Penerapan Algoritma MMB (Modular Multiplication-based Block Cipher) Pada Sebuah Perangkat Lunak

Cahya Dwi Rahayu[1], Triawan Adi Cahyanto, M.Kom [2 *]

[1,3] *Jurusan Teknologi Informasi*
Jln. Karimata no. 49 Sumbersari Jawa Timur 68121
[1]cahyadwir@gmail.com
[3*]penulis3@ugm.ac.id (penulis korespondensi)

Intisari— **Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi steganografi dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, steganografi digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi. Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya**. **Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi dapat dipandang sebagai kelanjutan kriptografi.** *Kata kunci*—Steganografi, elektronik, identifikasi, digital, kriptografi.

Abstract— **The more important the value of an information, then the more advanced methods that can be used to make the insertion of information is supported also with the growing electronic media. Various kinds of electronic media can now be used to perform various steganography functions with various purposes and functions expected by users. As a general function, steganography is used to provide a special stamp in a work made in electronic media format as identification. Steganography is a technique for hiding personal information with something that results will look like any other normal information. Digital steganography uses digital media as a container container, such as imagery, sound, text, and video. Secret hidden data can also be imagery, sound, text, or video. Steganography can be seen as a continuation of cryptography.** *Keywords*— Steganography, electronic, identification, digital, cryptography.

I. PENDAHULUAN

Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi steganografi dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, steganografi digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi.

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya “tersembunyi atau terselubung”, dan graphein, “menulis”. Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (file) komputer. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan tetap tersedia, maka dengan steganografi dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tapi metoda ini sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan. Kedua teknik ini dapat digabungkan untuk mendapatkan metoda pengiriman rahasia yang sulit dilacak. Pertama pesan dienkrip,

kemudian cipherteks disembunyikan dengan cara steganografi pada media yang tampak tidak mencurigakan. Cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan.

II. METODOLOGI PENELITIAN

Algoritma MMB merupakan algoritma block cipher dengan panjang 128 bit yang nantinya dibagi menjadi 4 sub-blok masing-masing berukuran 32 bit subblock text (x0, x1,x2, x3) dan 32 bit subblock kunci (k0. k1,k2, k3), dan penerapan proses operasi perkalian modulo 232–1, perhitungan fungsi non linier f pada proses enkripsi dan dekripsi, serta operasi invers pada proses dekripsi. Hasil yang diperoleh adalah algoritma MMB yang diterapkan pada aplikasi manajemen password dapat menjaga keamanan dan kerahasiaan data identitas digital pengguna dengan menerapkan proses enkripsi dan dekripsi antara plainteks dan cipherteks dengan kunci. Kelemahan dari aplikasi yang dibangun terletak pada pola plainteks, karena blok plainteks yang sama selalu menghasilkan blok cipherteks yang sama. Sehingga jika cryptanalyst mengetahui hasil enkripsi dari salah satu blok plainteks maka dia dapat dengan mudah mendekripsi cipherteks dengan bentuk yang sama setiap kali cipherteks tersebut terlihat di dalam pesan.

Steganography juga berbeda dengan cryptography yaitu terletak pada hasil keluarannya.Hasil dari cryptography biasanya berupa data yang berbeda dari bentuk aslinya dan biasanyadatanya seolah-olah berantakan namun dapat dikembalikan ke data semula. Sedangkan hasil dari keluaran steganography memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh komputer atau pengolah data digital lainnya. Selain itu pada steganography keberadaan informasi yang disembunyikan tidak terlihat/diketahui dan terjadi penyampulan tulisan (covered writing). Sedangkan pada cryptography informasi dikodekan dengan enkripsi atau teknik pengkodean dan informasi diketahui keberadaanya tetapi tidak dimengerti maksudnya. Namun secara umum steganography dan cryptography mempunyai tujuan yang sama yakni mengamankan data, bagaimana supaya data tidak dapat dibaca, dimengerti atau diketahui secara langsung. Steganography memanfaatkan kekurangan - kekurangan indra manusia seperti mata dan telinga. Dengan kekurangan inilah maka teknik ini dapat diterapkan dalam berbagai media digital. Media cover merupakan data digital yang akan ditempeli dengan data yang akan disembunyikan atau sering disebut dengan stego medium. Berbagai media yang dapat digunakan sebagai cover dari data atau informasi yang akan disembunyikan dengan berbagai teknik steganography. Media yang dimaksudkan adalah media dalam bentuk file digital dengan berbagai format, antara lain :Images (bmp, gif, jpeg, tif, dll), Audio (wav, Mp3, dll), Video, Teks.

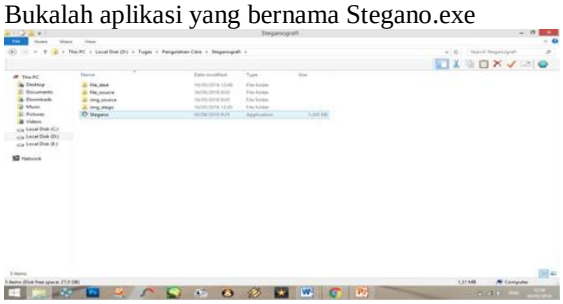
Tujuan dari teknik-teknik steganografi adalah menyembunyikan keberadaan pesan.Teknik watermarking, merupakan bagian dari steganografi yang ditujukan untuk perlindungan hak cipta, tidak hanya dimaksudkan untuk menyembunyikan keberadaan pesan atau informasi, tapi lebih diarahkan untuk menjamin informasi dapat selamat dari beragam serangan yang dimaksudkan untuk menghancurkan watermark.

III. HASIL DAN PEMBAHASAN

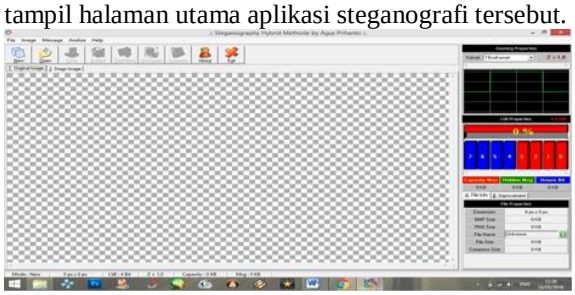
A. Cara Menggunakan Program

Adapun langkah-langkah menggunakan aplikasi steganografi ini adalah sebagai berikut:

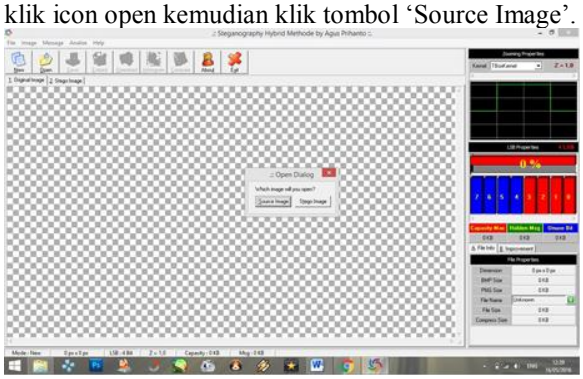
1. Bukalah aplikasi yang bernama Stegano.exe



2. Setelah anda membuka aplikasi tersebut, maka akan tampil halaman utama aplikasi steganografi tersebut.

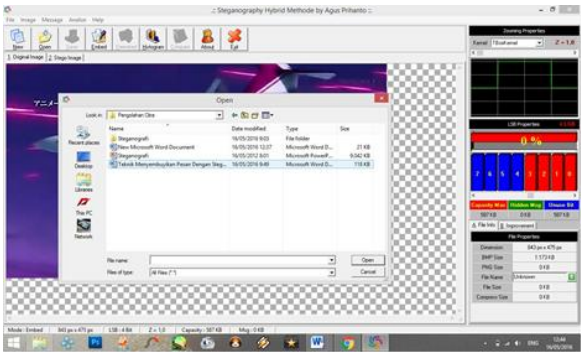


3. Untuk membuka gambar yang akan digunakan untuk menyembunyikan file rahasia yang ingin dimasukkan, klik icon open kemudian klik tombol ‘Source Image’.

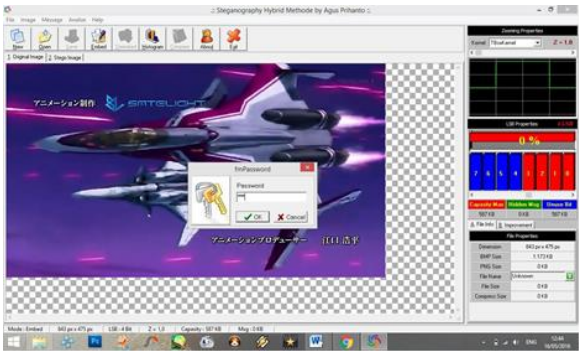


4. Setelah menentukan gambar yang akan digunakan, maka akan tampil gambar yang telah dipilih.

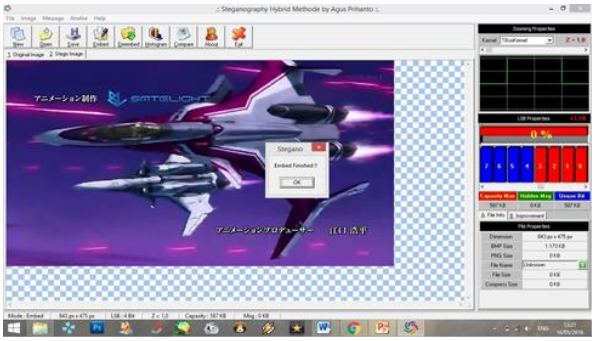
5. Selanjutnya, untuk menyisipkan file ke dalam gambar yang dipilih, klik icon



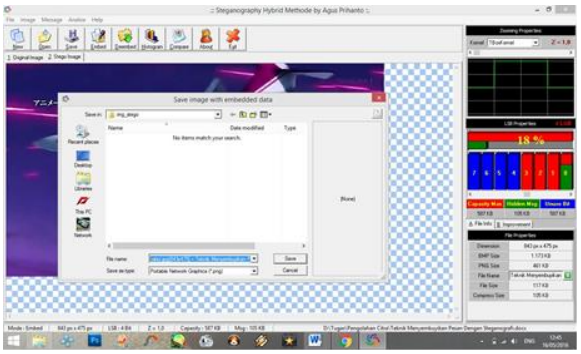
6. Setelah file dipilih, maka akan otomatis muncul tampilan seperti dibawah ini, kemudian silahkan masukkan password yang anda inginkan.



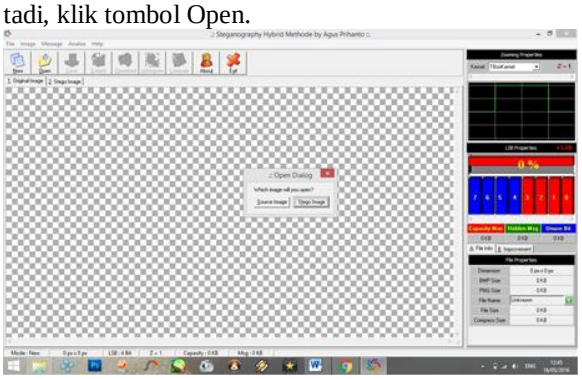
7. Setelah itu akan muncul tampilan seperti di bawah ini.



8. *Simpan gambar yang telah di embed tadi dengan mengklik ikon Save ke folder yang anda inginkan. Jika sudah selesai tutup program dengan mengklik ikon Exit.*Seluruh dokumen harus dalam Times New Roman

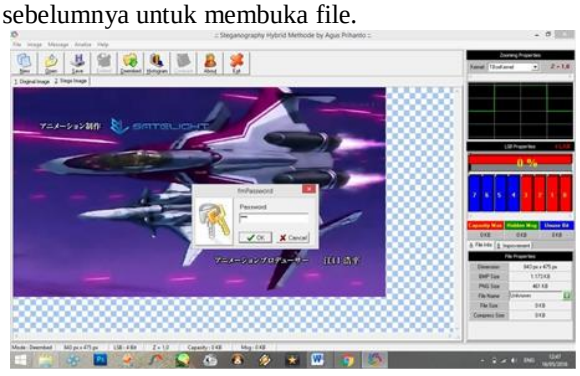


9. Jika anda ingin membuka gambar yang telah di embed tadi, klik tombol Open.

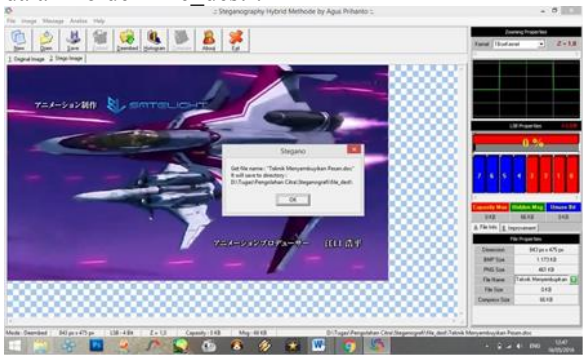


10. Setelah itu akan muncul tampilan seperti di bawah ini.

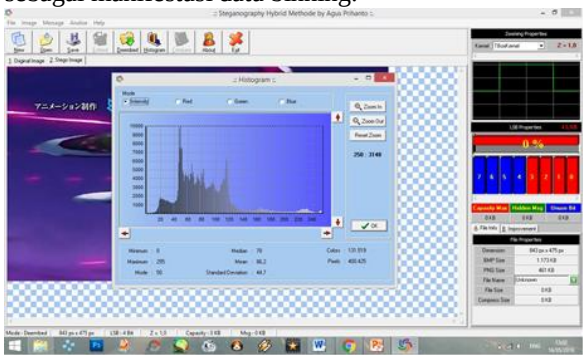
11. Setelah itu untuk membuka file yang akan di keluarkan, klik icon ‘Deembed’ maka akan otomatis muncul tampilan form password seperti dibawah ini kemudian masukkan password yang telah ditentukan sebelumnya untuk membuka file.



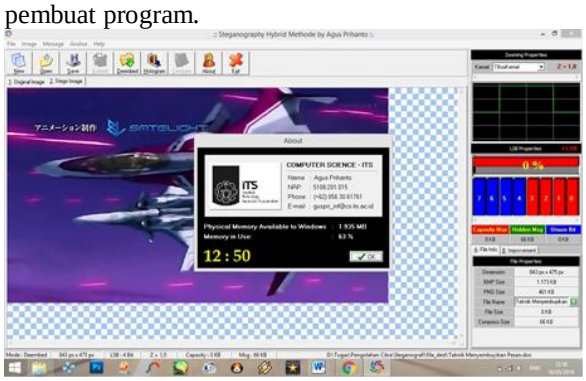
12. Setelah itu muncul pesan seperti di bawah ini. File yang sudah dikeluarkan tadi akan otomatis disimpan dalam folder ‘file_dest’.



13. Jika anda mengklik ikon Histogram, maka muncul form sebagai berikut. Tampilan ini menampilkan grafik dari tabulasi frekuensi warna dari citra digital yang digambarkan dengan grafis batangan sebagai manifestasi data binning.



14. Jika anda mengklik ikon About maka akan muncul tampilan yang berisi sekilas tentang nama pembuat program.



IV. KESIMPULAN

Teknik steganografi dibandingkan dengan kriptografi memiliki keunggulan yaitu dengan steganografi keberadaan dari informasi yang disembunyikan tidak dapat dideteksi dengan mudah, dengan steganografi informasi disembunyikan sedemikian rupa sehingga menghilangkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui.Kesimpulan ditulis dalam bentuk paragraf uraian. Hindari penggunaan bulleted list.

Keterbatasan manusia pada indera penglihatan dapat dimanfaatkan, terutama pada perubahan warna yang sangat sedikit dan perubahan kecil pada intensitas gambar. Penulis berkesimpulan bahwa dengan memberikan perubahan kecil pada warna di sebagian daerah berintensitas sangat rendah dari suatu citra digital (watemarking parsial), maka akan diperoleh citra yang sudah diberi tanda yang memiliki fidelity yang sangat baik, yaitu tingkat degradasinya tidak dirasakan oleh pengamatan manusia.

REFERENSI

[1] https://muhammadrida14.wordpress.

[2] http://rhyoeozonit29tugaskuliah.blogspot.co.id