Apa itu Steganography?

by webmaster - Saturday, November 21, 2015

http://suyatno.dosen.akademitelkom.ac.id/index.php/2015/11/21/apa-itu-steganography/

Steganography merupakan seni dari penyembunyian data yang kuno. Teknologi digital memberikan kita cara baru untuk menerapkan teknik steganography yang termasuk satu dari intrik dari penyembunyian da ta dalam citra digital. Steganography menyembunyikan data dengan cara yang mencegah terdeteksinya p esan tersembunyi. *Steganography*
diturunkan dari bahasa Yunani yang berarti “penulisan terselubung”. Ini mencakup kumpulan yang luas dari metode komunikasi rahasia yang menyembunyikan pesan dengan sangat handal. Metode ini termasu k didalamnya tinta tak tampak, mikrodot, penyusunan huruf, tanda tangan digital, dan komunikasi spektral tersebar.

Steganography dan Cryptography merupakan saudara sepupu dalam keluarga spionase. Cryptography me ngacak pesan sehingga tidak dapat difahami. Steganography menyembuntikan pesan sehingga tidak terli hat. Pesan dalam
teks tersandi atau *chipertext*
untuk cara cepat menimbulkan kecurigaan pada penerima, sedangkan pesan tak
tampak yang dibuat dengan metode steganography tidak.

Dalam artikel ini, kita akan berdiskusi mengenai file citra dan bagaimana menyembunyikan informasi did alamnya, dan hasil yang diperoleh dengan software steganographic.

Penyembunyian Data

Data yang akan disembunyikan, ke dalam citra membutuhkan 2 file. Pertama, citra yang tampak bagus ya ng
akan digunakan untuk m
enyimpan informasi yang disembunyikan, yang disebut *cover image.* Kedua adalah pesan yang merupaka n informasi yang akan disembunyikan. Pesan dapat berupa teks, teks teracak, citra yang
lain atau apapun yan
g dapat disembunyikan dalam deretan bit. Ketika digabungkan, *cover image* atau citra
sampul dan pesan yang disembunyikan membentuk *stego-image.* Sebuah kunci atau password
dapat digunakan untuk menyembunyikan kemudian mengekstraksi kembali pesan.

Gambar 1 Contoh Steganografi

Teknik dalam Citra Digital

Informasi dapat disembunyikan dengan beberapa cara yang berbeda dalam citra.Untuk menyembunyikan informasi, penyisipan informasi bisa dilakukan dengan mengkodekan setiap bit dari informasi ke dalam ci tra atau dengan memilih menyembunyikan pesan di dalam daerah terkena noise yang kurang memberika n perhatian. Pesan dapat juga disebar secara random ke seluruh permukaan citra. Terdapat beberapa cara yang ada untuk menyembunyikan informasi ke dalam citra digital, yaitu :

- Penyisipan LSB
- Masking dan Filtering
- Algoritma dan Transformasi

Least Significant Bits (LSB)

Penyisipan bit merupakan pendekatan yang sederhana untuk menyembunyikan informasi dalam file samp ul. Sayangnya, metode ini dapat dihilangkan dengan cara memanipulasi citra sampul. Mengkonversi citra dari
format GIF atau BMP, yang dapat merekontruksi citra secara tepat (*lossless compression*) ke JPEG yang (*lossy compression*) dapat merusak informasi yang disembunyikan dalam LSB. Untuk menyembunyikan pesan dalam LSB dari setiap byte dari citra 24 bit, maka kita dapat menyimpan 3 bit setiap piksel.

Citra sampul dengan ukuran 800 x 600 piksel dapat menyimpan pesan 180.000 bytes. Penyisipan LSB ha nya membutuhkan separuh dari bit dalam citra yang berubah.Kita dapat menyembunyikan data dalam bit terakhir dan yang kedua dari LSB dan mata manusia masih tidak dapat membedakan.

Gambar 2 Masking Watermark

Masking dan Filtering

Teknik masking dan filtering biasanya diterapkan pada citra gray scale dan 24 bit untuk menyembunyikan informasi dengan menandai citra, dalam cara yang mirip dengan kertas watermark. Teknik watermark dapat diterapkan tanpa menyebabkan rusaknya citra karena lebih terintegrasi dengan citra.

Perbedaan utama antara watermark dan steganography adalah digital watermark merupakan informasi tambahan dan menjadi atribut dari citra sampul, yang dapat berupa hak cipta, kepemilikan atau lesensi. Dalam steganography obyek dari komunikasi adalah pesan tersembunyi.

Sedangkan dalam watermark digital, obyek dari komunikasi adalah sampul. Untuk membuat citra terwatermark, kita dapat menambah luminansi dari daerah mask sebesar 15 %. Jika kita mengubah luminansi dengan presentasi
yang lebih kecil, ma
ka mask akan tidak terdeteksi oleh mata manusia. Masking lebih *robust* atau handal daripada penyisipan LSB.

Algoritma dan Transformasi

Manipulasi LSB merupakan cara yang cepat dan mudah untuk mrnyembunyikan informasi, tetapi sangat mudah hilang dengan perubahan yang kecil karena pengolahan citra atau kompresi lossy. Salah satu algoritma untuk menyembunyikan informasi adalah menyembunyikan informasi ke dalam citra sampul yang terkompresi seperti dengan Jpeg-

Jsteg. Jpeg Jsteg membuat citra stego JPEG dari masukan pesan yang akan disembunyikan dan citra sam pul lossless. Citra JPEG menggunakan transformasi cosinus diskrit (DCT) untuk mendapatkan kompresi. DCT merupakan transformasi untuk kompresi lossy karena nilai cosinus tidak dapat dihitung kembali sec ara tepat dan pengulangan perghitungan menggunakan ketelitian yang terbatas yang mengenalkan pembu latan pada hasil akhirnya.

Sejarah Steganography

Melalui sejarah, orang telah menyembunyikan informasi dengan banyak metode dan variasi. Sebagai cont oh penduduk Yunani menulis teks pada tongkat yang tersampul pita. Untuk memecahkan pesan yang ters embunyi kita harus menutupkan pita pada tongkat dan menampakkan pesan yang dikirimkan. Dan metod e jenius yang lain adalah dengan menuliskan pesan pada kepala pembawa pesan yang telah digunduli. Se hingga ketika rambutnya telah tumbuh maka pesan menjadi tidak terlihat.

Pada awal perang dunia II, teknologi steganography yang digunakan adalah tinta yang tidak tampak untuk menyembunyikan informasi rahasia. Dan dokumen sendiri dapat menyembunyikan pesan melalui null ci phers
(pesan yang tidak terenkripsi), yang menutup pesan sesungguhnya diantara pesan tersebut. Seperti pesan yang pernah dikirimkan oleh mata-mata Jerman yang berbunyi :

“Apparently neutral’s protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affec ts pretext for embargo on by-products, ejecting suets and vegetable oils”.

Untuk memecahkan pesan ini, kita dapat mengambil huruf kedua dalam setiap kata, sehingga diperoleh p esan berikut :

“Pershing sails from NY June 1”

Pendeteksian pesan diperbaiki dengan pengembangan teknologi baru yang dapat memecahkan lebih bany ak informasi. Dengan setiap penemuan dari pesan tersembunyi dengan aplikasi yang ada, aplikasi stegan ography yang baru akan ditemukan.

Saat ini berbagai metode data hiding telah distandarisasi, dan sekian banyak lagi metode dikembangkan ta npa mengikuti standar yang ada untuk keperluan keamanan. Semakin rumit metode yang digunakan akan semakin sulit memecahkannya. (suy@akademitelkom.ac.id)
