APLIKASI KEAMANAN DATA MENGGUNAKAN METODE MMB DAN LSB

Fajar Dewandaru[1], Cahya Rahmad[2]

[1] Teknik Informatika, Teknologi Informasi,Politeknik Negeri Malang
[1] fajar.dewandaru@gmail.com, [2] cahya.rahmad@yahoo.com

Abstrak

Teknologi informasi dapat membantu pekerjaan manusia khususnya yang berhubungan dengan pemrosesan ataupun pendistribusian informasi. Namun, seiring dengan berkembangnya hal tersebut berkembang pula pelangaran atau penyalahgunaan dalam keamanan pesan yang dikirim seperti dengan cara merusak, menyadap, merubah pesan tersebut untuk kepentingan pribadi. Untuk itu diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi menggunakan ilmu untuk menyembunyikan atau mengamankan suatu pesan atau informasi ke dalam pesan lain yaitu dengan teknik steganografi serta proses penyandian suatu informasi atau data rahasia yang berbentuk teks menjadi bentuk lain yang tidak dapat dipahami yaitu teknik kriptografi. Dengan penggabungan dari kedua metode ini maka pesan atau informasi yang disembunyikan akan sulit untuk dipecahkan atau dibobol, karena memiliki dua tingkat keamanan.

Kata kunci: steganografi, kriptografi, MMB, LSB.

1. Pendahuluan

Pada era modern saat ini, teknologi informasi dan komunikasi merupakan suatu kebutuhan manusia yang tidak dapat terpisahkan lagi dalam melakukan setiap kegiatan di bidang pendidikan maupun dunia kerja. Teknologi informasi dapat membantu pekerjaan manusia khususnya yang berhubungan dengan pemrosesan ataupun pendistribusian informasi. Seiring dengan berkembangnya teknologi informasi akan mempermudah manusia dalam berkirim pesan maupun menerima pesan. Pesan yang disampaikan ada kalanya berupa pesan yang bersifat rahasia sehingga tidak semua pihak dapat melihat pesan tersebut. Namun, seiring dengan berkembangnya hal tersebut berkembang pula pelangaran atau penyalahgunaan dalam keamanan pesan yang dikirim seperti dengan cara merusak, menyadap, merubah pesan tersebut untuk kepentingan pribadi. Kegiatan tersebut membuat informasi atau pesan yang bersifat rahasia dapat dilihat oleh orang yang tidak bertanggung jawab. Oleh karena itu, masalah keamanan informasi menjadi hal yang sangat penting dalam suatu sistem informasi untuk keamanan bersama maupun keamanan pribadi. Untuk itu diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi.

Menurut Cahyadi (2012), steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Metode steganografi yang sederhana dan mudah untuk diimplementasikan adalah metode LSB (*Least Significant Bit*). LSB adalah metode yang menggunakan algoritma sederhana yang menukar bit paling kecil ke dalam beberapa *byte* media penyembunyian secara berurutan. Kelemahan dari metode LSB adalah pesan rahasia yang telah disisipkan dapat dengan mudah diambil kembali dengan menggunakan metode LSB jika diketahui oleh orang lain. Untuk menutupi kekurangan dari metode tersebut dilakukan proses penyandian suatu informasi atau data rahasia yang berbentuk teks menjadi bentuk lain yang tidak dapat dipahami sebelum disisipkan menggunakan metode LSB, teknik ini disebut teknik kriptografi.

Kriptografi merupakan suatu ilmu yang mempelajari tentang teknik atau cara merahasiakan dan mengembalikan ke bentuk semula suatu pesan dengan cara unik yang berhubungan dengan aspek keamanan informasi. Metode kriptografi yang dapat digunakan untuk mengamankan data sangat beragam, salah satunya adalah metode MMB (*Modular Multiplication-based Block Cipher*). MMB adalah algoritma *block cipher* pengembangan dari metode kriptografi IDEA yang juga berbasis *block cipher* yang sebelumnya sering digunakan dalam mengenkripsi dan mendekripsi suatu pesan atau informasi.

Untuk meningkatkan kemanan pesan dan informasi yang dirahasiakan serta pengimplementasian metode tersebut dalam aplikasi maka penulis membuat "Aplikasi Keamanan Data Menggunakan Teknik Kriptografi dan Steganografi Dengan Metode MMB dan LSB", dengan cara pesan yang akan disisipkan menggunakan metode LSB terlebih dahulu dienkripsi menggunakan metode MMB.

2. Steganografi

Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi rahasia kedalam pesan lain. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. Menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan adalah tujuan utama dari steganografi (Cahyadi, 2010). Dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui adanya pesan rahasia. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau media digital lainnya dan terlihat seperti pesan biasa.

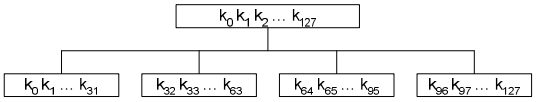
3. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek-aspek pada keamanan informasi misalnya kerahasiaan, integritas data, otentikasi pengirim / penerima data, dan otentikasi data. Teknik ini digunakan untuk mengubah data ke dalam kode-kode tertentu, dengan tujuan informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman tidak dapat dibaca oleh siapa pun kecuali orang-orang yang berhak.

Terdapat dua proses penting di dalam kriptografi yang berperan dalam merahasiakan suatu informasi yakni enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah transformasi data (*plaintext*) ke dalam bentuk yang hampir tidak dapat dibaca (*ciphertext*) tanpa pengetahuan yang cukup. Sedangkan dekripsi adalah kebalikan dari enkripsi, yakni transformasi dari data yang telah dienkripsi (*ciphertext*) kembali ke bentuk semula (*plaintext*). Proses enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi yang rahasia, yang sering disebut kunci (*key*) (Latief, 2010:1).

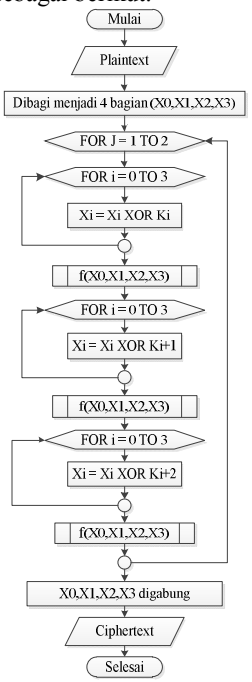
4. Metode MMB

Kriptografi metode MMB menggunakan *plaintext* 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik. Substitusi ini ditentukan oleh sebuah operasi perkalian modulo $2^{32} - 1$ dengan faktor konstan, yang memiliki tingkat sekuritas lebih tinggi. MMB menggunakan 32 bit *sub block text* (x0, x1, x2, x3) dan 32 bit *sub block* kunci (k0, k1, k2, k3). Hal ini membuat algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 bit. Sebuah fungsi non linier, f, diterapkan enam kali bersama dengan fungsi XOR (Latief, 2010: 4). Metode MMB menggunakan kunci sepanjang 128 bit. Proses pembentukan kunci pada metode MMB ini sangat sederhana. Kunci yang di-*input* hanya dibagi menjadi 4 buah *sub block* kunci dengan panjang masing-masing 32 bit. Proses pembentukan kunci pada metode MMB ini dapat dilihat pada bagan berikut ini:



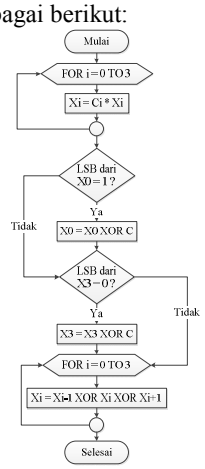
Gambar 2.5 Proses Pembentukan Kunci pada Metode MMB (Sumber: Latief, 2010: 4)

Metode MMB menggunakan kunci dan *plaintext* dengan panjang 16 karakter atau 128 bit. Proses enkripsi metode MMB digambarkan dengan diagram alur sebagai berikut:



Gambar 3.5 Proses Enkripsi MMB (Sumber: Latief, 2010: 4)

Fungsi f yang digunakan dijelaskan pada diagram alur sebagai berikut:



Gambar 3.6 Fungsi f Enkripsi (Sumber: Latief, 2010: 5)

Operasi perkalian yang digunakan merupakan operasi modulo $2^{32} - 1$. Konstanta yang digunakan dirincikan sebagai berikut:

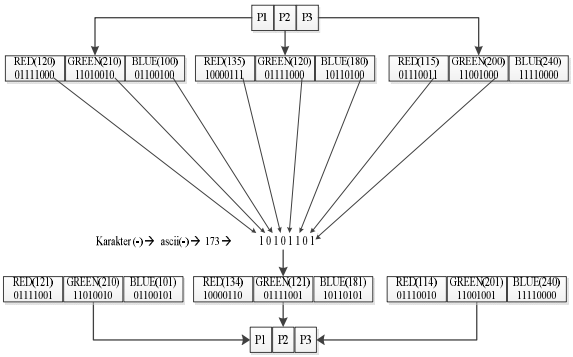
- $C = (2AAAAAAA)_{16}$
- $C_0 = (025F1CDB)_{16}$
- $C_1 = 2 * C_0$

- $C_2 = 2^3 * C_0$
- $C_3 = 2^7 * C_0$

5. Metode LSB

Metode LSB (*Least Significant Bit*) bekerja dengan cara mengganti bit terakhir dari masing-masing piksel dengan pesan yang akan disisipkan. LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekurangannya adalah pesan/ data yang akan disisipkan terbatas, sesuai dengan ukuran citra (Krisnawati, 2008: 40). Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya.

Sebagai contoh, Pada proses *encode* atau penyisipan untuk menyisipkan 1 karakter dibutuhkan 3 *pixel* gambar, contohnya dapat digambarkan sebagai berikut:

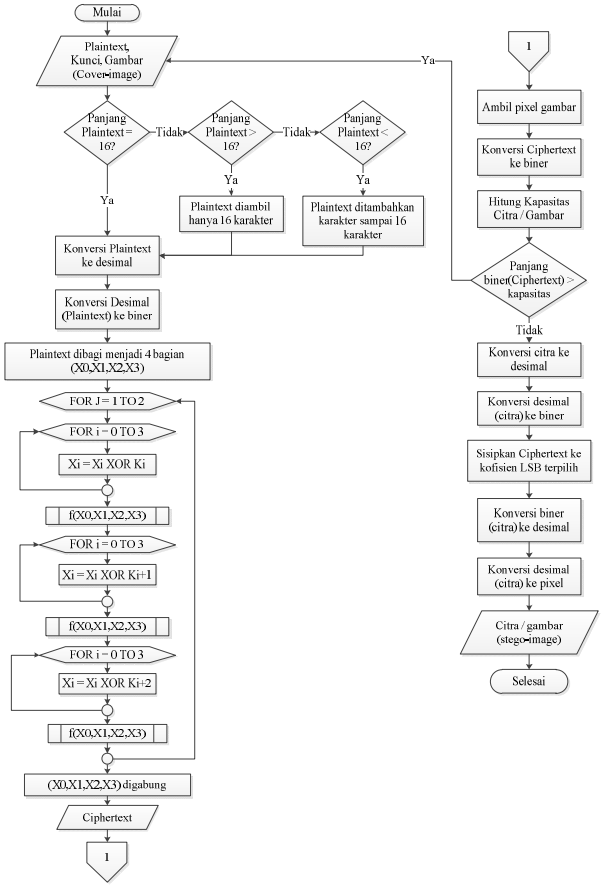


Gambar 4.1 *Encode* Metode LSB (Sumber: Implementasi)

6. Kombinasi Metode MMB dan LSB

Proses enkripsi dan *encode* membutuhkan pesan (*plaintext*) dan gambar yang akan disisipi (*cover-image*) yang selanjutnya *plaintext* digunakan dalam proses algoritma MMB dan menghasilkan pesan yang telah dienkripsi (*ciphertext*). Selanjutnya *ciphertext* disisipkan ke dalam gambar (*cover-image*) menggunakan algoritma LSB dan hasilnya adalah gambar yang telah disisipi (*stego-image*). Proses enkripsi dan *encode* tersebut dapat lebih dijelaskan secara rinci dengan diagram alur di dalam Gambar 3.10.

Dalam proses tersebut dibutuhkan masukan pesan (*plaintext*), kunci yang telah menjadi 4 bagian sama besar, dan gambar (*cover-image*) selanjutnya dilakukan penghitungan panjang dari *plaintext*, apabila panjang *plaintext* lebih besar dari 16 maka hanya diambil 16 karakter sebagai *plaintext*, apabila *plaintext* lebih kecil dari 16 maka ditambahkan karakter spasi sampai jumlah *plaintext* sama dengan 16, jika *plaintext* sama dengan 16 proses selanjutnya yaitu mengkonversi *plaintext* ke bentuk desimal, lalu konversi desimal tersebut ke biner, biner *plaintext* tersebut selanjutnya dibagi menjadi 4 bagian sama besar, selanjutnya dilakukan proses algoritma metode MMB yaitu operasi XOR antara *plaintext* dan kunci, fungsi f, mengikuti alur tersebut hingga menggabungkan kembali pesan dan menghasilkan pesan yang telah dienkripsi (*ciphertext*), selanjutnya mengambil *pixel* gambar, mengkonversi *ciphertext* ke bentuk biner, dan menghitung kapasitas tampung gambar (*cover-image*), jika memenuhi kebutuhan maka dilanjutkan dengan mengkonversi *pixel* gambar ke desimal dan konversi kembali ke bentuk biner, lalu menyisipkan biner *ciphertext* ke bit terakhir dari biner *pixel*, konversi biner *pixel* ke desimal dan konversi kembali menjadi *pixel* gambar, setelah itu akan menghasilkan keluaran gambar yang telah disisipi (*stego-image*).

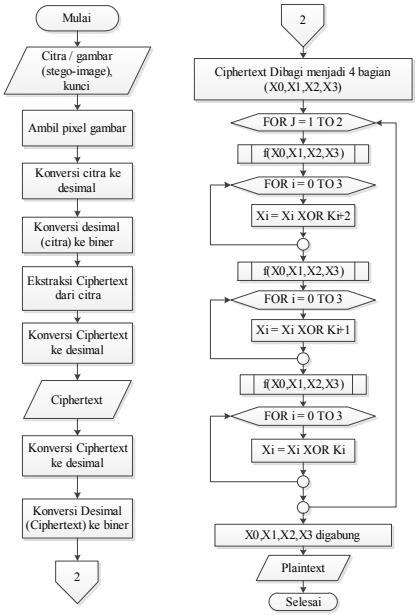


Gambar 3.10 Proses Enkripsi Kombinasi dari Metode MMB dan LSB (Sumber: Perancangan)

Setelah proses enkripsi dan *encode* dilakukan, untuk mengambil kembali pesan yang disembunyikan dilakukan proses dekripsi dan ekstraksi/ *decode* dengan alur di dalam Gambar 3.11.

Dari alur tersebut dibutuhkan masukan gambar (*stego-image*) dan kunci, mengambil *pixel* gambar (*stego-image*), konversi *pixel* ke desimal, konversi kembali ke bentuk biner, selanjutnya mengekstraksi *ciphertext* dari gambar dengan algoritma LSB dengan mengambil bit terakhir dari biner gambar (*stego-image*), konversi *ciphertext* ke bentuk desimal, konversi kembali ke bentuk biner, biner *ciphertext* dibagi menjadi 4 bagian yang sama besar, kemudian melakukan dekripsi menggunakan

algoritma MMB dengan melakukan fungsi f dekripsi, operasi XOR antara *ciphertext* dan kunci, lalu melakukan proses mengikuti alur tersebut hingga mengabungkan kembali pesan, konversi pesan tersebut ke desimal, dan menghasilkan *plaintext*.



Gambar 3.11 Proses Deskripsi Kombinasi dari Metode MMB dan LSB (Sumber: Perancangan)

7. Hasil Pengujian

Dari uji coba yang telah dilakukan terhadap 3 *file* teks dengan besar ukuran *file* 16 *bytes*, dalam melakukan proses enkripsi hasil yang didapatkan adalah perubahan pesan ke bentuk yang tidak dapat diartikan atau *ciphertext* sebagai berikut:

Tabel 5.3 Enkripsi *Plaintext*

No	Nama Plaintext	Plaintext	Kunci	Ciphertext
1	kampus.txt	TI POLTEK MALANG	Fajar Dewandaru!	-A•²£¶ËCè;'Ô6
2	nama.txt	Fajar Dewandarua	prodi informatik	tÓ]ç^{a}÷CO)DôO
3	ujiPlain.txt	TI Polinema bisa	angkatan ti 2011	õÒ7õØ…oufl GºÂÕ¨

Dari data tersebut, *ciphertext* yang dihasilkan disisipkan ke dalam gambar yang telah dipilih dengan rincian sebagai berikut:

Tabel 5.4 Hasil Enkripsi dan Penyisipan atau *Encode*

No	Sebelum Proses Enkripsi				Setelah Proses Enkripsi	
	Cover-image	Ukuran *Cover*	Dimensi	*Plaintext*	Ukuran *Stego*	Waktu Proses
1	airTerjun1.bmp	1351.254 *Bytes*	750 x 600	kampus.txt	1351.254 *Bytes*	0 : 0 : 23 : 307
				nama.txt	1351.254 *Bytes*	0 : 0 : 23 : 370
				ujiPlain.txt	1351.254 *Bytes*	0 : 0 : 23 : 137
2	boy2.bmp	810.294 *Bytes*	640 x 422	kampus.txt	810.294 *Bytes*	0 : 0 : 21 : 255
				nama.txt	810.294 *Bytes*	0 : 0 : 21 : 590
				ujiPlain.txt	810.294 *Bytes*	0 : 0 : 21 : 459
3	flying3.bmp	439.542 *Bytes*	448 x 327	kampus.txt	439.542 *Bytes*	0 : 0 : 20 : 272
				nama.txt	439.542 *Bytes*	0 : 0 : 20 : 323
				ujiPlain.txt	439.542 *Bytes*	0 : 0 : 20 : 176
4	pantai1.bmp	1200.054 *Bytes*	800 x 500	kampus.txt	1200.054 *Bytes*	0 : 0 : 22 : 727
				nama.txt	1200.054 *Bytes*	0 : 0 : 22 : 901
				ujiPlain.txt	1200.054 *Bytes*	0 : 0 : 22 : 937
5	merpati2.bmp	833.334 *Bytes*	640 x 434	kampus.txt	833.334 *Bytes*	0 : 0 : 21 : 569
				nama.txt	833.334 *Bytes*	0 : 0 : 21 : 614
				ujiPlain.txt	833.334 *Bytes*	0 : 0 : 21 : 599
6	bangun3.bmp	451.638 *Bytes*	448 x 336	kampus.txt	451.638 *Bytes*	0 : 0 : 20 : 215
				nama.txt	451.638 *Bytes*	0 : 0 : 20 : 409
				ujiPlain.txt	451.638 *Bytes*	0 : 0 : 20 : 171

Perbandingan gambar sebelum proses enkripsi dan penyisipan (*cover-image*) dengan gambar setelah proses enkripsi dan penyisipan (*stego-image*) sebagai berikut:

Tabel 5.7 Perbandingan *Cover-image* dan *Steganoimage*

No	Nama *Cover*	Gambar	Nama *Stego*	Gambar
1	airTerjun1.bmp		kampus1.bmp	
2	boy2.bmp		kampus2.bmp	
3	flying3.bmp		kampus3.bmp	
4	pantai1.bmp		kampus4.bmp	
5	merpati2.bmp		kampus5.bmp	
6	bangun3.bmp		kampus6.bmp	

Setelah melakukan proses enkripsi, selanjutnya pada proses dekripsi dihasilkan data sebagai berikut:

Tabel 5.5 Dekripsi *Ciphertext*

No	*Ciphertext*	Kunci	*Plaintext*
1	-A•²£¶ËCè;'Ô6	Fajar Dewandaru!	TI POLTEK MALANG
2	tÓ]ç^{a}÷CO)DôO	prodi informatik	Fajar Dewandarua
3	õÒ7õØ…oufl GºÂÕ¨	angkatan ti 2011	TI Polinema bisa

Hasil dekripsi dari *ciphertext* menghasilkan teks awal yang dimasukkan (*plaintext*) pada saat proses enkripsi. Dari data tersebut berikut data lengkap saat melakukan proses dekripsi di dalam Tabel 5.6.

Tabel 5.6 Hasil Proses Dekripsi dan Ekstraksi atau *Decode*

No	*Stego-image*	Ukuran *Stego*	Dimensi	File *Plaintext*	Ukuran *Plaintext*	Waktu Proses
1	kampus1.bmp	1351.254 *Bytes*	750 x 600	kampus1.txt	18 *Bytes*	0 : 0 : 21 : 249
2	nama1.bmp	1351.254 *Bytes*	750 x 600	nama1.txt	18 *Bytes*	0 : 0 : 21 : 571
3	ujiPlain1.bmp	1351.254 *Bytes*	750 x 600	ujiPlain1.txt	18 *Bytes*	0 : 0 : 21 : 239
4	kampus2.bmp	810.294 *Bytes*	640 x 422	kampus2.txt	18 *Bytes*	0 : 0 : 20 : 405
5	nama2.bmp	810.294 *Bytes*	640 x 422	nama2.txt	18 *Bytes*	0 : 0 : 20 : 647
6	ujiPlain2.bmp	810.294 *Bytes*	640 x 422	ujiPlain2.txt	18 *Bytes*	0 : 0 : 20 : 393
7	kampus3.bmp	439.542 *Bytes*	448 x 327	kampus3.txt	18 *Bytes*	0 : 0 : 19 : 908
8	nama3.bmp	439.542 *Bytes*	448 x 327	nama3.txt	18 *Bytes*	0 : 0 : 20 : 078
9	ujiPlain3.bmp	439.542 *Bytes*	448 x 327	ujiPlain3.txt	18 *Bytes*	0 : 0 : 19 : 676
10	kampus4.bmp	1200.054 *Bytes*	800 x 500	kampus4.txt	18 *Bytes*	0 : 0 : 21 : 070
11	nama4.bmp	1200.054 *Bytes*	800 x 500	nama4.txt	18 *Bytes*	0 : 0 : 21 : 337
12	ujiPlain4.bmp	1200.054 *Bytes*	800 x 500	ujiPlain4.txt	18 *Bytes*	0 : 0 : 21 : 104
13	kampus5.bmp	833.334 *Bytes*	640 x 434	kampus5.txt	18 *Bytes*	0 : 0 : 20 : 612
14	nama5.bmp	833.334 *Bytes*	640 x 434	nama5.txt	18 *Bytes*	0 : 0 : 20 : 762
15	ujiPlain5.bmp	833.334 *Bytes*	640 x 434	ujiPlain5.txt	18 *Bytes*	0 : 0 : 20 : 435
16	kampus6.bmp	451.638 *Bytes*	448 x 336	kampus6.txt	18 *Bytes*	0 : 0 : 19 : 790
17	nama6.bmp	451.638 *Bytes*	448 x 336	nama6.txt	18 *Bytes*	0 : 0 : 20 : 002
18	ujiPlain6.bmp	451.638 *Bytes*	448 x 336	ujiPlain6.txt	18 *Bytes*	0 : 0 : 19 : 819

8. Kesimpulan

Langkah pengamanan data pada aplikasi ini adalah data atau pesan teks terlebih dahulu dienkripsi menggunakan metode MMB yang selanjutnya disisipkan pada gambar menggunakan metode LSB. Besar ukuran file gambar sebelum dan setelah proses enkripsi tidak mengalami perubahan serta dapat menyembunyikan file teks ke dalam gambar tanpa diketahui oleh mata manusia secara kasat mata. Dengan kata lain perbandingan dari gambar sebelum dan sesudah proses hampir tidak ada perubahan atau perbedaan.

Besar file hasil dari proses dekripsi (plaintext) sebesar 18 bytes. Besar file tersebut didapat dari panjang plaintext sebesar 16 bytes dan penambahan 2 bytes atau 16 bit dari proses menggunakan metode MMB. Tingkat keberhasilan program 86% dan tingkat kegagalan program 14%.

Waktu proses yang dibutuhkan sesuai dengan dimensi gambar yang digunakan, semakin besar gambar tampungan (*cover-image*) semakin lama juga waktu yang dibutuhkan dalam proses enkripsi dan penyisipan atau *encode* maupun proses dekripsi dan ekstraksi atau *decode*.

9. Saran

Untuk penelitian selanjutnya data atau pesan yang diamankan dikembangkan menggunakan panjang teks lebih dari 16 karakter.

Untuk lebih meningkatkan keamanan disarankan mengkombinasikan metode MMB dengan teknik steganografi lainnya seperti Discrete Consine Transformation (DCT), Wavelet Transformation, Redundant Pattern Encoding, dan lain-lain..

Daftar Pustaka:

Adira, 2010, *Analisis dan Perancangan Aplikasi Steganografi pada Citra Digital Menggunakan Metode Least Significant Bit (LSB)*, UIN.

Afiadi, S. 2013. *Kriptografi Menggunakan Metoda MMB (Modular Multiplication-Based Block Cipher). Jurusan Teknik Informatika*, Universitas Muhammadiyah Jember: Laporan akhir Tidak dipublikasikan.

Anadra, Rezky, 2008, *Steganografi Pesan Pada Citra Menggunakan Metode LSB*, Bogor: Fakultas Ilmu Komputer Institut Pertanian Bogor.

Busran, 2012, *Analisa Komputasi Enkripsi Dan Dekripsi Data Gambar, Teks Dan Audio Dengan Menggunakan Algoritma RC4*, 5(1), 32-45

Cahyadi, Tri, 2012, *Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG,* Transient, 1(4), 282-290

Dahria, Muhammad, 2012, *Perangkat Lunak Pembelajaran Kriptografi Metode WAKE (Word Auto Key Encryption)*, Jurnal SAINTIKOM, 11(3), 143-162

Hidayat, Wildan, 2010, *Perlindungan Pesan Rahasia Pada Citra Digital Menggunakan Metode Least Significant Bit Steganografi*, Medan: Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sumatera Utara.

J, Vandewalee, et all, 1993, *Block Ciphers Based on Modular Arithmetic* (PDF).

K. Jia, et all, 2010. *Practical Time Attack on the Full MMB Block Cipher* (PDF)

Kromodimoeljo, Sentot, 2009, *Teori dan Aplikasi Kriptografi*, Bandung:SPK IT Consulting.

Latief, Mukhlisulfatih, 2010, *Studi Perbadingan Enkripsi Menggunakan Algoritma IDEA dan MMB*, Media Elektrik, 5(2),3-10

Munir Rinaldi, 2003, *Kriptografi, Diktat Kuliah IF5054 Kriptografi Program Studi Teknik Informatika*,, Institut Teknologi Bandung.

Prastyo, Fahri Perdana, 2010, *Steganografi menggunakan metode LSB dengan software Matlab*, Jakarta:UIN.

Rakhmat, Basuki, 2010, *Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan RC4*, Jurnal Dinamika Informatika, 5(2),1-17

Suranta, Ricardo Pramana, 2012, *Perbandingan Ketahanan Algoritma LSB dan F5 dalam Steganografi Citra*, Bandung:ITB