Bit-Plane Complexity Steganography dan Perbandingannya dengan *Least Significant Bit Steganography*

Heryanto (13504081) [1)]

1) Jurusan Teknik Informatika ITB, Bandung 40122, email: if14081@students.if.itb.ac.id

Abstract *– Steganografi adalah sebuah teknik untuk menyembunyikan keberadaan pesan rahasia. Berbeda dengan kriptografi yang menyembunyikan makna pesan sementara eksistensi pesan tetap ada. Steganografi membutuhkan dua komponen utama, yaitu media penampung dan pesan rahasia, yang dewasa ini berupa berkas digital. Ringkasnya, steganografi adalah teknik menanamkan embedded-message pada suatu cover-object, dimana hasilnya berupa stego-object. Karakteristik steganografi yang baik adalah imperceptibility tinggi, fidelity tinggi, dan recovy maksimum.*

Semua teknik steganografi dengan cover-object citra digital yang tradisional memiliki kapasitas penyembunyian informasi yang sangat terbatas, yaitu hanya sekitar 10% dari ukuran cover-image. Hal ini dikarenakan prinsip teknik tersebut adalah mengganti bagian penting pada frekuensi komponen, atau mengganti least significant bit dari cover-image dengan pesan rahasia.

Teknik steganografi yang dibahas di makalah ini menanam pesan rahasia dalam bit-plane dari cover-image. Teknik ini memanfaatkan karakteristik penglihatan manusia yang tidak bisa mengerti bentuk informasi dalam suatu pola biner yang sangat rumit. Kita dapat mengganti wilayah yang "noise-like" pada cover-image dengan data rahasia, tanpa merusak kualitas cover-image. Teknik ini dinamakan Bit-Plane Compelexity Segmentation Steganography.

Teknik ini ditemukan oleh Eiji Kawaguchi dan Richard O. Eason. Bagaimana perbandingan teknik BPCS dengan teknik LSB akan dijelaskan pada bagian makalah ini.

Kata Kunci*: steganografi, kriptografi, media penampung, pesan rahasia, embedded message, cover-object, stego-object, cover-image, imperceptibility, fidelity, recovery, bit-plane, noise-like, Bit-Plane Complexity Segmentation.*

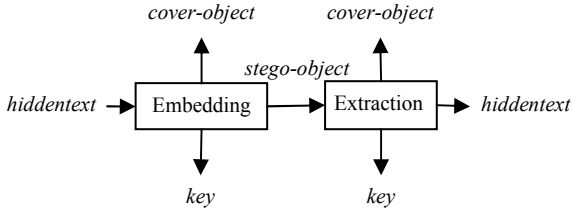
1. PENDAHULUAN

Dewasa ini, pertukaran informasi di internet telah menjadi bagian yang penting dalam perkembangan teknologi informasi di seluruh dunia. Namun, sesungguhnya media internet bukanlah media yang aman untuk pertukaran informasi. Seseorang bisa saja menyadap aliran data pengiriman email penting. Atau bahkan mengganggu transaksi online.

Oleh karena itu, digunakanlah teknik kriptografi. Sesuai perkembangan jaman, teknik kriptografi klasik berubah menjadi teknik kriptografi modern yang beroperasi pada satuan bit atau byte. Namun dengan kriptografi, walaupun makna suatu pesan menjadi hilang atau kacau, keberadaan akan pesan rahasia tersebut masih diketahui. Hal tersebut membuat penyadap informasi menyadari adanya pesan rahasia yang disembunyikan, dan mengundang kriptanalis untuk melakukan kriptanalisis.

Sedangkan, steganografi bisa dikatakan sangat kontras dengan kriptografi. Steganografi adalah teknik menyembunyikan keberadaan pesan rahasia dalam suatu penampung. Salah satu penggunaan steganografi klasik yang pernah dipakai adalah menyembunyikan pesan rahasia pada kepala budak yang dibotaki, lalu mengirimnya setelah kepala budak ditumbuhi rambut lagi. Steganografi modern menggunakan berkas digital untuk penampung pesannya. Berkas digital yang digunakan untuk penampung bisa bervariasi, mulai dari berkas teks, citra, suara (audio), atau bahkan video klip (audio-video). Steganografi juga sering disebut sebagai langkah setelah kriptografi karena pada kenyataannya, pesan yang disembunyikan sering dienkripsi terlebih dahulu.

Langkah steganografi secara umum adalah:



Gambar 1 Langkah-langkah steganografi secara umum

Tiap teknik steganografi biasanya berbeda tergantung jenis cover-object yang digunakan. Ada bermacam-macam teknik steganografi dengan cover-object berupa berkas citra. Beberapa teknik diantaranya menggunakan least significant bit untuk menyembunyikan data. Lainnya menggunakan teknik frekuensi spasial. Lainnya lagi menggunakan sampling error dalam image digitization. Namun, seluruh teknik tersebut hanya mampu menampung sekitar 5-15% dari ukuran cover-object nya.

Teknik yang akan dijelaskan pada makalah ini adalah teknik yang tidak berdasarkan teknik pemograman, tetapi teknik yang menggunakan sifat penglihatan manusia. Sifat penglihatan manusia yang dimanfaatkan yaitu ketidak-mampuan manusia menginterpretasi pola biner yang "noise-like". Pola tersebut akan diterangkan pada bagian berikutnya.

2. Teknik Steganografi BPCS

Teknik steganografi BPCS sebenarnya cukup sederhana, tetapi ada beberapa term, istilah, dan konvensi tertentu yang perlu diketahui. Term-term tersebut akan dijelaskan kemudian.

2.1. Bit-Plane

Sebuah citra multi-valued (citra dengan kedalaman warna lebih dari 1 bit) memiliki himpunan n-gambar biner. Sebagai contoh, misalkan ada citra dengan kedalaman n-bit, kita dapat menunjukkan

$$P = (P_1, P_2, \ldots, P_n) \quad (1)$$

Jika citra terdiri dari 3 warna, red, green, blue, maka citra P,

$$P = (P_{R1}, P_{R2}, \ldots, P_{Rn}, P_{G1}, P_{G2}, \ldots, P_{Gn}, P_{B1}, P_{B2}, \ldots, P_{Bn}) \quad (2)$$

Himpunan bit-plane pada citra biasanya direpresentasikan dengan Pure Binary Code. Selain dengan representasi itu, ada juga sistem representasi Canonical Gray Code. Representasi ini akan lebih baik diterapkan dalam pada teknik steganografi BPCS.

2.2. Kompleksitas citra biner

Sebetulnya tidak ada definisi standar tentang nilai kompleksitas suatu citra biner. Definisi kompleksitas yang akan digunakan pada makalah ini adalah definisi yang diadopsi dari paper milik Kawaguchi, yaitu black-white border image complexity.

Panjang pembatas hitam-putih dalam sebuah citra biner adalah ukuran yang bagus untuk mengukur kompleksitas citra. Jika pembatasnya panjang maka citra disebut kompleks. Total panjang pembatas hitam-putih adalah jumlah perubahan warna tiap baris dan kolom suatu citra. Sebagai contoh sebuah piksel hitam yang dikelilingi background putih memiliki panjang border 4.

Definisi kompleksitas citra biner adalah sebagai berikut:

$$\alpha = \frac{k}{\textit{Kemungkin maksimum perubahan biner dalam citra}}$$

Dimana k adalah total panjang pembatas hitam-putih. Jadi nilainya α berkisar antara:

$$0 \leq \alpha \leq 1 \quad (2)$$

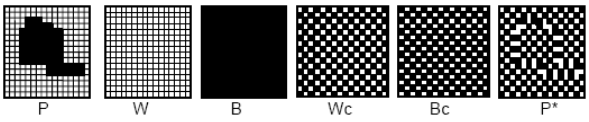
Pengukuran kompleksitas citra biner juga dapat diterapkan pada bagian dari citra biner.

2.3. Analisis bagian informatif dan "noise-like"

2.3.1. Konjugasi citra biner

Sebelum bisa menentukan bagaimana citra biner yang informatif dan bagaimana yang seperti noise, kita perlu mengetahui tentang konjugasi suatu citra biner

Misalkan P adalah citra hitam-putih berukuran 2^N x 2^N dengan gambar hitam sebagai foreground dan gambar putih sebagai background, W dan B masing-masing menunjukkan pola semua putih dan semua hitam. Lalu ada pola papan catur Wc dan Bc, dimana Wc memiliki piksel putih pada posisi atas-kiri, dan Bc sebagai komplemennya.



P diintepretasi sebagai berikut: piksel pada foreground memilik pola B dan piksel pada background memiliki pola W. Lalu kita definisikan P* sebagai konjugasi dari P yang memenuhi:

1. Bentuk foreground memiliki bentuk yang sama dengan P
2. Bagian foreground memiliki pola Bc
3. Bagian background memiliki pola Wc

Dengan demikian pernyataan berikut akan selalu bernilai benar:

1. P* = P xor Wc
2. (P*)* = P
3. P* ≠ P
4. Jika α(P) adalah kompleksitas P, maka α(P*) = 1 - α(P)

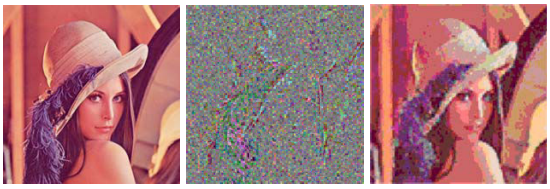
2.3.2. Kriteria bagaimana bagian bit-plane adalah informatif atau seperti noise

Pertama-tama kita harus mencari nilai kompleksitas untuk semua kemungkinan citra biner pada segmen tertentu, misal untuk segmen 8x8 piksel. Namun untuk melakukannya terlalu lama, oleh karena itu digunakan simulasi berupa penciptaan citra-biner secara acak untuk ukuran 8x8 piksel. Setelah itu kita lihat ternyata kompleksitas terdistribusi normal, dan ternyata rata-rata kompleksitas adalah 0.5. Lalu deviasi standarnya adalah 0.047, dinotasikan dengan sigma.

Untuk membuang data berarti mengganti citra sebelumnya dengan pola lain. Jika Pola lokal α_L dan pola baru dengan kompleksitas α, maka jika $\alpha_L \leq \alpha$ maka citra masih dapat dibuang. Jika $\alpha = \alpha_L$ adalah kompleksitas minimum agar citra tetap baik, maka α_L digunakan sebagai threshold value.

Supaya dianggap penting, jika suatu citra masih berupa citra yang mirip setelah dibuang dengan data citra lain dengan kompleksitas α dimana $\alpha = \alpha_U$ dan jika kita buang lagi menghasilan nilai yang semaking tidak mirip citra tersebut, maka α_U digunakan sebagai batas informatif kompleksitas citra.

Jika α_L dan α_U sama nilainya, maka nilai tersebut dapat digunakan untuk membagi apakash citra informatif atau mirip noise. Nilai tersebut disebut α_0



Gambar di atas menunjukkan bahwa jika kita mengganti bagian bit-plane yang kompleksitasnya rendah, hasilnya akan seperti gambar ke-2, jika kita mengganti segmen bit-plane yang kompleksitasnya tinggi, hasilnya akan seperti gambar ke-3.

2.4 Algoritma BPCS Steganography

BPCS adalah teknik steganografi yang memiliki kapasitas penyembunyian yang besar. Sepeti yang telah dibahas sebelumnya, segmen bit-plane yang dianggap noisy dapat diganti dengan pesan rahasia yang ingin kita embed. Berikut ini langkah kerjanya, dengan menganggap bahwa segmen citra biner yang dipakai adalah 8x8 piksel dan format cover object adalah citra berkas BMP.

1. Ubah cover-object menjadi himpunan bit-plane dengan representasi CGC (representasi BMP yang normal adalah PBC).
2. Pecah tiap segmen bit-plane menjadi segmen yang informatif dan noise-like dengan nilai threshold yang ditentukan. Biasanya nilai threshold $\alpha_0 = 0.3$.
3. Pecah berkas pesan rahasia menjadi sekumpulan secret block dimana secret block tersebut adalah block yang seukuran nilai bit piksel segmen, jika segmen 8x8 maka nilai blok senilai 8x8 bit.
4. Jika blok (misalkan blok S) kurang kompleks dibandingkan nilai threshold, maka konjugasikan untuk membuat block S* dengan kompleksitas yang pasti lebih kompleks dibandingkan threshold
5. Tanam blok pesan rahasia pada hasil langkah-4 kepada segmen bit-plane yang noise-like, dengan cara menggantinya. Jika blok pesan rahasia adalah blok pesan rahasia yang terkonjugasi, makan, simpan dalam "conjugation map"
6. Tanam juga conjugation map setelah menanam seluruh blok pesan rahasia.
7. Petakan kembali format representasi dari CGC ke PBC agar bisa dibaca sebagai berkas BMP yang standar.

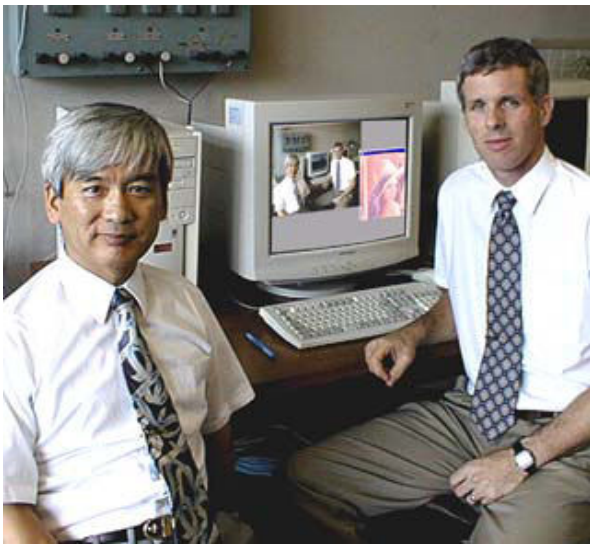
Dari langkah tersebut, hasilnya kita mendapatkan stego-object. Lalu cara mengekstrak informasinya adalah dengan:

1. Ubah stego-object dari representasi PBC ke CGC
2. Tentukan segmen mana yang informatif dan segmen mana yang noise-like dengan threshold yang sama dengan threshold ketika proses embedding. Dengan kata lain nilai threshold adalah salah satu dari stego-key.
3. Ambil segmen data dari segmen bit-plane yang dianggap noise-like.
4. Terjemahkan tiap segmen data tersebut menjadi blok data
5. Terjemahkan juga conjugation map
6. Lakukan tranformasi yang diperlukan agar terutama untuk mengetahui segmen mana yang telah dikonjugasi.
7. Rangkai blok-blok tersebut menjadi pesan rahasia yang diinginkan.

3. HASIL DAN PEMBAHASAN

3.1. Pengujian Algoritma BPCS

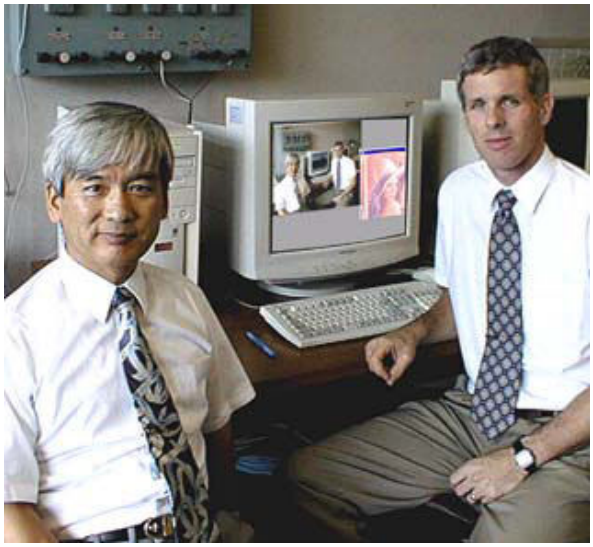
Berikut ini hasil simulasi menggunakan program steganografi BPCS. Untuk berkas yang diuji, kita menggunakan berkas di bawah:



Gambar 2 Cover-Objet Steganografi BPCS

Berkas tersebut adalah berkas bmp berukuran 617 x 504 piksel. Data yang akan diembed adalah berupa beberapa berkas gambar BMP juga. Total berkas gambar yang ditanam dalam gambar di atas adalah sebanyak 1,212,744 byte (melebihi ukuran cover-objectnya!) yang kemudian dikompres secara lossless dengan algortima tertentu sampai berukuran 441,318 byte.

Berikut di bawah ini adalah gambar hasil steganografi, yaitu stego-objectnya.



Gambar 3 Stego-object BPCS steganography

Gambar 4 Embedded-message steganografi BPCS

Ukuran berkas original adalah 933,408 byte. Ternyata BPCS mampu menampung berkas berukuran 441,318 byte dalam cover-object. Dengan kata lain kapasitas penyimpanannya mencapai 30% lebih. Selain itu jika kita hitung lagi bahwa data yang ditanam adalah hasil kompresi dari ukuran 1,212,744 byte, hasil steganografi ini terasa menakjubkan. Lebih baik lagi jika hasil stego-object dikompresi dengan kompresi yang lossless. Pada simulasi ini, kompresi dilakukan sampai stego-object berukuran 505,502 byte. Dengan kata lain data yang disimpan dalam stego-object berukuran 505,502 byte ini adalah sebanyak data embedded message yang belum dikompresi yaitu sebesar 1,212,744 byte. Pesan yang disimpan mencapain 2.5x ukuran stego-object!

3.2. Perbandingannya dengan metode LSB biasa

Metode LSB biasa jelas telah terbukti telah memiliki sifat imperceptibility yang baik, tetapi, kapasitas data nya cukup kecil, karena hanya bisa menyimpan pada least significant bit setiap piksel pada tiap warna. Jika gambar yang akan diuji dengan steganografi biasa adalah gambar yang sama dengan gambar di atas, kapasitas data-hiding maksimumnya adalah:617 x 504 x 3 bit adalah 116613 byte. Sedangkan data yang akan diembed adalah sebesar 441,318 byte, dengan teknik BPCS, penanaman data tersebut dapat dilakukan.

Namun kapasitas BPCS juga tergantung pada kualitas cover-object. Penelitian menunjukkan bahwa cover-object yang berupa hasil foto kamera digital memiliki kapasitas yang cenderung lebih baik dari citra hasil olahan komputer.

Namun karena teknik ini tergantung pada kualitas cover-object, ada kelemahan yang bisa timbul. Hal ini terutama karena representasi bit-plane PBC maupun CGC kadang-kadang tidak mampu menghasilkan hasil sesuai. Misalnya kadang-kadang bagian citra yang terlihat seperti informatif oleh mata manusia (memiliki pergantian warna yang sedikit), ketika direpresentasikan dalam PBC maupun CGC akan terlihat seperti noise. Hal ini tentu harus dihindari, karena akan mengganggu imperceptibility stego-object.

4. KESIMPULAN

Kesimpulan makalah ini:

1. Kapasitas penyimpanan data dengan teknik BPCS lebih baik daripada metode LSB, metode LSB hanya sekitar 10%, sedangkan dengan BPCS, bisa sekitar 30-50%.
2. Kekurangan metode BPCS dibandingkan metode LSB adalah kapasitas data hiding terlalu tergantung kepada jenis cover-object.
3. BPCS secara keseluruhan memiliki proses yang lebih rumit dari metode LSB. Hal ini bisa dilihat dari jumlah langkah-langkah yang dimiliki metode BPCS. Walaupun begitu, dengan teknologi komputer saat ini, waktu proses tidak terasa begitu lama.

DAFTAR REFERENSI

[1] Rinaldi M, *Diktat Kuliah IF5054 Kriptografi*, Institut Teknologi Bandung 2006.

[2] Eiji Kawaguchi, et al: Depth-First Picture Expression Viewed from Digital Picture Processing, IEEE Trans. on PAMI, Vol.PAMI-5,No.4, pp.343-384, July, 1983.

[3] Sei-ichiro Kamata, et al: Depth-First Coding for Multi-Valued Pictures Using Bit-Plane Decomposition, IEEE Trans. on CT, Vol.43,No.5, pp.1961-1969, May, 1995.

[4] Koichi Nozaki, et al: A Large Capacity Steganography Using Color BMP Images, Proc. ACCV'98, pp.112-119, (1998-01).

[5] Eiji Kawaguchi, et al: Principle and applications of BPCS-Steganography, SPIE's International Symposium on Voice, Video, and Data Communications, (1998-11