IMPLEMENTASI STEGANOGRAFI IMAGE MENGGUNAKAN ALGORITMA LSB (LEAST SIGNIFICANT BIT), BBS (BLUM BLUM SHUT) DAN KOMPRESI HALF-BYTE PACKING PADA MMS (MULTIMEDIA MESSAGING SERVICE)

Ariyanto Mei Yuwono[1], Tjokorda Agung Budi Wirayuda[2], Retno Novi Dayawati[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Pengiriman pesan melalui media ponsel sudah biasa dipakai sekarang ini akan tetapi keamanan dari sebuah pesan tidak bisa terjamin. Pesan yang bersifat rahasia misalnya: pesan yang berisi nomor PIN atau password harus dijaga keamanannya dari pihak-pihak yang tidak berkepentingan, pesan yang digunakan untuk melakukan operasi rahasia kepolisisan seperti operasi penangkapan atau penggrebekan terhadah buronan juga harus dijaga keamanannya sehingga informasi tersebut tidak bocor. Untuk itu diperlukan adanya aplikasi untuk menyembunyikan pesan sehingga pesan yang dikirim tidak diketahui pihak lain. Penyembunyian pesan menggunakan Steganografi image akan dapat menyembunyikan pesan yang dikirim pada media image sehingga orang lain tidak sadar bahwa image tersebut telah disisipi oleh sebuah pesan rahasia.

Steganografi yang digunakan adalah LSB dengan pengacakan tempat penyisipan menggunakan BBS. Sebelum pesan disisipkan dilakukan kompresi menggunakan half-byte packing. Steganografi image dikirimkan menggunakan ponsel dengan fasilitas MMS.

Setelah dilakukan percobaan terbukti bahwa steganografi LSB dengan pengacakan BBS dan kompresi LSB dapat menyembunyikan pesan dan dapat diimplementasikan dengan baik pada ponsel. Penggunaan pengacakan BBS dapat menghasilkan pesan yang berbeda jika kunci yang digunakan salah. Kompresi half-byte packing dapat mengkompresi pesan dengan space savings mencapai 42%.

Kata Kunci : steganografi, LSB, BBS, half-byte packing, MMS.

Abstract

Sending message from cellular phone is common used now, but the security of message could not reliable. The security of message for example, message that contains PIN number or password, must be protected from unauthorized people. Message, which is used for police private operation, like arrest or raid criminal operation, also must be protected in order its information is not leak. So that, application for hiding message from unauthorized people is needed. Hiding message by image steganography can hide sent message on image media so unauthorized people does not know that image is inserted by private message.

LSB is one of steganography algorithm which is used for this thesis, with BBS for randomization insertion place. Before inserting the message, half-byte packing is used for compretion. Image steganography is sent through MMS by cellular phone.

After the experiment, it is prove that LSB steganography with BBS randomization and compretion, LSB can hide message and can be implemented on cellular phone. BBS randomization can produce different message if the key is wrong. Half-byte packing compretion can compress the message with space savings until 42%.

Keywords : steganography, LSB, BBS, half-byte packing, MMS.

1. Pendahuluan

1.1 Latar Belakang

Pengiriman pesan melalui media ponsel sudah biasa dipakai sekarang ini akan tetapi keamanan dari sebuah pesan tidak bisa terjamin. Pesan yang bersifat rahasia misalnya: pesan yang berisi nomor PIN atau password harus dijaga keamanannya dari pihak-pihak yang tidak berkepentingan, pesan yang digunakan untuk melakukan operasi rahasia kepolisisan seperti operasi penangkapan atau penggrebekan terhadah buronan juga harus dijaga keamanannya sehingga informasi tersebut tidak bocor. Untuk itu diperlukan adanya aplikasi untuk menyembunyikan pesan sehingga pesan yang dikirim tidak diketahui pihak lain. Penyembunyian pesan menggunakan Steganografi image akan dapat menyembunyikan pesan yang dikirim pada media image sehingga orang lain tidak sadar bahwa image tersebut telah disisipi oleh sebuah pesan rahasia.

Image yang telah disisipi pesan rahasia tersebut dikirimkan menggunakan media ponsel melalui layanan MMS. Pemilihan media ponsel untuk mengirim dan menerima image karena ponsel merupakan alat telekomunikasi yang mayoritas selalu dibawa sehingga dapat fleksibel untuk digunakan kapanpun dan dimanapun.

Algoritma yang digunakan adalah steganografi LSB. Algoritma ini dipilih karena dapat melakukan proses steganografi dengan waktu yang relative cepat dan hanya menggunakan resource memori yang kecil. Kebutuhan akan kecepatan dan penggunaan memori yang kecil merupakan sesuatu yang harus dipenuhi karena aplikasi ini akan berjalan pada media/device ponsel yang memiliki keterbatasan dalam hal resource memori dan kemampuan memproses data.

Untuk meningkatkan keamanan steganografi LSB digunakan metode BBS untuk melakukan pengacakan lokasi penempatan bit-bit pesan ke dalam pixel-pixel pada image. Metode BBS merupakan metode pembangkit bilangan acak dengan menggunakan kunci (key) sehingga jika menggunakan key yang sama maka akan dapat membangkitkan bilangan acak yang sama pula. Dengan adanya key tersebut maka lokasi penempatan bit-bit dapat dibangkitkan kembali sehingga bit-bit yang disisipkan dapat disatukan lagi menjadi pesan sebelum disisipkan pada image.

Pada image steganografi terdapat keterbatasan tempat penampung bit-bit pesan. Bit-bit pesan yang dapat ditampung maksimal sebanyak jumlah pixel yang ada pada image wadahnya. Untuk meningkatkan jumlah pesan yang dapat disisipkan digunakan teknik kompresi data half-byte packing. Teknik ini dipilih karena pada setiap karakter pada kode ASCII memiliki perubahan yang mencolok pada setengah byte terakhir (4 bit terakhir) sehingga ada kemungkinan untuk dapat mengurangi jumlah bit pesan yang akan disisipkan.

1.2 Rumusan Masalah

Permasalahan yang dijadikan objek penelitian dalam tugas akhir ini antara lain :

1. Bagaimana mengimplementasikan image steganografi dengan algoritma LSB, BBS dan half-byte packing pada ponsel?
2. Apakah steganografi dengan algoritma LSB dapat menghasilkan stego image yang kualitasnya hampir sama dengan image aslinya?
3. Apakah algoritma kompresi half-byte packing dapat meningkatkan jumlah karakter pesan yang dapat disisipkan pada Image steganografi?
4. Apakah steganografi algoritma LSB tahan terhadap pengaruh kompresi JPEG dan impulsive noise?

Untuk menghindari meluasnya materi pembahasan tugas akhir ini, maka penulis membatasi permasalahan dalam tugas akhir ini hanya menggunakan media penyisipan berupa image dengan ukuran kurang dari 30kB.

1.3 Tujuan

Dalam tugas akhir ini, hal-hal yang diharapkan untuk dicapai adalah sebagai berikut :

1. Merancang dan membangun aplikasi dengan mengimplementasikan metode image steganografi dengan algoritma LSB, BBS dan half-byte packing pada ponsel.
2. Menganalisa performansi berdasarkan lama proses dan memori yang digunakan untuk proses enkripsi dan dekripsi baik pada emulator maupun pada ponsel.
3. Menganalisa kualitas stego image dengan menggunakan perhitungan nilai MSE.
4. Menganalisa algoritma kompresi half-byte packing dengan menghitung *space savings*.
5. Menganalisa ketahanan algoritma LSB terhadap kompresi JPEG dan impulsive noise.

1.4 Metodologi Penyelesaian Masalah

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

1. Studi literatur

   Mengumpulkan literatur yang relevan dengan Tugas Akhir yang akan dibuat ini baik itu berupa buku, artikel, dan sumber lain yang berhubungan yaitu mengenai citra digital, teori dasar *steganografi*, LSB, BBS dan *half-byte packing*.

2. Pengumpulan data penunjang tugas akhir

   Pada tahap ini dilakukan pengumpulan data penunjang yang dapat membantu perancangan sistem. Data penunjang tersebut berupa *source code* yang bersifat *open source*, manual pemrograman, contoh image yang akan digunakan untuk pengujian dan analisis, maupun data-data lain yang membantu terselesainya tugas akhir ini.

3. Pemodelan sistem

Pada tahap ini dilakukan perancangan sistem dari studi pustaka dan data-data penunjang, serta analisis terhadap rancangan yang dikembangkan.
Proses enkripsi merupakan proses menyisipkan pesan ke dalam image. Pesan dikompresi terlebih dahulu dengan menggunakan metode half-byte packing. Setelah itu user memasukkan kunci yang digunakan untuk membangkitkan bilangan acak pada metode BBS. Bilangan semu ini digunakan untuk memilih lokasi pixel pada image yang akan dilakukan proses LSB.

Proses dekripsi merupakan proses membangkitkan atau mengambil kembali pesan yang telah disisipkan dalam image. Setelah aplikasi menerima image hasil steganografi, user memasukkan kunci yang sama dengan kunci yang digunakan pada waktu melakukan enkripsi sehingga bilangan acak yang dihasilkan dari pembangkit bilangan BBS akan sama dengan pada saat proses enkripsi. Bilangan acak tersebut digunakan untuk mengambil kembali bit-bit pesan yang disisipkan dalam image dengan mengambil least significant bit (LSB) yang ada pada pixel yang ditunjuk oleh bilangan acak tersebut. Setelah bit-bit tersebut digabungkan barulah dilakukan proses dekompresi pesan menggunakan half-byte packing sehingga dihasilkan pesan semula.

4. Realisasi sistem

Padat tahap ini dilakukan realisasi sistem dari rancangan yang dikembangkan. Sistem direalisasikan dengan menggunakan program aplikasi berbasis java midlet. Realisasi sistem dilakukan secara bertahap pada masing-masing modul dan kemudian digabungkan. Setelah program aplikasi jadi, maka aplikasi tersebut akan diinstall pada ponsel.

5. Evaluasi unjuk kerja sistem

Pada tahap ini dilakukan evaluasi dari realisasi sistem yang dikembangkan. Evaluasi berdasarkan unjuk kerja masing-masing modul serta evaluasi unjuk kerja keseluruhan modul. Evaluasi dilakukan dengan melakukan percobaan pada berbagai kunci, banyaknya pesan, dan ukuran image yang berbeda. Pada tiap-tiap percobaan akan diukur sesuai parameter pada tujuan pembahasan. Pengukuran waktu proses enkripsi dan dekripsi dilakukan pada aplikasi yang telah diinstall pada ponsel dan pada emulator.

1.5 Sistematika Penulisan

Sistematika penulisan pada Tugas Akhir ini terdiri dari lima bab yaitu :

1. Pendahuluan

Bab ini berisi uraian mengenai latar belakang pembuatan Tugas Akhir, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi penelitian dan sistematika penulisan.

2. Dasar Teori

Bab ini menjelaskan seluruh teori yang mendukung cara kerja dari proses *steganografi* pada citra digital dengan LSB, BBS, dan *half-byte packing*.

3. Pemodelan Sistem

Bab ini membahas rancangan sistem secara umum, perangkat keras dan perangkat lunak pendukung yang dibutuhkan untuk mengoperasikan sistem yang dibuat.

4. Pengujian dan Analisis

Bab ini membahas analisis dari proses *steganografi* citra digital yang diperoleh pada tahap perancangan meliputi lama proses enkripsi dan dekripsi pada steganografi (lama proses LSB, BBS dan half-byte packing), memori yang digunakan, kualitas gambar dengan menggunakan MSE, *space savings*, dan ketahanan terhadap kompresi JPEG dan impulsive noise.

5. Kesimpulan dan Saran

Bab ini membahas kesimpulan-kesimpulan serta saran yang dapat ditarik dari keseluruhan Tugas Akhir ini dan kemungkinan pengembangan topik yang bersangkutan.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil penelitian yang telah dilakukan terhadap permasalahan steganografi berbasis MMS menggunakan metode *least significant bit, half-byte packing,* dan *blum-blum shut* ini, dapat diambil beberapa kesimpulan sebagai berikut:

1. Aplikasi steganografi dengan metode steganografi *least significant bit*, kompresi *half-byte packing*, dan pengacakan *blum-blum shut* memerlukan waktu proses yang cepat dan menggunakan memori yang kecil sehingga dapat diimplementasikan pada ponsel.
2. Metode kompresi *half-byte packing* memiliki *space savings* maksimum 42,105 % pada kondisi karakter teks pesan yang terurut memiliki kesamaan setengah byte depan.
3. Metode steganografi *least significant bit* dapat menghasilkan gambar steganografi yang memiliki kualitas baik.
4. Kunci p,q, dan s memiliki pengaruh yang sama terhadap pesan hasil dekripsi sehingga jika terdapat kesalahan pada salah satu kunci dapat menghasilkan pesan dekripsi yang sangat berbeda dengan pesan aslinya.
5. Metode steganografi LSB masih baik digunakan pada aplikasi berbasis MMS meskipun metode ini tidak tahan terhadap adanya gangguan impulsive noise karena pada jaringan MMS sendiri sudah menjaga agar tidak terjadi gangguan akibat adanya noise transmisi.
6. Kompresi gambar menggunakan *half-byte packing* dapat menjadi alternatif untuk mengurangi besar data gambar yang dikirim melalui MMS pada steganografi LSB dengan pesan berupa teks.
7. Penggunaan metode LSB gabungan MER dengan XOR dapat meningkatkan ketahanan dan kualitas gambar hasil steganografi.

5.2 Saran

Hasil evaluasi dan analisis terhadap steganografi berbasis MMS menggunakan metode *least significant bit, half-byte packing,* dan *blum-blum shut* menunjukkan sistem masih dapat dikembangkan. Beberapa saran perkembangan yang bisa dilakukan yaitu:

1. Metode kompresi yang digunakan diganti dengan metode kompresi lain yang lebih cocok digunakan pada pesan teks.
2. Pesan yang dikirimkan tidak hanya berbasis teks saja tetapi dapat berupa file.
3. Media yang digunakan sebagai wadah pada LSB dapat diganti dengan menggunakan format lain seperti audio maupun video.

Daftar pustaka

[1]. Damayanti, Retno, "*Implementasi Sistem Keamanan Data Menggunakan LSB Steganografi dan Algoritma Kriptografi IDEA pada MMS Berbasis J2ME* ", Tugas Akhir IT Telkom,2008.

[2]. Hakim, Muhammad, "*Studi dan Implementasi Steganografi Metode LSB dengan Preprosesing kompresi data dan ekspansi wadah*", http://www.informatika.org/~rinaldi/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-077.pdf, diakses tanggal 5 November 2008.

[3]. Held, Gilbert, "*Data Compression*", John Wiley & Sons, 1991.

[4]. http://en.wikipedia.org/wiki/steganography, diakses tanggal 5 November 2008.

[5]. Konheim, Alan G, "*Computer Security and Cryptography*", John Wiley & Sons, 2007.

[6]. MOTODEV Staff, "*Introduction of MMS in J2ME*", http://www.developer.motorola.com/docstools/articles/MMS_20060901.pdf/, diakses tanggal 5 November 2008.

[7]. Munir, Rinaldi, "*kriptografi*", penerbit informatika, 2006.

[8]. Silahuddin, M dan S, Rosa A, "*Pemrograman J2ME: Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile*", Bandung, Informatika Bandung, 2006.

[9]. Usman, Uke Kurniawan dan Indriani, Heni, "*Performance Analysis of MMS Service on CDMS 200-1X at Telkom Flexi*", IJJSS'04, 20-22 oktober 2004.

[10]. Yuliawan, Fajar, "*Studi dan Perbandingan CSPRNG Blum Blum Shub dan YARROW*", http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah2/Makalah-047.pdf, diakses tanggal 25 November 2008.