 22 | 208 | 164 |

# Steganalisis dan Stegosystem

- Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi.
- Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendeteksian bahwa sebuah berkas yang diyakini berisikan data terselubung.
- Seperti dalam Kriptanalisis, diasumsikan bahwa sistem steganografi telah diketahui oleh si penyerang. Maka dari itu, keamanan dari sistem steganografi bergantung hanya pada fakta bahwa kunci rahasia tidak diketahui oleh si penyerang.

# Steganalisis dan Stegosystem

- Stegosystem berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif di mana penyerang hanya dapat memotong data, dan penyerangan-penyerangan aktif di mana penyerang juga dapat memanipulasi data.

# Penyerangan-penyerangan dalam stegosistem

- *Stego-Only-Attack (Penyerangan hanya Stego).*
  Penyerang telah menghalangi stego data dan dapat menganalisisnya.
- *Stego-Attack (Penyerangan Stego).*
  Pengirim telah menggunakan cover yang sama berulangkali untuk data terselubung. Penyerang memiliki berkas stego yang berasal dari cover file yang sama. Dalam setiap berkas stego tersebut, sebuah pesan berbeda disembunyikan.
- *Cover-Stego-Attack (Penyerangan selubung Stego).*
  Penyerang telah menghalangi berkas stego dan mengetahui cover file mana yang digunakan untuk menghasilkan berkas stego ini. Ini menyediakan sebuah keuntungan melalui penyerangan stego-only untuk si penyerang.
- *Manipulating the stego data (Memanipulasi data stego).*
  Penyerang memiliki kemampuan untuk memanipulasi data stego. Jika penyerang hanya ingin menentukan sebuah pesan disembunyikan dalam berkas stego ini, biasanya ini tidak memberikan sebuah keuntungan, tapi memiliki kemampuan dalam memanipulasi data stego yang berarti bahwa si penyerang mampu memindahkan pesan rahasia dalam data stego (jika ada).
- *Manipulating the cover data (Memanipulasi data terselubung).*
  Penyerang dapat memanipulasi data terselubung dan menghalangi hasil data stego. Ini dapat membuat tugas dalam menentukan apakah data stego berisikan sebuah pesan rahasia lebih mudah bagi si penyerang.