PENERAPAN ALOGRITMA LIPAT PADA STEGANOGRAFI YANG MEMANFAATKAN RMS (*RECORD MANAGEMENT SYSTEM*) DI J2ME

Hero Wintolo, Nurcahyani Dewi Retnowati, Prastyo Fendriyanto
Teknik InformatikaSTTA Yogyakarta
informatika@stta.ac.id

ABSTRACT

The continued development of technology driven by the growing digital media facilities. A digital device in particular should pay attention to the level of security. Ease of sending messages in both text and image becomes very easy. However, one thing is important in the information, which can be performed using encryption steganography.In this thesis, steganography implemented by utilizing the mobile phone messaging facilities. The process of insertion into the text is converted into a binary image first, then take the final bit of the binary to insert text to be inserted. After the insertion process, the message to be sent by using the provider as the link destination address.The process of sending a message that has been tested on several telecommunication provider in Indonesia indicates the existence of different delivery success rate, but the message until it can not be opened unless the application has been made.

Keywords: *Steganography,mobile phone, message, provider, pictures.*

1. PENDAHULUAN

Perkembangan teknologi, telepon seluler sekarang memungkinkan telepon tidak hanya melakukan panggilan telepon maupun melakukan pesan singkat atau *Short Messages Service* (SMS). Hal ini disebabkan bertambahnya fitur-fitur pendukung dalam sebuah telepon seluler yang harus dilakukan oleh produsen telepon seluler. Fitur-fitur *Multimedia Message Service* (MMS), *Instant Messaging* atau *chatting* serta *push-email* yang memungkinkan untuk mengirim atau menerima email selayaknya SMS. Dari berbagai fitur yang di berikan oleh setiap produsen telepon seluler tentunya keamanan atau kerahasian data menjadi sebuah hal pokok yang menjadi pertimbangan sebuah konsumen untuk menggunakannya dalam hal yang sifatnya pribadi atau rahasia. pesan menggunakan SMS dan MMS mempunyai format yang mudah di mengerti oleh pengguna handphone karena tidak ada pengamanan tertentu didalamnya, sehingga sangat berbahaya bila dalam SMS atau MMS tersebut berisi pesan yang bersifat rahasia dan perlu dibuat menjadi lebih aman dengan Steganografi.

Steganografi membutuhkan processor dan memori yang sangat cepat agar dapat menangani proses perhitungan yang rumit, sedangkan telepon seluler pada umumnya tidak memiliki *processor* maupun memori yang cepat layaknya *Personal Computer* (PC) maupun *smartphone*, sehingga proses steganografi menggunakan metode *Least Significant Bit* (LSB). Hasil dari proses disimpan di *Record Management System* (RMS).

RMS pada *Java to Micro Edition* (J2ME) merupakan suatu mekanisme yang digunakan oleh *Mobile Information Device Profile* (MIDP) untuk menyimpan data, pada dasarnya RMS menyimpan kumpulan kumpulan record pada memori *persistance*, memori persistance adalah suatu bentuk penyimpanan non-volatile dalam sebuah aplikasi Midlet, untuk menyimpan data tersebut diperlukan sebuah class RecordStore, class ini digunakan untuk membuka suatu ruang penyimpan (Anonim , 2010, Pengertian J2ME dan Arsitektur, scribd.com).

Sistem merupakan hal yang wajib di ketahui dalam pembuatan sebuah aplikasi, sistem yang bagus berawal dari algoritma yang digunakan. Algoritma juga akan menentukan kecepatan sistem karena algoritma merupakan suatu perintah untuk menyelesaikan suatu masalah. Algoritma lipat adalah algoritma yang dipakai dalam applikasi ini.

2. LANDASAN TEORI

2.1 Citra

Citra atau gambar ditinjau dari sudut pandang matematis merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dwimatra (Munir, 2004, Steganografi dan Watermarking). Citra Digital adalah hasil digitalisasi citra kontinu agar dapat diolah pada komputer, salah satu cara digitalisasi citra kontinu adalah dengan menggunakan metode sampling, yaitu dengan mengambil nilai diskrit koordinat ruang (x,y) dari citra kontinu tersebut. Citra digital tersusun atas sejumlah elemen yang disebut dengan piksel.

Piksel merupakan kependekan dari picture element, piksel adalah representasi suatu titik terkecil dalam citra digital, tiap piksel mempunyai nilai yang menunjukkan intensitas cahaya pada suatu citra digital. Piksel juga dapat digunakan sebagai satuan ukuran gambar, misalnya suatu gambar dengan ukuran 1024 x 800 piksel berarti gambar tersebut tersusun atas 1024 baris dan 800 kolom. Citra digital disimpan dalam media penyimpanan dengan menyimpan piksel penyusunnya, oleh karena itu semakin besar piksel suatu gambar maka akan semakin besar memori yang diperlukan.

Citra Digital juga dibedakan menjadi citra berwarna dan citra hitam putih atau citra grayscale. Citra hitam putih juga disebut dengan citra satu kanal karena warnanya hanya ditentukan oleh satu fungsi intensitas saja. Citra berwarna juga dikenal dengan nama citra spectral karena warna pada citra berwarna disusun oleh 3 komponen warna yaitu warna merah, hijau dan biru, intensitas piksel pada citra berwarna merupakan kombinasi dari tiga intensitas keabuan dari warna merah, hijau dan biru (RGB).

Kedalaman warna dalam citra digital dinyatakan dengan bit, 1 bit citra berarti 21 = 2 warna, biasa direpresentasikan dengan warna hitam dan putih, citra 8 bit atau true color memiliki 256 warna didalamnya. Dalam kaitannya dengan steganografi, makin besar bit

citra maka akan makin besar pula data yang bisa disisipkan dalam citra tersebut.

2.2 Steganografi

Steganografi (steganography) berasal dari bahasa Yunani steganos, yang artinya 'tersembunyi/terselubung', dan graphein, 'menulis' sehingga kurang lebih artinya "menulis (tulisan) terselubung". Steganografi merupakan seni untuk menyembunyikan pesan di dalam pesan lainnya sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Dalam Steganografi dibutuhkan wadah penampung dan data rahasia yang akan ditampilkan, steganografi digital menggunakan media digital sebagai wadah penampung, misalnya audio, teks dan video.

Beberapa metode yang digunakan dalam steganografi digital yaitu Least Significant Bit Insertion (LSB), Algorithms and Transformation, Redundant Pattern Encoding, Spread Spectrum method dan End Of File. Metode-metode tersebut digunakan dalam steganografi dengan media dan fungsi yang berbeda-beda untuk memaksimalkan pengamanan suatu data (informasi) agar menjadi rahasia (Munir, 2004, Steganografi dan Watermarking).

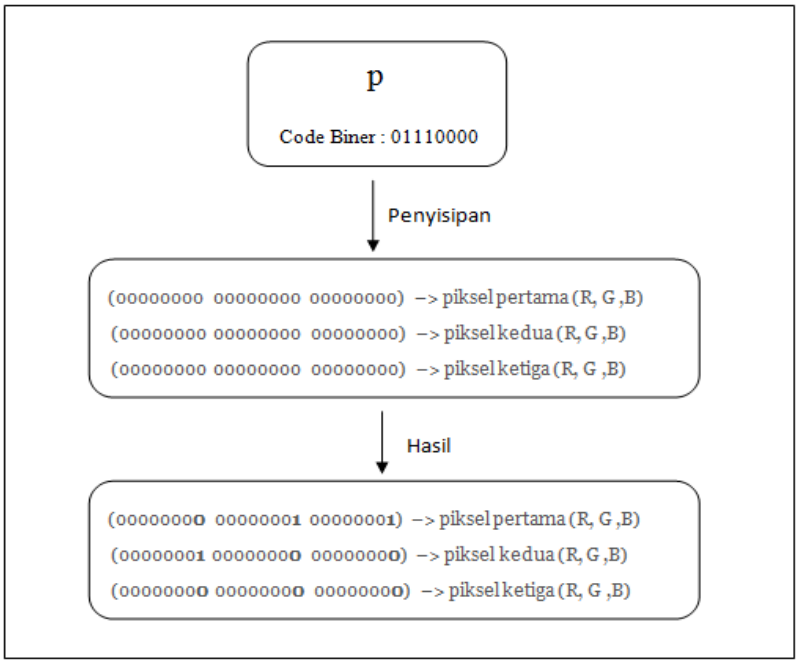
2.3 *Least Significant Bit* (LSB)

Bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri (Tjong, Andreas, Steganografi : LSB).

Pada citra digital terdapat beberapa jenis penamaan berdasarkan pewarnaan dari citra digital tersebut, seperti grayscale atau citra yang memiliki warna hitam dan putih maupun RGB dan CYMK. Pada citra RGB bitmap 24 bit berarti dalam tiap piksel citra tersebut tersusun atas 8 bit Red, 8 bit Green dan 8 bit Blue dimana masing-masing elemen red, green dan blue mempunyai nilai dari 0 sampai 255 atau dilambangkan dengan 00000000 sampai 11111111 dalam bilangan biner.

Prinsip dari metode LSB adalah dengan menyisipkan bit yang merupakan representasi dari informasi yang kemudian disembunyikan dalam bit yang paling kurang berarti atau pada bit terendah citra yang biasanya berada pada 4 bit terakhir, karena disisipkan pada bit terendah maka perbedaan citra sebelum dan sesudah disisipi bit tidak terlihat secara jelas atau mencolok.

Tahap pertama dalam metode LSB adalah mengubah data teks menjadi bilangan biner. Dimisalkan untuk menyisipkan huruf "p" ke dalam sebuah gambar grayscale, jika direpresentasikan ke dalam bilangan biner, maka huruf "p" menjadi seperti yang ditampilkan dalam gambar 1.Contoh, akan disisipkan huruf P kedalam data berwarna hitam.



Gambar 1 Penyisipan huruf "p" ke dalam gambar

2.4 *Record Management System* (RMS)

RMS pada J2ME RMS(Record Management System) merupakan suatu mekanisme yang digunakan oleh MIDP untuk menyimpan data, pada dasarnya RMS menyimpan kumpulan kumpulan record pada memori persistance, memori persistance adalah suatu bentuk penyimpanan non-volatile dalam sebuah aplikasi Midlet, untuk menyimpan data tersebut diperlukan sebuah class RecordStore, class ini digunakan untuk membuka suatu ruang penyimpan (altanovela, simple-rms-pada-j2me, altanovela.wordpres.com).

2.5 AlgoritmaLipat(Kelipatan Empat)

Algoritma lipat (kelipatan empat) adalah algoritma yang digunakan untuk menyisipkan pesan kedalam data (gambar) kedalam bit yang paling akhir dengan menggunakan rumus 'increment-_PANJANG_PESAN % 4 != 0'.

Dengan perhitungan seperti itu maka akan didapat, pesan yang akan disisipkan tidak akan dimasukan kedalam urutan ke-4. Jadi pesan dalam bentuk biner akan disisipkan kedalam pixel dengan format RGB dengan mengabaikan A (Alpha).

Gambar akan diubah menjadi bytePixel, yang bertujuan untuk mendapatkan array bit. Array bit ini merupakan suatu tempat untuk memasukan pesan yang akan disisipkan. Oleh karena itu sebelum masuk ke proses akhir penyisipan yang menggunakan nilai dari array bit dilakukan terlebih dahulu menghitung jumlah pesan. Ini dilakukan agar dapat menggambil jumlah array bit yang akan digunakan. Setelah mendapat array bit yang dibutuhkan kemudian melakukan penyisipan dengan merubah bit teks per-karakter, dimasukan dengan rumus 'increment-_PANJANG_PESAN % 4 != 0'. increment-_PANJANG_PESAN adalah bertambahnya nilai mulai dari 0 sampai panjang pesan

dengan perulangan. Dalam pertambahan tersebut pesan akan dimasukan jika increment-_PANJANG_PESAN tidak menghasilkan nilai 0 jadi setiap biner data akan dimasukan dengan tidak kelipatan empat.

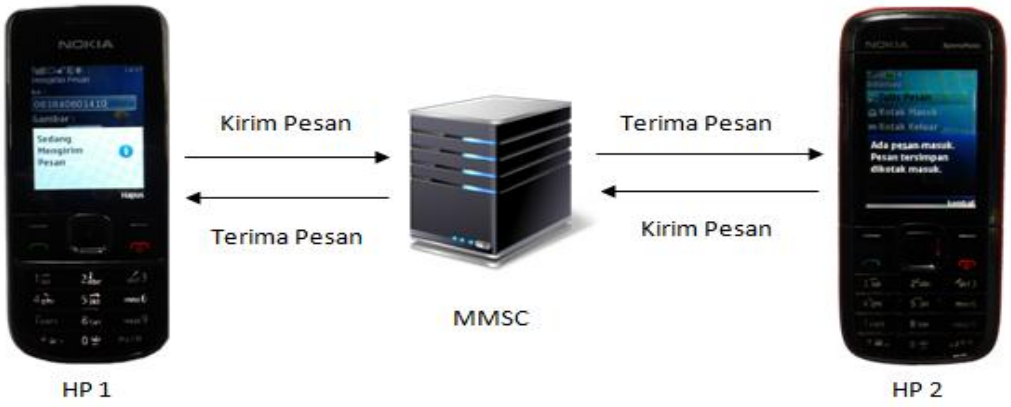
Tabel 1 Penyisipan Code Biner Mengunakan Algoritma Lipat

Sebelum Disisipkan	Code Biner P	Hasil Penyisipan
00000000	x	00000000
11111110	0	11111110
11111110	1	1111111
11111110	0	11111110
00000000	x	00000000
11111110	1	1111111
11111110	0	11111110
11111110	0	11111110
00000000	x	00000000
11111110	0	11111110
11111110	0	11111110

3. PENGUJIAN DAN ANALISIS

3.1 Penjelasan Aplikasi

StegaMMS merupakan nama dari aplikasi yang telah dibuat. StegaMMS merupakan suatu aplikasi yang membantu user untuk mengirimkan pesan yang sifatnya pribadi atau rahasia. StegaMMS dibangun dengan algoritma lipat (kelipatan empat) yang khususnya terdapat dalam proses penyisipan pesan teks kedalam gambar yang memungkinkan kelebihan keamanan teks yang telah disisipkan dan menggunakan MMS untuk membantu pengiriman pesan gambar. Proses dari aplikasi StegaMMS dapat dilihat pada Gambar 2.



Gambar 2 Proses pengiriman pesan dari HP 1 dan penerimaan pesan dari HP 2

MMS merupakan salah satu aplikasi yang dikembangkan pada *platform* teknologi 2.5G. Tidak seperti SMS yang dikirimkan menggunakan kanal kontrol (control Chanel), MMS menggunakan GPRS dalam pengirimannya. MMS dikirimkan secara "*store and forward*" yang artinya MMS mula-mula disimpan dalam *Message Centre* (MMSC) baru kemudian dinotifikasikan (diberitahukan) kepada penerima. Pada MMS,

pesan MMS pada *server* atau MMSC akan disimpan dalam batas waktu tertentu. Dalam StegaMMS secara otomatis aplikasi akan mengunduh pesan yang telah dikirim, kemudian akan disimpan pada aplikasi menggunakan RMS.

Sebelum pengiriman pesan melalui MMS pada aplikasi StegaMMS, HP 1 akan dihadapkan pada penulisan pesan terlebih dahulu sebelum HP 1 mengirimkan pesan ke HP 2. Berikut merupakan detail alur pengiriman dan penerimaan pesan pada gambar 3a sampai gambar 3c yang mengacu pada gambar 2 dengan menguraikan langkah-langkah yang harus dilakukan oleh HP 1 maupun HP 2 dalam mengirimkan pesan maupun memproses pesan yang diterima.

Gambar 3a,b,c. Proses pengiriman pesan

Gambar 4a,b,c. Proses pengirman pesan

HP 1 akan dihadapkan pada menu utama sebelum mengirim pesan, yang dapat dilihat pada gambar 4.a. HP 1 memilih menu tulis pesan untuk membuat pesan baru. Pada gambar 4.b HP 1 memilih gambar untuk pesan yang akan dikirim. Dalam proses pemilihan gambar, di *handphone* yang khusunya mendukung j2me *user* akan diminta untuk ijin akses aplikasi pada gambar 4.c sebelum gambar dimasukkan.

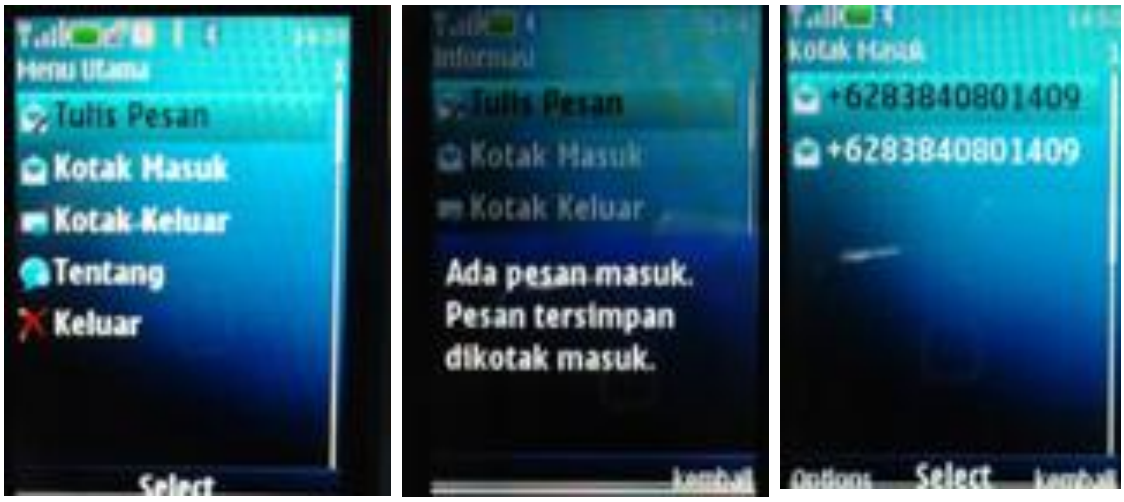
Setelah gambar berhasil dimasukan, selajutnya pada gambar 4.1.d HP 1 akan menuliskan pesan teks yang akan dikirimkan

ke HP 2. Untuk masukan teks, aplikasi telah membatasi sebanyak 255 karakter.

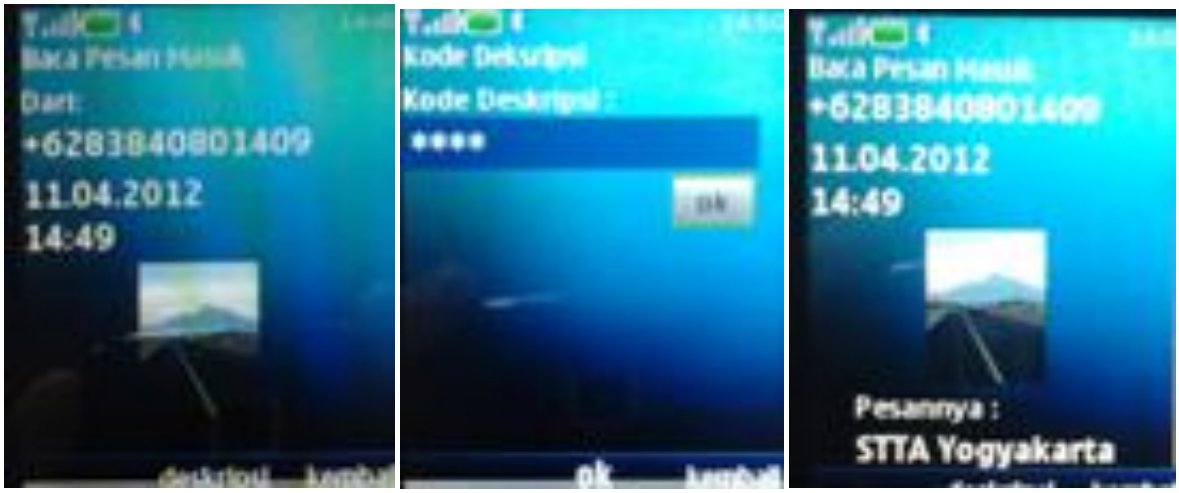
Teks dan gambar sudah terisi, HP 1 akan menekan tombol enkripsi dan setelah pesan disisipkan kedalam gambar maka pesan yang akan dikirimkan kepada HP 2 hanya berupa gambar. Pada gambar 4.1.e setelah gambar yang akan dikirim berhasil disisipkan pesan selanjutnya HP 1 memasukan nomor telephone HP 2.

Pada gambar 4.1.f terjadi proses pengiriman setelah HP 1 menekan tombol kirim, proses ini akan berakhir setelah pesan benar-benar terkirim. Proses pesan ini dapat diidentifikasi manual dengan melihat tanda huruf E (*Edge*) yang berarti menggunakan jalur GPRS dalam pengiriman pesan.

Pesan telah terkirim ke nomor tujuan namun sebelum terkirim kenomor tujuan pesan akan tersimpan di MMSC terlebih dahulu. Adapun detail alur sebelum pesan itu masuk kedalam HP 2. Pada gambar 4.1.g sampai 4.1.l akan menjelaskan alur pesan yang diterima.



Gambar 5a,b,c. Proses penerimaan pesan



Gambar 6a,b,c. Proses penerimaan pesan

Gambar 5a HP 2 mendapatkan pesan dari HP 1, hal ini dapat terlihat dari HP 2 mengunduh terlebih dahulu pesan yang dikirim, pengunduhan pesan ini dapat dilihat dari tanda E (Edge) dibagian atas handphone. Setelah download selesai pesan akan langsung disimpan di RMS. Gambar 5b merupakan peringatan adanya pesan baru dan memberitahu letak pesan yang telah diterima. Pesan yang telah diterima tersimpan di RMS dan ditampilkan di menu kotak masuk pada gambar 5c.

Untuk membuka pesan tekan tombol pilih maka pesan akan terbuka. Pada gambar 6a. merupakan pesan yang diterima tetapi ketika dibuka hanya terdapat gambar dan nomor pengirim saja. Untuk membuka pesan tersebut tekan tombol deskripsi dan akan seperti gambar 6b. Untuk bisa membaca pesan masukan kode yang telah disimpan ketika program aplikasi ini pertama diinstal. Jika kode yang anda masukan benar maka akan seperti gambar 6c. sehingga akan muncul pesan yang disembunyikan.

3.2 Uji Fungsi

Pengujian terhadap keamanan pesan yang disisipkan kedalam pesan berupa gambar dilakukan dengan menggunakan software Hexa Editor WinHex. Aplikasi StegaMMS itu sendiri sebetulnya dalam prosesnya tidak menyimpan gambar secara utuh dalam format jpg, maupun png namun aplikasi ini menyimpan gambar dalam bentuk byte sehingga tanpa menggunakan aplikasi ini gambar tidak dapat dibuka.

Pengujian ini dilakukan untuk menguatkan algoritma lipat dalam hal keamanannya. Dengan mengunakan algoritma ini bahwa pesan yang telah disisipkan tidak akan mudah untuk dibaca dengan software apapun kecuali dengan algoritma lipat yang mendeskripsikan terhadap pesan yang akan dibaca. Berikut pengujian file gambar dengan menggunakan winhex. Nama file : hitamsaja.png, dan pesan disembunyikan : STTA Yogyakarta

Dalam winhex terdapat 3 bagian yang terpenting untuk melihat detail gambar, yaitu offset, hexadecimal, dan block. Offset digunakan untuk mengindentifikasi baris per hexadecimal. Kemudian hexadecimal adalah nilai dari hexa yang ada didalam gambar, dan yang ketiga adalah block. Block ini mempunyai fungsi menerjemahkan nilai hexadecimal kedalam teks.

Dari pengujian file yang telah dimasukan teks dengan menggunakan algoritma lipat seperti gambar 4.5, bahwa pesan secara langsung tidak dapat dibaca dengan winhex. Dilihat dibagian block tidak ada kata yang dapat diterjemahkan secara langsung.

4. KESIMPULAN

1. Aplikasi yang dirancang dengan metode steganografi, dapat digunakan pada handphone yang licensi-nya sesuai dengan licensi dari open source.
2. Steganografi menggunakan metode LSB dengan memanfaatkan algoritma lipat menghasilkan keberhasilan yang baik karena pesan teks yang disisipkan tidak terbaca di winhex.
3. Pengiriman pesan dengan StegaMMS mempunyai tingkat keberhasilan yang

baik dengan menggunakan provider axis, xl, dan 3 meskipun memberikan delay dalam pengiriman pesan selanjutnya.

4. Algoritma yang digunakan dapat diterapkan dalam aplikasi

DAFTAR PUSTAKA

Batara, Simon, 2008, *Studi Steganografi Pada File MP3*, Makalah, Teknik Informatika ITB, Bandung.

Daryamto, Budi , dkk, 2007, *Pemrograman Berorientasi Objek dengan Java 2 Platform Micro Edition (J2ME)*, Java Competency Center – ITB, Bandung.

Keogh, James, 2003, *The Complete Reference J2ME*, McGraw-Hill, California.

Mansur, Ahmad, 2009, *Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit*, Tugas Akhir, Teknik Informatika ITS, Surabaya.

Munir, Rinaldi, 2004, *Diktat kuliah Kriptografi : Steganografi dan Watermarking*, Departemen Teknik Informatika Institut Teknologi Bandung, Bandung.

Munir, Rinaldi, 2004, *Pengolahan Citra Digital*, Informatika, Bandung.

Shiralli, Mohammad, 2009, *An Improved Method for Steganography on Mobile Phone*, Paper, Allameh Helli Pre-University, Tehran, Iran.

Altanovela , 2009, *Simple RMS*, *altanovela.wordpress.com*/, pada tanggal 23 april 2012

Tjong, Andreas, 2008 Steganografi : LSB (Least Significant Bit), *http://andreastjong.wordpress.com*/, pada tanggal 14 Mei 2011

Irawan, R, 2009, Multimedia Messaging Service, *http://digilib.ittelkom.ac.id*/, pada tanggal 19 Mei 2011