NAMA : WENNY PRASTIWI

NIM : 18050623024

PRODI : D3 MANAJEMEN INFORMATIKA 2018

MATA KULIAH KEAMANAN JARINGAN

RESUME STEGANOGRAFI

A. Definisi Steganografi

Steganografi berasal dari bahasa Yunani: steganos + graphien, yang artinya yaitu :

“steganos” (στεγανός) : tersembunyi

“graphien” (γραφία) : tulisan

Jadi jika di artikan secara harfiah, steganografi adalah tulisan tersembunyi (covered writing)

Steganography adalah ilmu dan seni menyembunyikan pesan rahasia dengan suatu cara sedemikian sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut.

- Tujuan : pesan tidak terdeteksi keberadaannya

B. Perbedaan Kriptografi dan Steganografi

- **Kriptografi** : menyembunyikan isi (content) pesan

  Tujuan: agar pesan tidak dapat dibaca oleh pihak ketiga (lawan)
- **Steganografi** : menyembunyikan keberadaan (existence) pesan

  Tujuan: untuk menghindari kecurigaan (conspicuous) dari pihak ketiga (lawan)

C. Information Hiding

Information hiding: bidang ilmu yang mempelajari cara menyembunyikan pesan sehingga tidak dapat dipersepsi (baik secara visual maupun audial).

Yang termasuk ke dalam information hiding:

1. Kriptografi
2. Steganografi

D. Sejarah Steganografi

Usia steganografi setua usia kriptografi, dan sejarah keduanya berjalan bersamaan. Periode sejarah steganografi dapat dibagi menjadi:

1. Steganografi kuno (ancient steganography)
2. Steganografi zaman renaisans (renaissance steganography).
3. Steganografi zaman perang dunia
4. Steganografi modern

E. Detail Periode Sejarah Steganografi

1. Ancient Steganography

a. Steganografi dengan media kepala budak Ditulis oleh Herodatus (485 – 525 BC), sejarawan Yunani pada tahun 440 BC di dalam buku: Histories of Herodatus). Kisah perang antara kerajaan Persia dan rakyat Yunani.

Detail cerita :

Herodatus menceritakan cara Histaiaeus mengirim pesan kepada Aristagoras of Miletus untuk melawan Persia. Caranya: Dipilih beberapa budak. Kepala budak dibotaki, ditulisi pesan dengan cara tato, rambut budak dibiarkan tumbuh, budak dikirim. Di tempat penerima kepala budak digunduli agar pesan bisa dibaca.

b. Penggunaan tablet wax
Orang-orang Yunani kuno menulis pesan rahasia di atas kayu yang kemudian ditutup dengan lilin (wax). Di dalam bukunya, Heradatus menceritakan Demaratus mengirim peringatan tentang serangan yang akan datang ke Yunani dengan menulis langsung pada tablet kayu yang kemudian dilapisi lilin dari lebah.

c. Penggunaan tinta tak-tampak (invisible ink)
Pliny the Elder menjelaskan penggunaan tinta dari getah tanaman thithymallus. Jika dituliskan pada kertas maka tulisan dengan tinta tersebut tidak kelihatan, tetapi bila kertas dipanaskan berubah menjadi gelap/coklat

d. Penggunaan kain sutra dan lilin
Orang Cina kuno menulis catatan pada potongan-potongan kecil sutra yang kemudian digumpalkan menjadi bola kecil dan dilapisi lilin. Selanjutnya bola kecil tersebut ditelan oleh si pembawa pesan. Pesan dibaca setelah bola kecil dikeluarkan dari perut si pembawa pesan.

2. Renaissance Steganography

Tahun 1499, Johannes Trithemius menulis buku Steganographia, yang menceritakan tentang metode steganografi berbasis karakter. Selanjutnya tahun 1518 dia menulis buku tentang steganografi dan kriptografi, Berjudul Polygraphiae. Giovanni Battista Porta menggambarkan cara menyembunyikan pesan di dalam telur rebus. Caranya, pesan ditulis pada kulit telur yang dibuat dari tinta khusus yang dibuat dengan satu ons tawas dan setengah liter cuka. Prinsipnya penyembunyiannya adalah tinta tersebut akan menembus kulit telur yang berpori, tanpa meninggalkan jejak yang terlihat. Tulisan dari tinta akan membekas pada permukaan isi telur yang telah mengeras (karena sudah direbus sebelumnya). Pesan dibaca dengan membuang kulit telur

3. World War Steganography

a. Penggunaan tinta tak-tampak (invisible ink) dalam spionase. - Pada Perang Dunia II, tinta tak-tampak digunakan untuk menulis pesan rahasia - Tinta terbuat dari campuran susu, sari buah, cuka, dan urine. - Cara membaca: Kertas dipanaskan sehingga tulisan dari tinta tak-tampak tersebut akan menghitam.

b. Steganografi dalam Perang Dunia II: Null Cipher
Pesan berikut dikirim oleh Kedubes Jerman pada PD II: 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. Ambil huruf kedua setiap kata, diperoleh pesan berikut: Pershing sails from NY June 1.

Contoh Null Cipher lainnya:

- Big rumble in New Guinea. The war on celebrity acts should end soon. Over four die ecstatic elephants replicated.
Hasilnya :
Bring two cases of deer

- Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

Dengan mengambil huruf ketiga pada setiap kata diperoleh pesan berikut:
Send Lawyers, Guns, and Money.

c. Steganografi dan Terorisme
Ilmu steganografi mendadak naik daun ketika pasca 11 September 2001 pihak FBI menuding Al-Qaidah menggunakan steganografi untuk menyisipkan pesan rahasia melalui video atau gambar yang mereka rilis secara teratur di Internet.

4. Steganografi Modern - The Prisoner's Problem

Diperkenalkan oleh Simmons – 1983 • Dilakukan dalam konteks USA – USSR nuclear non-proliferation treaty compliance checking

a. Steganografi Digital
Steganografi digital: penyembunyian pesan digital di dalam dokumen digital lainnya.
Carrier file: dokumen digital yang digunakan sebagai media untuk menyembunyikan pesan.
1. Teks "Kita semua bersaudara"
2. Audio
3. Gambar (image)
4. Video - bmp - jpeg - gif - wav - mp3 -Txt - doc - html -Mpeg - avi – dll

b. Terminologi Steganografi
1. Embedded message (hiddentext) atau secret message: pesan yang disembunyikan . Bisa berupa teks, gambar, audio, video, dll
2. Cover-object (covertext): pesan yang digunakan untuk menyembunyikan embedded message. Bisa berupa teks, gambar, audio, video, dll
3. Stego-object (stegotext): pesan yang sudah berisi pesan embedded message.

4. Stego-key: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.

F. Kriteria Steganografi yang Bagus

1. Imperceptible Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audio (untuk stego-audio).
2. Fidelity. Kualitas cover-object tidak jauh berubah akibat penyisipan pesan rahasia.
3. Recovery. Pesan yang disembunyikan harus dapat diekstraksi kembali.
4. Capacity Ukuran pesan yang disembunyikan sedapat mungkin besar

Catatan: Robustness bukan isu penting di dalam steganografi

G. Tiga Tipe Steganografi

1. Pure steganography Tidak membutuhkan kunci sama sekali. Keamanan steganografi seluruhnya bergantung pada algoritmanya.
   Contoh: Null Cipher Prinsip Kerkhoff juga seharusnya pada steganografi, bahwa keamanan sistem seharusnya tidak didasarkan pada kerahasaiaan algoritma embedding, tetapi pada kuncinya. Pure steganography -> tidak disukai

2. Secret (or symmetric) key Steganography Menggunakan kunci yang sama untuk embedding dan extraction. Contoh: - kunci untuk pembangkitan bilangan acak - kunci untuk mengenkripsi pesan dengan algoritma kriptografi simetri (DES, AES, dll)

3. Public-key Steganography Menggunakan dua kunci: kunci publik untuk embedding dan kunci privat untuk extraction. Contoh: kunci publik RSA untuk mengenkripsi hidden message kunci privat RSA untuk mendekripsi hidden message

H. Ranah Steganografi

Berdasarkan ranah operasinya, metode-metode steganografi dapat dibagi menjadi dua kelompok

1. Spatial (time) domain methods Memodifikasi langsung nilai byte dari cover-object (nilai byte dapat merepresentasikan intensitas/warna pixel atau amplitudo)
   Contoh: Metode modifikasi LSB
2. Tranform domain methods Memodifikasi hasil transformasi sinyal dalam ranah transform (hasil trnasformasi dari ranah spasial ke ranah lain (misalnya ranah frekuensi).
   Contoh: Metode Spread Spectrum

I. Teknik Dasar dalam Steganografi

1. Substitution techniques : mengganti bagian yang redundan dari cover-object dengan pesan rahasia. Contoh: metode modifikasi LSB
2. Transform domain techniques : menyisipkan pesan rahasia ke dalam sinyal dalam ranah transform (misalnya dalam ranah frekuensi).
3. Spread spectrum techniques : menyisipkan pesan rahasia dengan mengadopsi ide komunikasi spread spectrum.
4. Statistical techniques : menyisipkan pesan dengan mengubah beberapa properti statistik dari cover-object dan menggunakan metode uji hipotesis pada proses ekstraksi pesan.
5. Distortion techniques : menyimpan pesan rahasia dengan distorsi sinyal dan mengukur deviasinya dari cover-object pada proses ekstraksi pesan.

6. Cover generation techniques : tidak menyisipkan pesan pada cover-object yang dipilih secara acak, tetapi membangkitkan cover yang cocok untuk pesan yang disembunyikan.

J. Program Stegano shareware

- InPlainView: http://www.simtel.net/product.php%5Bid%5D12796%5 BSiteID%5Dsimtel.net Keterangan: hanya untuk citra .bmp 2. S-tools
- http://digitalforensics.champlain.edu/download/stools4.zip Keterangan: untuk citra GIF dan BMP
- Daftar 100 kakas steganografi lainnya: http://www.jjtc.com/Steganography/toolmatrix.html Beberapa diantaranta berjalan di Linux:
  1. JPHS (JPHide JPSeek, JP hide and seek) http://linux01.gwdg.de/~alatham/stego.html
  2. Steghide
  3. 3. Outguess
  4. 4. Blindside
  5. 5. Gifshuffle
  6. 6. GzSteg
  7. 7. Dll

K. Metode LSB

Citra Digital

- Citra terdiri dari sejumlah pixel. Citra 1200 x 1500 berarti memiliki 1200 x 1500 pixel = 1.800.000 pixel
- Setiap pixel panjangnya n-bit. Citra biner -> 1 bit/pixel Citra grayscale ◊ 8 bit/pixel Citra true color ◊ 24 bit/pixel

Citra Lenna

Pada citra 24-bit (real image), 1 pixel = 24 bit, terdiri dari komponen RGB (Red-Green-Blue)

Bitplane pada Citra Digital

Nilai pixel pada koordinat (x, y) menyatakan intensitas nilai keabuan pada posisi tersebut.
- Pada citra grayscale nilai keabuan itu dinyatakan dalam integer berukuran 1 byte sehingga rentang nilainya antara 0 sampai 255.
- Pada citra berwarna 24-bit setiap pixel tediri atas kanal red, green, dan blue (RGB) sehingga setiap pixel berukuran 3 byte (24 bit).
- Di dalam setiap byte bit-bitnya tersusun dari kiri ke kanan dalam urutan yang kurang berarti (least significant bits atau LSB) hingga bit-bit yang berarti (most significant bits atau MSB).
- Susunan bit pada setiap byte adalah b8b7b6b5b4b3b2b1
- Bitpline LSB, yaitu bitplane 0, terlihat seperti citra acak (random image).
- Bitpline LSB merupakan bagian yang redundan pada citra.
- Artinya, perubahan nilai bit pada bagian tersebut tidak mengubah persepsi citra secara secara keseluruhan.
- Inilah yang mendasari metode steganografi yang paling sederhana, yaitu metode modifikasi LSB. Rinaldi Munir/IF4020 Kriptografi

L. Metode Modifikasi LSB

Merupakan metode steganografi yang paling populer. Memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar

Caranya: Mengganti bit LSB dari pixel dengan bit pesan. Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya -> tidak berpengaruh terhadap persepsi visual/auditori.

Misalkan semua bit LSB pada citra berwarna dibalikkan Dari semula 0 menjadi 1; dari semula 1 menjadi 0

M. Ekstraksi Pesan dari Stego-object

Bit-bit pesan yang disembunyikan di dalam citra harus dapat diekstraksi kembali. λ Caranya adalah dengan membaca byte-byte di dalam citra, mengambil bit LSB-nya, dan merangkainya kembali menjadi bit-bit pesan.

Contoh: Misalkan stego-object adalah sbb 00110011 10100011 11100011 10101010 00100110 10010111 11001000 11111001 10001001 10100011 Ekstrak bit-bit LSB: 1110010111

N. Menghitung Ukuran Pesan yang dapat Disembunyikan

Ukuran pesan yang akan disembunyikan bergantung pada ukuran cover-object.

- Misalkan pada citra grayscale (1 byte/pixel) 256 x 256 pixel : - jumlah pixel = jumlah byte = 256 x 256 = 65536 - setiap byte dapat menyembunyikan 1 bit pesan di LSB-nya - jadi ukuran maksimal pesan = 65536 bit = 8192 byte = 8 KB

- Pada citra berwarna 24-bit berukuran 256 × 256 pixel: - jumlah pixel 256 x 256 = 65536 - setiap pixel = 3 byte, berarti ada 65536 × 3 = 196608 byte. - setiap byte dapat menyembunyikan 1 bit pesan - jadi ukuran maksimal pesan = 196608 bit = 24576 byte = 24KB

O. Beberapa Varian Metode LSB

1. Sequential

Bit-bit pesan disembunyikan secara sekuensial pada pixel-pixel citra.

2. Ekstraksi pesan dari Stego-image

- Pada proses ekstraksi pesan, pixel-pixel dibaca secara sekuensial mulai dari pixel pertama sampai pixel yang menyimpan bit pesan terakhir
- Ambil setiap byte dari pixel, ekstraksi bit LSB-nya.
- Rangkailah bit-bit LSB menjadi bit-bit pesan semula.

3. Acak

- Untuk membuat penyembunyian pesan lebih aman, bit-bit pesan tidak disimpan pada pixel-pixel yang berurutan, namun dipilih secara acak.
- Pembangkit bilangan acak-semu (PRNG: pseudo-random number generator) digunakan untuk membangkitkan bilangan acak.
- Umpan (seed) untuk pembangkit bilangan acak berlaku sebagai kunci (stego-key).

4. m-bit LSB

Untuk meningkatkan ukuran pesan yang disembunyikan, maka digunakan lebih dari 1 bit LSB untuk setiap byte.

- Susunan bit pada setiap byte adalah b7b6b5b4b3b2b1b0 . Jika diambil 2-bit LSB, maka bit yang digunakan adalah bit b1 dan bit b0 Contoh: 11010010 -> 2 bit LSB terakhir dipakai untuk menyembunyikian pesan.
- Trade-off: Semakin banyak bit LSB yang digunakan, semakin besar ukuran pesan yang dapat disembunyikan, tetapi semakin turun kualitas stego-image.
- Pesan dapat disembunyikan secara sekuensial atau secara acak pada pixel-pixel di dalam citra.

5. Enkripsi XOR
   - Pesan dapat dienkripsi terlebih dahulu sebelum disembunyikan ke dalam citra.
   - Teknik enkripsi yang sederhana adalah dengan meng-XORkan bit-bit pesan dengan bit-bit kunci. Jumlah bit-bit kunci sama dengan jumlah bit pesan.
   - Bit-bit kunci dibangkitkan secara acak.
   - Kunci untuk pembangkitan bit-bit kunci menjadi stego-key.
   - Jika dipakai teknik acak dalam memilih pixel-pixel, maka ada dua stego-key: satu untuk pembangkitan bit-bit kunci, satu lagi untuk pembangkitan posisi pixel yang dipilih untuk menyembunyikan pesan.

6. PSNR
   PSNR = Peak-Signal-to-Noise Ratio

- Merupakan metrik untuk mengukur kualitas (fidelity) citra setelah proses manipulasi.
- Selalu dibandingkan dengan citra semula (yang belum dimanipulasi).

P. Steganalysis

Tujuan: menentukan apakah sebuah media suspect mengandung pesan tersembunyi

Informasi rahasia tersebut dapat berupa pesan biasa, pesan kejahatan, program jahat, bahkan virus komputer! Pernah terima surel (e-mail) dari orang tak dikenal dan mengandung file attachmet berupa gambar.

Steganalisis diperlukan di dalam forensic image analysis

- Forensic Image Analysis is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters.

- Subdisiplin dari Forensic Image Analysis:

(1) Photogrammetry (2) Photographic Comparison (3) Content Analysis (4) Image Authentication

Salah satu pekerjaan di dalam content analysis adalah mendeteksi apakah ada pesan tersembunyi di dalam sebuah gambar.

- Contoh sebuah skenario: Mr. Abdul, seorang investigator forensik, diminta Lab Forensik Polri untuk menginvestigasi sebuah cybercrime berupa foto. Sebagai investigator forensik yang ahli, dia menganalisis foto untuk menemukan pesan tersembunyi di dalamnya dengan kakas steganalisis
- Tujuan utama steganalisis adalah untuk membedakan apakah sebuah media mengandung pesan rahasia atau tidak.
- Steganalisis dianggap berhasil jika ia dapat menentukan apakah sebuah media mengandung pesan tersembunyi dengan peluang lebih tinggi daripada menerka secara acak.
- Selain tujuan utama di atas, terdapat beberapa tujuan minor steganalisis: - menentukan panjang pesan - menentukan tipe algoritma penyisipan - kunci yang digunakan Jenis-jenis steganalis

Q. Jenis-jenis steganalisis

1. Targeted steganalysis - Teknik steganalisis yang bekerja pada algoritma steganografi spesifik, dan kadang-kadang dibatasi hanya pada format media tertentu saja. - Teknik ini mempelajari dan menganalisis algoritma penyisipan, lalu menemukan statistik yang

berubah setelah penyisipan. - Hasil steganalisis sangat akurat, tetapi tidak fleksibel karena tidak dapat diperluas untuk algoritma steganografi yang lain atau format media yang berbeda.

2. Blind steganalysis - Teknik steganalisis yang bekerja pada sembarang algoritma steganografi dan sembarang format media. - Teknik ini mempelajari perbedaan antara statistik coverobject dan stego-object dan membedakannya. Proses pembelajaran (learning) dilakukan dengan melatih (training) mesin pada sekumpulan database media. Model machine learning yang digunakan misalnya jaringan syaraf tiruan. - Hasil steganalisis kurang akurat dibandingkan dengan teknik targeted steganalysis, tetapi kelebihannya adalah dapat diperluas untuk algoritma yang lain.

R. Metode Steganalisis

1 . Serangan berbasis visual (visual attacks) - Khusus untuk stego-object berupa citra - Bersifat subjektif, karena melakukan pengamatan secara kasat mata dengan melihat artefak yang mencurigakan di dalam stego-image, lalu membandingkannya dengan citra asli (cover image) - Digunakan pada masa-masa awal riset steganalisis

- Contoh serangan visual: a. LSB plane attack b. Filtered visual attack (Enhanced LSB)

2. Serangan berbasis statistik (statistical attack) - Menggunakan analisis matematik pada citra untuk menemukan perbedaan antara cover image dengan stego image. - Didasarkan pada fakta bahwa penyembunyian pesan ke dalam media menimbulkan artefak yang dapat dideteksi secara statistik sehingga dapat mengungkap penyembunyian pesan atau pesan yang disembunyikan itu sendiri.

- Contoh serangan statistik: a. histogram analysis b. Regular-singular (RS) analysis c. Chi-square analysis d. Sample pair (SP) analysis

S. Visual Attack

Memanfaatkan indera penglihatan -> inspeksi kerusakan pada gambar akibat penyisipan [WES99] - Ide dasar : media pembawa/ steganogram diserang ekstraksi bit-bit yang berpotensi menjadi bit Pesan Ilustrasi visual dari bit-bit yang telah diekstraksi dengan posisi yang sesuai dengan pixel sumbernya.

- Metode enhanced-LSB bagus untuk citra dengan kontras tinggi, yaitu citra yang memiliki warna latar yang jelas atau memiliki perbedaan warna yang kontras antara latar dengan gambar utama
- Untuk citra dengan kontras rendah (seperti citra hasil fotografi), metode enhanced LSB seringkali menyulitkan steganalis. Karena steganalis akan kesulitan membedakan antara gambar yang seharusnya muncul dengan pesan rahasia.

T. Metode Chi-square

- Chi-square attack merupakan serangan berbasis statistik yang menganalisis histogram dari PoV (Pairs of Value).
- PoV adalah pasangan nilai yang hanya berbeda pada bit LSB-nya saja.
  Contoh: 10 dan 11 (0000101**0** dan 0000101**1**) 128 dan 129 (1000000**0** dan 1000000**1**)
- Penyisipan pesan dengan metode LSB pada dasarnya mengganti bit LSB dengan bit pesan.

- Penggantian bit LSB tersebut hanya mengubah nilai bit LSB dari 0 menjadi 1 atau dari 1 menjadi 0 (flip embedding).
- Ini berarti nilai-nilai di dalam setiap PoV hanya mengalami swapping (saling dipertukarkan)
- Chi-square attack menganalisis histogram dari PoV yang nilai-nilainya saling dipertukarkan (swapping) selama proses penyisipan pesan.

U. Referensi

Li, F., The art and science of writing hidden messages: Steganography

Khan, M. M. , Steganography λ Wohlgemuth, S. (2002), IT-Security: Theory and Practice : Steganography and Watermarking, University of Freiburg, Denmakr, 2002.

Wong, P.W. (1997). A Watermark for Image Integrity and Ownership Verification. Prosiding IS&T PIC Conference.

Tawalbeh, L. (2006), Watermarking, Information System Security AABFS-Jordan.

Bae, S.H. (2006), Copyright Protection of Digital Image, Tongmyong University of information technology

Yuli Anneria Sinaga, Steganalisis dengan Metode Chi-square dan RSanalysis, Tugas Akhir Informatika, IT

Wikipedia