# STEGANOGRAFI DENGAN METODE LSB (LEAST SIGNIFICANT BIT) DAN METODE MMB (MULTIPICATION-BASED BLOCK CIPHER) UNTUK PENGAMANAN DATA BERBENTUK TEKS

Agi Ayu Nurdianta Barus[1], Mutammimul 'Ula[2]
[1]Mahasiswa Teknik Informatika Universitas Malikussaleh
[2]Dosen Teknik Informatika Universitas Malikussaleh

**Abstract**

*Security and confidentiality of data and information is the most important aspect of human activity undertaken. One way to maintain the security and confidentiality of personal data and the group is through cryptography and steganography techniques are believed to provide protection to the data and information held on the parties concerned. Through the incorporation of cryptography and steganography is expected to improve security on the data and information. This research was conducted by combining methods MMB on cryptography and steganography method of LSB in that run on Windows-based operating systems and can only hide a message with .txt format bitmap image format. MMB method is the development of IDEA method that uses 128 bit keys along the subblok divided into four pieces, each of which has a length of 32 bits. LSB method is a method that inserts the last bit of each pixel with a bit of the message.*

## Pendahuluan

Teknologi informasi dan komunikasi yang sangat berkembang saat ini dianggap semakin mempermudah proses pengolahan, penyimpanan dan pendistribusian data dan informasi sehingga memudahkan semua pihak termasuk pihak yang tidak berwenang untuk mengakses data dan informasi. Pada perusahaan besar, penyimpanan dokumen serta data-data penting adalah kewajiban yang harus dilakukan. Apabila data dan informasi penting tersebut dapat diakses oleh pihak yang tidak berwenang maka dapat berakibat kerugian bagi pihak perusahaan tersebut. Untuk itu, salah satu cara yang dapat digunakan untuk menjaga kerahasiaan data dan informasi penting tersebut adalah dengan mengubahnya kedalam bentuk sandi yang tidak bermakna yang hanya diketahui oleh pihak terkait. Hal ini dapat dilakukan dengan kriptografi.

Algoritma kriptografi modern pada umumnya beroperasi dalam mode bit daripada mode karakter seperti yang dilakukan pada chiper subtitusi atau chiper transposisi dari algoritma kriptografi klasik. Operasi pada mode bit berarti semua data dan informasi baik itu kunci, *plaintext, chipertext* dinyatakan dalam rangkaian bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plainteks yang dienkripsi menjadi *chipertext* dalam bentuk rangkaian bit ataupun sebaliknya. Salah satu algoritma kriptografi yang modern adalah *IDEA,* MMB dan masih banyak lagi yang lain. Kelemahan dari metode IDEA yang menggunakan *plaintext* 64 bit dan operasi perkalian modulo $2^{16} + 1$, diperbaiki oleh Joan Daemen dalam sebuah algoritma yang dinamakan MMB (*Modular Multiplication-based Block cipher*). Dengan menggunakan *plaintext* 64 bit (4 buah 16 bit *subblock text*), metode IDEA hanya dapat diimplementasikan pada prosesor 16 bit, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 bit. Kriptografi metode MMB menggunakan *plaintext* 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci).

Kerumitan algoritma ini, yang terletak pada proses operasi perkalian modulo $2^{32} - 1$, perhitungan fungsi non linier f pada proses enkripsi dan dekripsi, serta operasi *invers* pada proses dekripsi, menyebabkan algoritma ini sulit diproses secara manual.

Selain itu jika hanya sekedar mengacak pesan awal menjadi pesan tidak bermakna saja tidak dapat memberikan jaminan data akan tetap aman tanpa diketahui pihak lain. Seiring perkembangan ilmu pengetahuan, banyak pula cara untuk membongkar pesan rahasia yang telah diamankan menggunakan kriptografi tersebut. Untuk meningkatkan keamanan data, maka pada penelitian ini menambahkan metode LSB pada steganografi sehingga pesan rahasia yang telah diubah menggunakan kriptografi disisipkan kembali pada sebuah media berbentuk citra yang disebut steganografi.

## Kriptografi

Menurut kamus bahasa inggris Oxford kriptografi adalah "seni menulis atau pemecahan kode" ini dianggap sebagai sejarah yang dapat dipertanggungjawabkan sedangkan secara keseluruhan tidak dapat dibatasi pada hal tersebut saja. Selama berabad-abad lamanya definisi kriptografi hanya berfokus pada kode-kode yang memungkinkan untuk digunakan sebagai alat komunikasi rahasia tetapi dewasa ini kriptografi mencangkup lebih dari: hubungan mekanisme untuk kepastian integritas dan teknik untuk bertukar kunci rahasia.

## Algoritma *Modular Multiplication-Based Block Cipher* (MMB)

Metode MMB (*Modular Multiplication-based Block Cipher*) adalah sebuah perulangan blok *cipher* yang dirancang oleh Daemen, Govaerts dan Vandewalle sebagai perbaikan dari metode IDEA. Dengan *plaintext* 64 bit, metode IDEA hanya dapat diimplementasikan pada prosesor 16 bit, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 bit. Sedangkan metode MMB hadir dengan menggunakan plaintext 128

bit dan perulangan algorita yang terdiri atas langkah-langkah linier dan aplikasi paralel dari empat subtitusi non linier besar yang dapat dibalik. MMB menggunakan urutan kunci sederhana yang berurut dari posisi kiri, misalnya kunci untuk putaran ke-0 adalah $k_0$, $k_1$, $k_2$, $k_3$, kunci untuk putaran ke-1 adalah $k_1$, $k_2$, $k_3$, $k_0$ dan seterusnya.

**Enkripsi**

Enkripsi merupakan proses pengacakan data yang bertujuan untuk menyembunyikan pesan dari pihak ketiga atau pihak yang tidak berhak atas pesan tersebut. Enkripsi pada metode MMB terdapat enam buah transformasi rotasi. Dimana $X_j$ dengan panjang 128 bit diinputkan pada putaran (j+1) dan $X_0$ merupakan *plaintext*. *Ciphertext* dinotasikan sebagai c. Pada metode MMB konstanta yang digunakan pada proses enkripsi dapat dirincikan sebagai berikut:

i. $C = (2AAAAAAA)_{16}$
ii. $c_0 = (025F1CDB)_{16}$
iii. $c_1 = 2 * c_0$
iv. $c_2 = 2^3 * c_0$
v. $c_3 = 2^7 * c_0$

**Dekripsi**

Dekripsi merupakan proses kebalikan dari proses enkripsi, merubah *ciphertext* kembali ke dalam bentuk *plaintext*. Sedangkan konstanta pada metode MMB yang digunakan pada proses dekripsi dapat dirincikan sebagai berikut

i. $C = (2AAAAAAA)_{16}$
ii. $c_0^{-1} = (0DAD4694)_{16}$
iii. $c_1^{-1} = 2^{-1} * c_0^{-1}$
iv. $c_2^{-1} = 2^{-3} * c_0^{-1}$
v. $c_3^{-1} = 2^{-7} * c_0^{-1}$

**Steganografi**

Steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Steganografi sebagai suatu teknik penyembunyian informasi pada data digital lainnya

### *Least Significant Bit* (LSB)

Salah satu metode steganografi adalah LSB (Least *Significant Bit*). Langkah digunakan yaitu dengan menyisipkan bit terakhir (*least*) pada setiap *pixel* dengan bit pesan. Penyisipan pada LSB akan merubah nilai bit, tetapi tidak tampak kasat mata, sehingga pihak ketiga tidak mengetahui adanya pesan rahasia dibalik media *cover.*

### Proses Enkripsi Dan Steganografi

Adapun proses enkripsi dan steganografi yang terjadi pada sistem ini adalah sebagai berikut :

i. Input teks, teks dapat diinput langsung pada sistem atau melalui *file* teks dengan ektensi file .txt.

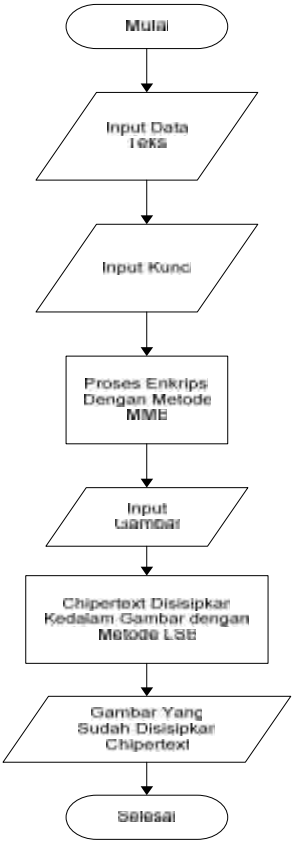
ii. Input kunci, panjang kunci maksimal 16 karakter.

iii. Kemudian sistem melakukan proses enkripsi dengan metode MMB.

iv. Input gambar yang akan dijadikan media penyisipan teks hasil enkripsi, gambar yang diinput dengan ektensi file .bmp.

v. Selanjutnya sistem akan melakukan penyisipan file teks dengan metode LSB.

vi. Lalu sistem akan menghasilkan gambar yang telah berhasil disisipkan file yang telah menjadi *ciphertext*




Gambar 1. Diagram Sistem Proses Enkripsi Dan Steganografi

**Proses Dekripsi Dan Ekstraksi**

Adapun proses dekripsi dan ekstraksi yang terjadi pada sistem ini adalah sebagai berikut :

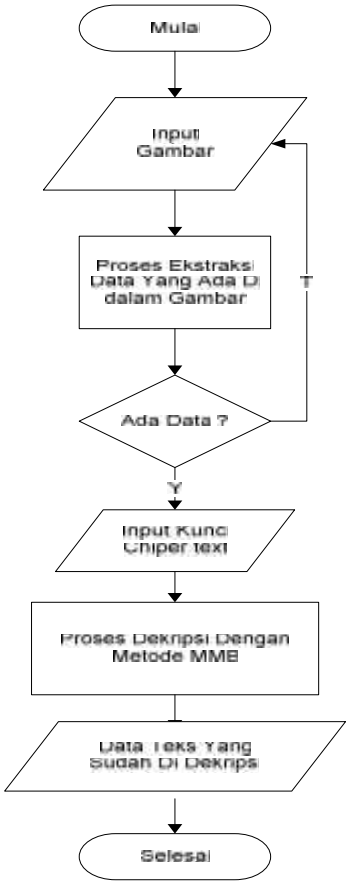
i. Input gambar yang dijadikan media penyisipan teks hasil enkripsi, gambar yang diinput dengan ektensi *file* .bmp.

ii. Proses ekstraksi data yang ada didalam gambar.

iii. Jika ada data maka sistem akan meminta input kunci, jika tidak ada data maka sistem akan meminta input gambar kembali.

iv. Kemudian sistem akan melakukan proses dekripsi dengan metode MMB.

v. Sistem akan menghasilkan data teks yang telah berhasil didekripsi




Gambar 2. Diagram Sistem Proses Dekripsi Dan Ekstraksi

## Unjuk Kerja Sistem

Unjuk kerja sistem ini dilakukan berdasarkan pengukuran seluruh data pengujian dari 10 sampel gambar terhadap 1 sampel data teks yang akan diinputkan dan 10 sampel data teks terhadap 1 sampel gambar. Pengujian pertama dilakukan pada 10 file gambar terhadap 1 file teks yang diinputkan. Dalam pengujian ini, peneliti menginputkan file teks dengan judul "Pendahuluan" dengan kapasitas 5 kb dengan jumlah karakter 4558

| File Gambar | Kapasitas Gambar Asli | Kapasitas Gambar Setelah Proses |
|---|---|---|
| Gambar 1 | 858KB | 2.25MB |
| Gambar 2 | 826KB | 2.25MB |
| Gambar 3 | 108KB | 549KB |
| Gambar 4 | 581KB | 2.25MB |
| Gambar 5 | 81,4 KB | 549KB |
| Gambar 6 | 41,5KB | 197KB |
| Gambar 7 | 157KB | 1.73MB |
| Gambar 8 | 27,3KB | 87,9KB |
| Gambar 9 | 95KB | 732KB |
| Gambar 10 | 26,8KB | 117KB |
| **Total** | **2802KB** | **10711,9KB** |
| **Nilai Rata-Rata** | **280.2KB** | **10961,9KB** |

Gambar 3 Unjuk kerja sistem pengujian pertama

Pengujian kedua dilakukan pada 10 file teks terhadap 1 file gambar. Dalam pengujian ini, peneliti menginputkan file gambar dengan kapasitas gambar 157KB dan resolusi gambar 800 x 600

| File Teks | Jumlah Karakter Teks | Kapasitas Gambar Setelah Proses |
|---|---|---|
| Teks 1 | 789 | 1,37MB |
| Teks 2 | 1699 | 1,37MB |
| Teks 3 | 2213 | 1,37MB |
| Teks 4 | 2863 | 1,37MB |
| Teks 5 | 3484 | 1,37MB |
| Teks 6 | 3729 | 1,37MB |
| Teks 7 | 4279 | 1,37MB |
| Teks 8 | 4529 | 1,37MB |
| Teks 9 | 4859 | 1,37MB |
| Teks 10 | 5875 | 1,37MB |
| **Total** | **34316** | **13.7MB** |
| **Nilai Rata-Rata** | **3431.6** | **1.37MB** |

Gambar 4. Unjuk kerja sistem pengujian kedua

Pengujian ketiga dilakukan pada 10 file gambar terhadap 1 file teks. Dalam pengujian ini, peneliti menginputkan file gambar dengan kapasitas gambar yang berbeda, akan tetapi resolusi gambar yang sama yaitu sebesar 500 x 500 dan ukuran file text sebesar 1,16 KB

| File Gambar | Resolusi Gambar | Kapasitas Gambar Sebelum Proses | Kapasitas Gambar Setelah Proses |
|---|---|---|---|
| Gambar 1 | 500 x 500 | 92,1KB | 732KB |
| Gambar 2 | 500 x 500 | 99,3KB | 732KB |
| Gambar 3 | 500 x 500 | 40,7KB | 732KB |
| Gambar 4 | 500 x 500 | 122KB | 732KB |
| Gambar 5 | 500 x 500 | 55,8KB | 732KB |
| Gambar 6 | 500 x 500 | 110KB | 732KB |
| Gambar 7 | 500 x 500 | 38,9KB | 732KB |
| Gambar 8 | 500 x 500 | 82,3KB | 732KB |
| Gambar 9 | 500 x 500 | 50,5KB | 732KB |
| Gambar 10 | 500 x 500 | 31,6KB | 732KB |
| **Total** | - | **1023.2KB** | **7320KB** |
| **Nilai Rata-Rata** | - | **551.6KB** | **732KB** |

Gambar 5. Unjuk kerja sistem pengujian ketiga

Pengujian keempat dilakukan pada 1 gambar terhadap 10 file teks. Dalam pengujian ini, peneliti menginputkan file teks dengan kapasitas ataupun jumlah karakter yang berbeda dan kapasitas gambar yang digunakan

| File Teks | Jumlah Karakter Teks | Status Proses |
|---|---|---|
| Teks 1 | 4551 | Berhasil |
| Teks 2 | 5056 | Berhasil |
| Teks 3 | 6044 | Berhasil |
| Teks 4 | 9769 | Berhasil |
| Teks 5 | 14338 | Berhasil |
| Teks 6 | 22425 | Gagal |
| Teks 7 | 20039 | Gagal |
| Teks 8 | 19468 | Gagal |
| Teks 9 | 18905 | Gagal |
| Teks 10 | 14954 | Berhasil |
| **Total** | **135549** | - |
| **Nilai Rata-Rata** | **13555** | - |

Gambar 6. Unjuk kerja sistem pengujian keempat

Berdasarkan hasil pengujian diatas dapat diambil kesimpulan bahwa kapasitas gambar sebelum disisipkan file teks akan terjadi penambahan kapasitas gambar, dan perubahan kapasitas gambar tidak berpengaruh dari besar atau tidaknya file teks yang akan disisipkan, melainkan yang mempengaruhi dari perubahan kapasitas gambar adalah dari resolusi gambar itu sendiri

## Kesimpulan

Dengan menggunakan dikombinasikan steganografi dengan kriptografi ini dapat meningkatkan jaminan kerahasiaan pesan maupun file-file informasi. Berdasarkan pengujian pertama, kedua ketiga dan keempat kapasitas gambar yang digunakan untuk proses steganografi akan terjadi penambahan dari kapasitas

gamabar semula, akan tetapi perubahan kapasitas gambar tidak berpengaruh dari kapasitas file teks yang akan disisipkan.

**Referensi**

[1]. Ashur, Tomer. Orr Dunkelman, 2013. " A Practical Related-Key Boomerang Attack for the Full MMB Block Cipher". Springer International Publishing Switzerland.

[2]. Jia, Keting. Jiaze Chen, Meiqin Wang, Xiaoyun Wang, 2012. "Practical Attack on the Full MMB Block Cipher". Springer-Verlag Berlin Heidelberg.

[3]. Katz, Jonathan. Yehuda Lindell, 2015. Intoduction to Modern Cryptography Second Edition. CRC Press.

[4]. Rakhmat, Basuki. Muhammad Fairuzabadi, 2010. "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere dan RC4".Jurnal Dinamika Informatika.

[5]. Thangadurai, K. G.Sudha Devi, 2014. "An analysis of LSB Based Image Steganography Techniques". International Conference on Computer Communication and Informatics (ICCCI).