IMPLEMENTASI SISTEM KEAMANAN DATA MENGGUNAKAN LSB STEGANOGRAFI DAN ALGORITMA KRIPTOGRAFI IDEA PADA MMS BERBASIS J2ME

Retno Damayanti[1], Iwan Iwut Tritoasmoro[2], Maman Abdurohman[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Teknologi komunikasi bergerak saat ini berkembang dengan sangat cepat, begitu juga perkembangan fitur-fitur layanan yang yang mendukung dalam sistem GSM. Salah satu layanan yang ditawarkan dari GSM adalah MMS (Multimedia Messaging Service) yang merupakan perkembangan dari SMS (Short Message Service) yang memungkinkan untuk melakukan pengiriman data yang berupa image. Tingkat keamanan data yang dikirim melalui MMS masih belum terjamin, karena pihak penyelenggara jaringan atau operator masih dapat mengetahui isi pesan yang dikirim. Pada tugas akhir ini akan dibangun suatu perangkat lunak yang dapat berguna untuk meningkatkan keamanan pesan yang terjadi pada komunikasi melalui MMS. Perangkat lunak dibangun untuk meningkatkan keamanan pesan dengan cara menyisipkan pesan berupa text ke dalam suatu image. Untuk melakukannya diperlukan suatu key yang hanya diketahui oleh pengirim dan penerima saja. Sistem tersebut dikenal dengan steganografi pada image Untuk lebih meningkatkan keamanan pesan yang akan disisipkan pada image maka terlebih dahulu dilakukan kriptografi text. Metode yang digunakan pada sistem steganografi adalah metode Least Significant Bit (LSB), sedangkan pada kriptografi menggunakan algoritma International Data Encryption Algorithm (IDEA).

Perangkat lunak yang dibangun menggunakan platform J2ME yang dapat ditanamkan pada mobile phone. Berdasarkan pengujian perangkat lunak yang dilakukan dapat dilihat bahwa perangkat lunak dapat berjalan dengan baik dan algoritma steganografi LSB dan kriptografi IDEA dapat diimplementasikan untuk enkripsi MMS pada mobile phone.

Kata Kunci : MMS, steganografi, LSB, kriptografi, IDEA, J2ME

Abstract

Present mobile communication technology develop fast, equal with service features development that support in GSM system. One kind of service that offered is MMS (Multimedia Messaging Service), kind of technology that developed from SMS (Short Message Service), so it will be possible to send image data. Safety level data that has been sent through MMS still have not guaranteed yet, because network vendor or operator side still can know message content that sent. This final project will build software that has advantage to increase message security that happened on communication through MMS.

Software built to improve message security with inserted message from text form to be image form. To reach goal need a key that only known by sender and receiver. That system called image steganography. For higher security, the message that will be inserted to image, it must be done with text cryptography. Method that used on steganography system is Least Significant Bit (LSB) method, but for cryptography using International Data Encryption Algorithm (IDEA).

Software that built using J2ME platform can be set on mobile phone. Based on software trial, it can be seen that software done well and steganography algorithm LSB and IDEA cryptography can be implemented to encrypt MMS on mobile phone.

Keywords : MMS, steganography, LSB, cryptography, IDEA, J2ME

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi komunikasi bergerak saat ini berkembang dengan sangat cepat, begitu juga perkembangan fitur-fitur layanan yang yang mendukung dalam sistem GSM. Salah satu layanan yang ditawarkan dari GSM adalah MMS (*Multimedia Messaging Service*) yang merupakan perkembangan dari SMS (*Short Message Service*). MMS merupakan salah satu jenis layanan yang memungkinkan untuk melakukan pengiriman data yang berupa *image*. Tingkat keamanan data yang dikirim melalui MMS masih belum terjamin, karena pihak penyelenggara jaringan atau operator masih dapat mengetahui isi pesan yang dikirim. Sehingga apabila *user* dari *mobile phone* tersebut ingin mengirimkan pesan melalui MMS yang bersifat rahasia, *user* masih belum merasa aman karena timbul kekhawatiran terhadap kerahasian pesan yang akan dikirim.

Untuk meningkatkan keamanan data yang akan dikirim melalui MMS maka dirancang suatu aplikasi yang dapat menunjang kerahasian pesan dari pihak-pihak yang tidak diinginkan untuk mengetahui pesan tersebut. Aplikasi ini dirancang untuk menyisipkan pesan berupa *text* ke dalam suatu *image.* Untuk melakukannya diperlukan suatu *key* yang hanya diketahui oleh pengirim dan penerima saja. Sehingga pihak lain tidak mengetahui bahwa di dalam *image* tersebut ada suatu pesan rahasia, karena yang dilihat hanya sebuah *image* biasa.

Sistem tersebut dikenal dengan steganografi pada *image* Untuk lebih meningkatkan keamanan pesan yang akan disisipkan pada *image* maka terlebih dahulu dilakukan kriptografi *text*. Metode yang digunakan pada sistem steganografi adalah metode *Least Significant Bit* (LSB), sedangkan pada kriptografi menggunakan algoritma *International Data Encryption Algorithm* (IDEA). Kedua sistem tersebut kemudian di implementasikan ke dalam *mobile phone* dengan menggunakan *platform* J2ME.

1.2 Tujuan Penelitian

Tujuan penelitian yang akan dilakukan, antara lain:

1. Mengimplementasikan steganografi pada *image* dengan menggunakan algoritma LSB dimana *text* yang akan disisipkan di-kriptografi dengan menggunakan algoritma IDEA ke dalam program aplikasi berbasis J2ME.
2. Menganalisa performansi sistem MMS steganografi.

1.3 Rumusan Masalah

Penelitian yang dilakukan akan membahas beberapa hal berikut:

1. Memastikan bahwa informasi yang berada dalam suatu sistem hanya dapat diakses oleh pihak yang diberi hak.
2. Merancang aplikasi yang mampu melakukan fungsi-fungsi sebagai berikut:
   - Dari sisi pengirim dapat mengenkripsi *image* asli dan mengekripsi *plaintext* dengan menggunakan *key* dan dapat mengirimkannya pada nomor ponsel yang dituju.
   - Dari sisi penerima dapat mendekripsi *image* stego dan mendekripsi *chipertext* yang diterima, sehingga penerima dapat mendeteksi keutuhan pesan.
3. Analisa performansi sistem, yang meliputi:
   - Waktu yang diperlukan untuk proses enkripsi dan dekripsi
   - Konsumsi memori yang digunakan pada proses enkripsi dan dekripsi

1.4 Batasan Masalah

1. Masukan bagi perangkat lunak yang dirancang adalah *image* dengan format PNG *true color* 24 bit dan *text* dengan kode ASCII (UTF-8).
2. Ukuran image yang digunakan lebih kecil dari 30 kB.
3. Algoritma kriptografi yang digunakan adalah algoritma *private key* dengan kunci simetrik yaitu algoritma IDEA (*International Data Encryption Algorithm*) mode operasi CBC (*Cipher Block Chaining*).
4. Algoritma steganografi yang digunakan adalah algoritma LSB (*Least Significant Bit*).
5. Aplikasi J2ME yang akan dibangun adalah aplikasi *Multimedia Message Service* (MMS).
6. Spesifikasi *mobile phone* yang digunakan untuk perancangan adalah Nokia S60 3*rd Edition, Feature Pack* 2.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam tugas akhir ini adalah :

1. Studi literatur dan kepustakaan dari sumber-sumber penunjang yang berkaitan dengan steganografi, kriptografi, dan *image processing*.
2. Implementasi sistem dengan menggunakan *software* J2ME *Wireless Toolkit 2.5*.
3. Pengumpulan data-data yang diperlukan untuk proses analisa dari karakteristik keluaran sistem yang telah diimplementasikan.
4. Penulisan laporan

1.6 Sistematika Penulisan

Bab I Pendahuluan

Merupakan uraian mengenai latar belakang masalah, tujuan penelitian, perumusan masalah, batasan masalah, metode penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Berisi tentang teori tentang J2ME, *multimedia message service*, citra dan citra digital, steganografi dengan algoritma LSB dan kriptografi dengan menggunakan algoritma IDEA.

Bab III Perancangan dan Implementasi

Bab ini berisi tentang perancangan sistem steganografi dan kriptografi secara keseluruhan baik pada enkripsi dan dekripsi. Pada bab ini juga berisi pemodelan sistem steganografi dan kriptografi menggunakan *software* J2ME.

Bab IV Pengujian dan Analisa

Bab ini berisi hasil analisa dari hasil implementasi berdasarkan parameter-parameter yang telah ditentukan, dan pengujian sistem secara keseluruhan.

Bab V Kesimpulan dan Saran

Berisi kesimpulan dari hasil simulasi, tingkat keberhasilan sistem, serta saran-saran yang dapat digunakan untuk penelitian berikutnya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari hasil perancangan dan implementasi image steganografi ini antara lain:

1. Perangkat lunak ini dapat berjalan baik pada emulator dan mobile phone.
2. Perangkat lunak ini dapat berjalan baik pada mobile phone yang memiliki spesifikasi J2ME dengan WMA 2, CLDC 1.1, MIDP 2.0.
3. Semakin panjang plaintext dan semakin besar ukuran image, maka waktu dan memory yang digunakan untuk memproses semakin besar pula.
4. Adanya perbedaan waktu proses dan memori yang digunakan pada emulator dan pada *mobile phone* disebabkan karena keterbatasan *processor embedded.*

5.2 Saran

Berdasarkan hasil perancangan dan aplikasi yang sudah dibuat, ada beberapa saran agar dapat dilakukan pengembangan, antara lain:

1. Menggunakan format image uncompresion atau format *compresion* lainnya yang sudah didukung oleh *mobile phone*, seperti *bmp, *jpeg.
2. Dilakukan kompresi terlebih dahulu terhadap *text* yang akan disisipkan ke dalam *image*, sehingga pesan yang akan disisipkan menjadi lebih panjang.
3. Menggunakan algoritma steganografi yang lain, seperti LSB dengan menggunakan *pseudo random* untuk mengacak peletakan bit-bit yang akan disisipkan.
4. Menggunakan algoritma kriptografi lainnya (algoritma kunci simetri atau asimetri).