STEGANOGRAFI DENGAN CHAOTIC LEAST SIGNIFICANT BIT ENCODING PADA TELEPON GENGGAM

Susany Soplanit [*], Constantine Bandaria [**]
*) Program Studi Sistem Komputer
**) Program Studi Teknik Informatika
Fakultas Teknologi Informasi Universitas Tarumanagara
Jl. Let.Jend. S. Parman No.1, Jakarta Barat – 11440
Email: susany@tarumanagara.ac.id

ABSTRAK: Telepon genggam saat ini dapat digunakan untuk menyimpan data-data yang bersifat pribadi atau rahasia, oleh karena itu pengamanan data pada telepon genggam akan menjadi hal yang penting di masa ini ataupun di masa yang akan datang. Sistem pengamanan data yang efektif pada telepon genggam selain kriptografi adalah Steganografi yaitu penyembunyian data dalam sebuah media. Dalam perancangan ini metode yang digunakan adalah *Chaotic Least Significant Bit Encoding* (CLSBE). Hasil pengujian membuktikan bahwa pesan yang tersembunyi dalam citra digital dengan format PNG masih dapat diambil kembali dengan benar. Implementasi pada emulator telah berjalan dengan baik, namun untuk telepon genggam perlu penyesuaian dengan fasilitas pada telepon tersebut.

Kata kunci: *CLSBE, steganografi, stego-image, cover-image.*

***ABSTRACT**: The issues of security in mobile phone in recent days become crucial. Many privacy or secretly data is stored using unsecured protocol or sometimes without the security procedures at all. This will lead to great awareness about security in mobile phone. The effective ways to secure data are steganography and cryptography. The first one concentrate to data hiding in a certain media. In this paper, we present Chaotic Least Significant Bit Encoding (CLSBE) as a steganography method in our system design. The experiment results show that hidden messages in PNG form can be retrieved correctly. The implementation of system in emulator works well but depends on mobile phone features and environment.*

***Keywords**: CLSBE, steganografi, stego-image, cover-image.*

PENDAHULUAN

Dengan teknologi telekomunikasi yang ada saat ini penyampaian informasi sangatlah mudah dan cepat. Banyak perangkat keras yang dapat digunakan untuk mengirim atau menerima suatu informasi. Salah satu perangkat keras yang cukup banyak digunakan pada saat ini adalah telepon genggam (*hand phone*). Tercatat lebih dari 1,5 miliar para pengguna telepon genggam atau sekitar seperempat dari penduduk di dunia [1], dan sekitar 20 juta para pengguna telepon genggam di Indonesia yang masih akan terus berkembang [2].

Keamanan pada suatu informasi atau data pada saat ini dapat dibagi menjadi dua, yakni: Kriptografi dan Steganografi. Dari dua metode tersebut, metode yang satu dapat menjadi tambahan bagi metode yang lain. Kriptografi adalah suatu seni untuk mengacak suatu informasi atau data yang memiliki arti, menjadi sesuatu yang tidak dapat dimengerti atau seakan-akan tidak berarti. Berbeda dengan kriptografi, Steganografi adalah suatu seni untuk menyembunyikan suatu data, dimana data tersebut disembunyikan ke dalam suatu media yang tampak biasa saja [9]. Media informasi yang umum dipakai adalah media gambar atau citra. Sehingga untuk melakukan penyembunyian pesan ke suatu citra tidak akan menimbulkan banyak perhatian dari pihak-pihak yang tidak dikehendaki.

Dengan mempertimbangkan keunggulan dari steganografi pada citra, dan juga dengan semakin berkembangnya perangkat keras telepon genggam, maka akan dirancang suatu aplikasi steganografi sebagai salah satu cara untuk mengamankan suatu informasi pada telepon genggam. Metode steganografi yang dipakai merupakan metode yang berbasis sistem *chaos*. Dalam ilmu fisika dan matematika, teori *chaos* berhubungan dengan suatu kegiatan atau kebiasaan sistem non linear yang dinamis, yang untuk beberapa kondisi menampilkan sebuah fenomena acak (*chaos*) [3]. Salah satu metode *chaos* yang ada adalah *Chaos Least Significant Bit Encoding* (CLSBE). Metode ini diambil karena merupakan salah satu metode yang

sederhana dan tidak membutuhkan algoritma yang terlalu rumit, sehingga kapasitas pada telepon genggam yang terpakai kecil. Penggunaan citra digital dibatasi pada citra dengan format PNG (*Portable Network Graphic*) karena format ini telah didukung oleh hampir semua telepon genggam.

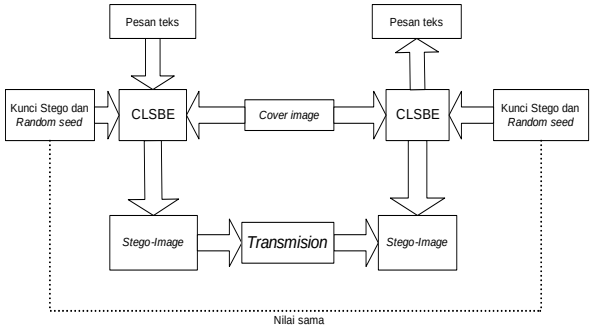
STEGANOGRAFI

Steganografi adalah sebuah seni dan ilmu untuk menyembunyikan sebuah pesan dengan cara yang sedemikian rupa sehingga tidak ada orang lain, selain dari penerima yang dituju yang mengetahui mengenai pesan tersebut [8]. Keunggulan steganografi dari kriptografi adalah kemampuannya untuk membuat suatu pesan rahasia menjadi tidak terlihat, atau tidak mengundang orang lain yang tidak mengetahui untuk peduli atau penasaran, lain halnya dengan kriptografi yang mengacak sebuah pesan tertulis menjadi suatu yang tidak berarti, yang dapat membuat orang lain menjadi penasaran dan ingin mengetahui arti dari pesan acak tersebut, hingga akhirnya melakukan percobaan untuk menerjemahkan pesan tersebut.

Steganografi biasanya terdiri dari dua sistem, yaitu sistem untuk menyembunyikan pesan dan sistem untuk mengambil pesan. Dalam sistem-sistem tersebut terkandung enam komponen penyusun, antara lain [9]:

1. Pesan rahasia (M)
2. *Cover Document* (C)
3. *Stego Document* (Z)
4. *Stego Key* (K)
5. Fungsi penyembunyi $f(M,C,K) \rightarrow Z$
6. Fungsi detektor $f'(Z,C,K) \rightarrow M$

Untuk steganografi pada gambar digital tentunya *cover document* dari komponen-komponen di atas adalah sebuah citra digital atau biasa disebut *cover-image*. Steganogafi ini akan menghasilkan output berupa citra baru yang mengandung pesan yang sudah disembunyikan oleh algoritma steganografi, secara umum disebut *stego-image*. Dalam steganografi pengirim dan penerima harus memiliki kunci *(stego-key)* yang sama yang tentunya dirahasiakan dari pihak-pihak lain yang tak diinginkan untuk mengetahui isi pesan tersebut. Selain itu penerima harus menggunakan gambar yang mengandung pesan tersembunyi *(stego-image)* untuk dapat menerima pesan rahasia tersebut. Untuk lebih jelas mengenai diagram steganografi, dapat dilihat pada Gambar 1.



Gambar 1. Diagram Alur Proses Steganografi

CHAOTIC LEAST SIGNIFICANT BIT ENCODING

Salah satu metode yang paling sederhana dalam steganografi adalah penyembunyian pesan pada *Least Significant Bit* dari setiap *pixel* pada *cover-image* nya, karena pada gambar digital perubahan satu-dua bit pada setiap *pixel* tidak akan terlihat oleh mata telanjang.

Sebelum proses penyembunyian pesan dilakukan, terlebih dahulu ditentukan lokasi penyembunyiannya. Penentuan dari lokasi penyembunyian pada gambar digital ditentukan dengan cara sebagai berikut[10]:

1. Untuk *cover-image* RGB $c(x, y) = [R_c, G_c, B_c]$ berukuran MxN, tentukan sebuah *random seed* dan bangkitkan *pseudorandom number* kemudian susun menjadi sebuah *pseudo-image* RGB $p(x, y) = [R_p, G_p, B_p]$ berukuran MxN.
2. Hitung jarak antara $c(x, y)$ dan $p(x, y)$ dengan menggunakan rumus jarak dua vektor

$$d(x,y) = \sqrt{(R_c - R_p)^2 + (G_c - G_p)^2 + (B_c - B_p)^2} \quad (1)$$

3. Penyembunyian dimulai dari lokasi dengan jarak terkecil hingga jarak terbesar. Pengurutan jarak menggunakan algoritma pengurutan data.

Setelah penentuan lokasi selesai, maka proses selanjutnya adalah melakukan penyembunyian pesan. Penyembunyian pesan pada gambar digital dengan format RGB (masing-masing 8 bit) dilakukan dengan proses sebagai berikut:

1. Tentukan *random seed* dan bangkitkan *pseudo-random number* $x_i \ {}_{i=0}^{MN+1}$ kemudian ubah menjadi $b_i \ {}_{i=0}^{MN+1}$ dengan

$$b_i \ {}_{i=0}^{MN+1} = \begin{cases} 0 \ ; \ x_i = genap \\ 1 \ ; \ x_i = ganjil \end{cases} \quad (2)$$

2. Susun *pseudo-image* $p(x,y)= b_{k-1} + 2b_{k+1}$ (3) dengan $k = (x-1)' N + y$
3. Bit-bit informasi a_i akan disembunyikan pada pixel $c(x,y)$ dengan ketentuan:
   a. Sembunyikan 3 bit a_i di LSB *Red, Green, Blue* jika $p(x,y)= 0$
   b. Sembunyikan 1 bit a_i di LSB *Red* jika $p(x,y)= 1$
   c. Sembunyikan 1 bit a_i di LSB *Green* jika $p(x,y)= 2$
   d. Sembunyikan 1 bit a_i di LSB *Blue* jika $p(x,y)= 3$
4. Tentukan *random seed* kedua dengan cara ROL (*random seed*) kemudian bangkitkan *pseudorandom number* x_i yang baru sebanyak bit data a_i. x_i akan menentukan apakah a_i akan disembunyikan di LSB pertama atau LSB kedua sebuah komponen $c(x,y)$ dengan ketentuan sebagai berikut:
   a. Sembunyikan a_i di LSB pertama jika x_i genap.

$$c'(x,y)=\begin{cases} c(x,y)+1 & ; \ LSB_1[c(x,y)]=0 \,\&\, a_i=1 \\ c(x,y)-1 & ; \ LSB_1[c(x,y)]=1 \,\&\, a_i=0 \\ c(x,y) & ; \ otherwise \end{cases} \quad (4)$$

   b. Sembunyikan a_i di LSB kedua jika x_i ganjil.

$$c'(x,y)=\begin{cases} c(x,y)+1 & ; \ LSB_2[c(x,y)]=0 \,\&\, a_i=1 \\ c(x,y)-1 & ; \ LSB_2[c(x,y)]=1 \,\&\, a_i=0 \\ c(x,y) & ; \ otherwise \end{cases} \quad (5)$$

Proses deteksi informasi tersembunyi secara umum sama dengan proses penyembunyian informasi. Perbedaannya hanya pada saat pengambilan informasi dari LSB sebuah komponen $c(x,y)$ (langkah keempat pada proses penyembunyian) menggunakan [10]:

$$a'_i=\begin{cases} c'(x,y)\ AND\ 1 \ ; \ x_i = genap \\ c'(x,y)\ AND\ 2 \ ; \ x_i = ganjil \end{cases} \quad (6)$$

IMPLEMENTASI

Implementasi algoritma CLSBE dilakukan dengan 2 cara, yaitu:

1. Penyembunyian 1 bit dilakukan di bit pertama

a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

2. Penyembunyian 1 bit dilakukan di bit kelima

a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0

Format *key* yang diinputkan untuk proses steganografi berupa teks dengan panjang maksimal 10 karakter. Setiap karakter tersebut diambil diubah menjadi kode ASCII kemudian dijumlahkan menjadi bilangan bulat yang digunakan sebagai *random seed* awal proses steganografi. Contohnya, *key* yang diinputkan adalah ABC dimana A = 65, B = 66, C = 67. *Random seed* yang dihasilkan dari ABC adalah 65 + 66 + 67 = 198. Sedangkan untuk proses pengurutan data, mengunakan algoritma Bubble Sort.

Implementasi menggunakan J2ME yang dijalankan pada emulator maupun telepon genggam Sony Ericsson W810 dengan menggunakan citra format PNG. Setelah aplikasi selesai dibuat, dilakukan pengujian. Pengujian dibagi menjadi dua bagian, yaitu pengujian yang dilakukan pada emulator telepon genggam dan pengujian pada telepon genggam yang sebenarnya. Pada Tabel 1 terdapat gambar asli, gambar steganografi beserta hasil yang didapat ketika aplikasi mencoba untuk mendapatkan pesan yang tersembunyi, dengan seluruh input yang dimasukan adalah benar.

Untuk penyembunyian yang dilakukan di bit ke-1, pengujian yang dilakukan pada emulator berhasil dengan baik, semua pesan ditampilkan dengan baik jika input-inputnya benar. Sedangkan pengujian yang dilakukan pada telepon genggam Sony Ericsson W810 tidak berjalan dengan yang direncanakan. Dikarenakan telepon genggam tersebut hanya mempunyai kedalaman warna yang berbeda dengan format file PNG yang dihasilkan aplikasi, yaitu 24 bit, oleh karena itu bit pesan yang dibaca telepon genggam ada yang hilang, sehingga pesan tersembunyi tidak dapat ditampilkan dengan baik walaupun pengguna memasukan *input-input* yang benar.

Namun, jika penyembunyian setiap bit pesan bukan disembunyikan pada bit ke-1 (LSB), melainkan pada bit ke-5, maka aplikasi ini akan menampilkan pesan tersembunyi dengan baik. Tabel 2 menampilkan hasil pengujian dengan penyembunyian dilakukan pada bit ke-5.

Tabel 1. Hasil pengujian pada bit ke-1 di emulator dan telepon genggam

	Key	PNG file: blank1	PNG file: stegoImage	Pesan	Pesan terbaca
Emulator Sony Ericsson W800	ABCDEF			Untar	Untar
Emulator Standar J2ME WTK	ABCDEF			Untar	Untar
Telepon Gengam W810	ABCDEF			Untar	U||||

Tabel 2. Hasil pengujian pada bit ke-5 di emulator dan telepon genggam

	Key	PNG file		Pesan	Pesan terbaca
		blank1	stegoImage		
Emulator Sony Ericsson W800	ABCDEF			Untar	Untar
Emulator Standar J2ME WTK	ABCDEF			Untar	Untar
Telepon Gengam W810	ABCDEF			Untar	Untar

PEMBAHASAN

Kegunaan aplikasi steganografi dengan metode CLSBE ini berdasarkan hasil pengujian secara keseluruhan yaitu memiliki kemampuan untuk menyembunyikan pesan ke dalam sebuah gambar. Dimana gambar tersebut jika dilihat dengan mata telanjang tidak terdapat perubahan. Program aplikasi ini juga dapat mengambil kembali pesan yang disembunyikan tersebut dengan baik, jika telepon genggam mendukung.

Keterbatasan pada aplikasi ini dibagi menjadi dua, keterbatasan yang berasal dari aplikasi dan keterbatasan yang berasal dari luar aplikasi (telepon genggam). Keterbatasan yang berasal dari aplikasi, yaitu:

1. Kecepatan proses penyembunyian data terasa lambat.
2. Program aplikasi ini tidak dapat berjalan pada ponsel yang tidak mendukung PDAAPI, MIDP 2.0, CLDC 1.1.
3. Pengguna tidak dapat memilih sendiri lokasi penyimpanan hasil dari steganografi. Aplikasi yang menentukan sendiri lokasi penyimpanannya yaitu di c:\pictures. Oleh karena itu aplikasi ini hanya dapat berjalan dengan baik pada vendor Sony ericsson dan vendor lainnya, jika path yang dimiliki telepon genggam tersebut sama dengan path yang telah ditentukan.
4. Tidak menampilkan *progress bar* secara *real-time*, sehingga pengguna tidak mengetahui proses penyembunyian data berjalan atau tidak.

Sedangkan keterbatasan yang berasal dari luar aplikasi adalah kedalaman bit-bit gambar yang berbeda-beda pada tiap telepon genggam, yang mengakibatkan adanya bit-bit yang hilang pada saat proses pengambilan pesan pada gambar steganografi. Untuk penyembunyian pada bit ke-1, tidak dapat diterapkan pada telepon genggam Sony Ericsson W810, namun penyembunyian pada bit ke-5 berhasil dengan baik pada telepon genggam Sony Ericsson W810.

KESIMPULAN

Kesimpulan yang dapat diambil dari perancangan dan pembuatan program aplikasi steganografi dengan metode CLSBE pada telepon genggam ini antara lain:

1. Program aplikasi ini dapat melakukan penyembunyian pesan dan melakukan deteksi pesan tersembunyi dengan baik pada emulator Sony ericsson.
2. Program aplikasi ini sudah berjalan dengan baik pada emulator J2ME WTK dan pada telepon genggam Sony W810. Untuk telepon genggam yang lain diperlukan penyesuaian baik dengan menggunakan metode penyembunyian pesan yang lain atau telepon genggam yang mendukung kedalaman warna 24 bit, yaitu kedalaman warna dari *stego image* yang dihasilkan oleh aplikasi.
3. *Password* atau *key* yang digunakan untuk melakukan proses penyembunyian dan pengambilan pesan harus sama, jika *password* atau *key* yang dimasukan berbeda ketika mengambil suatu pesan tersembunyi, maka pesan yang ditampilkan juga tidak akan sama dengan pesan yang disembunyikan.

Berdasarkan hasil perancangan dan pembuatan program aplikasi ini, ada beberapa saran agar dapat dilanjutkan dengan beberapa pengembangan, antara lain:

1. Program aplikasi ini diharapkan dapat dikembangkan untuk dapat membaca pesan yang tersembunyi pada telepon genggam dengan cara menggunakan metode penyisipan gambar yang berbeda, misalnya dengan melakukan penyisipan gambar pada bit ke lima, sehingga aplikasi dapat bekerja dengan baik pada telepon genggam yang kedalaman warnanya kurang dari 24 bit.
2. Perlu dilakukan penelitian pada berbagai jenis ponsel sehingga dapat diperbaiki untuk diterapkan pada berbagai jenis ponsel.
3. Proses dari program aplikasi ini dapat dipercepat jika menggunakan algoritma sorting *quick sort* atau *radix sort*, yang memiliki tingkat kecepatan dalam melakukan pengurutan data di atas dari kecepatan *bubble sort* dalam mengurutkan data [11].

DAFTAR PUSTAKA

1. Suara Merdeka. Seperempat Warga Dunia Pakai HP.*http://www.suaramerdeka.com/harian/0412/10 / int7.htm*. 10 Desember 2004.
2. Tempo Interaktif. MMS Lintas Tiga Operator, *http://www.tempointeraktif.com/hg/ekbis/2004/04/ 13/ brk*, 20040413-13, id.html, 13 April 2004.
3. Wikipedia. Chaotic. *http://en.wikipedia.org/wiki/ Chaotic*. 10 Febuari 2006.
4. Wikipedia.Digital Image. *http://en.wikipedia.org/ wiki/Digital_image*. 3 Februari 2006.
5. Wikipedia. Pixel, *http://en.wikipedia.org/wiki/Pixel*. 3 Februari 2006.
6. Wikipedia. Bitmap. *http://en.wikipedia.org/wiki/ Bitmap*. 3 Februari 2006.
7. Wikipedia. PNG. *http://en.wikipedia.org/wiki/PNG* 5 Febuari 2006.
9. Wikipedia.Steganography*: http://en.wikipedia.org/ wiki/Steganography*. 4 Febuari 2006.
9. Lin, Eugene T. and Delp, Edward J. A Review of Data Hiding in Digital Image, *http://www.ece. purdue.edu/ ~ace*, 18 Juli 2004.
10. Susany Soplanit, Sendy Christina Sunarsa, Dali Santun Naga. *Pengamanan Data dengan Chaotic Least Significant Bit Encoding (Clsbe) dan New Chaotic Substitution Image Encryption (NCSIE)*. Prosiding Seminar Nasional SIIT 2005, Universitas Kristen Petra, Surabaya, 28 Juli 2005.
11. Wikipedia. Bubble sort. *http://en.wikipedia.org/ wiki/Bubble_sort*. 31 Mei 2006.