ISBN: 978-602-60280-1-3

Implementasi Teknik Steganografi Pada Pesan Teks dan Emoji Menggunakan Metode LSB (Least Significant Bit) dan Algoritma Hill Cipher

Muhammad Syaiful Amin[1], Dani Arifudin[2], Dony Ariyus[3]
Program Studi Magister Teknik Informatika
Universitas Amikom Yogyakarta
Email: othiwa22@gmail.com,
barudhani@gmail.com,
dony.a@amikom.ac.id

ABSTRAK-Perkembangan penggunaan teknologi informasi saat ini, terutama penggunaan social media semakin memudahkan aktivitas kejahatan komputer (cyber crime) seperti cracker, script kiddies, carder dan lamer dan sebagainya. Penyalahgunaan teknologi komputer tersebut merupakan aktivitas yang sangat mengganggu privasi seseorang. Oleh karena itu diperlukan sebuah sistem pengamanan data Untuk mempersulit para pelaku kejahatan komputer. Metode enkripsi algoritma Hill Cipher dan metode steganografi LSB (Least Significant Bit), dapat diimplementasikan untuk menambah keamanan sebuah data. Metode LSB (Least Significant Bit) melakukan penyimpanan data dengan cara mengganti bit-bit yang tidak signifikan (least significant pixel) pada berkas (file) wadah (cover) dengan bit-bit berkas yang akan disimpan. Penelitian ini berfokus pada pengamanan pada informasi pesan wassap. Hasil dari penelitian ini adalah sebuah aplikasi untuk menyimpan informasi rahasia yang akan disebarkan melalui pesan wassap.

Kata Kunci: Steganografi, Hill Cipher, Least Significant Bit, Enkripsi, Emoji

I. PENDAHULUAN

Hampir setiap orang yang mempunyai smartphone telah memiliki akses untuk memanfaatkan social media.Teknologi informasi sangat berkembang dengan pesat dan memberikan pengaruh besar bagi seluruh kehidupan manusia. Seiring Perkembangan teknologi informasi yang ada, internet tidak lagi menjamin penyediaan informasi yang aman. Berbagai mesin pencari (*search-engine*) ditambah dengan serangan virus, penyadap, spam maupun hacker yang menjamur dapat mencuri data-data bersifat rahasia. Social media menjadi salah satu target untuk melakukan tindakan yang tidak diinginkan dengan mudah. Untuk mengatasi hal tersebut berbagai cara untuk meningkatkan keamanan data terus dikembangkan, diantaranya kriptografi dan steganografi.

Secara umum, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentifikasi data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih kearah metode-metode yang digunakan [1]. Salah satu metode yang akan dibahas dalam penelitian ini adalah proses enkripsi algoritma *Hill Cipher* dengan menambahkan steganografi. Steganografi merupakan seni untuk menyembunyikan pesan di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut [2].

Pada penelitian kali ini, peneliti mencoba untuk fokus membahas teknik steganografi untuk pengamanan pada pengiriman teks wassap. Keamanan informasi pada teks wassap sangat diperlukan untuk memberikan pesan informasi yang rahasia. Umumnya pada aplikasi wassap, ketika kita akan menuliskan pesan dengan huruf biasa, maka akan muncul teks yang sama. Hal ini akan sangat berbahaya apabila pesan kita telah diketahui oleh pihak yang tidak bertanggung jawab. Oleh karena itu peneliti mencoba untuk membuat sebuah aplikasi yang bertujuan untuk merahasiakan informasi yang akan disampaikan dengan menggunakan imoji.

Teknik yang digunakan yaitu dengan mengenkripsi pesan terlebih dahulu (kriptografi), kemudian menyisipkannya ke media cover (steganografi). Namun, proses penyisipan dapat berpengaruh pada kualitas media cover tersebut. Upaya untuk meminimalisir perubahan kualitas *cover* dapat dilakukan dengan penyisipan pada bit terakhir (*least significant bit*). Perubahan kualitas *cover* tidak tampak kasat mata, tetapi penyisipan pada bit terakhir dapat mengakibatkan pesan rusak ketkia citra dikompresi. Ketahanan terhadap *robust* dapat dilakukan dengan pemilihan pada bit pertama (*most significant bit*), tetapi justru mengakibatkan perubahan kualitas *cover* menjadi tampak dan dapat dicurigai [3].

II. TINJAUAN PUSTAKA

A. Enkripsi dan Dekripsi

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi merupakan proses perubahan data asli (*plaintext*) menjadi *ciphertext* (data yang tidak dapat dimengerti) sedangkan, sedangkan Dekripsi kebalikan dari enkripsi yaitu proses pengembalian bentuk *ciphertext* menjadi *plaintext* kembali sehingga bisa dipahami. Enkripsi dan Dekripsi dilakukan menggunakan kunci yang sudah ditentukan [4].

B. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Menurut Bruce Schneier [5], kriptografi dapat diartikan

ISBN: 978-602-60280-1-3

sebagai ilmu pengetahuan dan seni untuk menjaga keamanan pesan. Dalam penelitian ini kriptografi akan digunakan sebagai pengganti kunci pada proses steganografi sekaligus memberikan perlindungan tambahan terhadap data yang disembunyikan.

Kriptografi terdiri dari dua proses utama yaitu enkripsi dan dekripsi. Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, terdapat dua jenis algoritme kriptografi yaitu kunci asimetri dan simetri. Algoritma kunci simetri terbagi ke dalam dua kategori [6], yaitu:

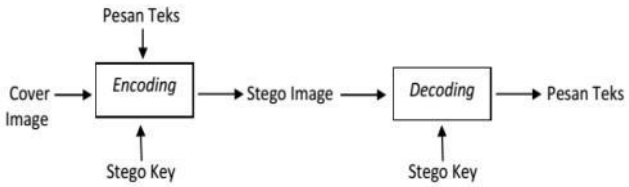
1. *Stream cipher* Algoritma ini mengolah data dalam bentuk bit-bit tunggal. Proses enkripsi/dekripsi akan dilakukan pada satu bit dalam satu waktu.
2. *Block cipher* Algoritma ini memecah data yang masuk menjadi beberapa blok dengan panjang data tertentu. Proses enkripsi/dekripsi akan dilakukan pada satu blok data dalam satu waktu

C. Steganografi

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainnya. Steganografi mempnyai sejarah yang hampir sama dengan kriptografi, keduanya banyak di gunakan terutama pada zaman perang. Steganografi dapat di pelajari lebih jauh dalam. Perbedaan steganografi dengan kriftografi terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. Kriptografi melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya, sedangkan steganografi menyembunyikan dalam data lain yang akan di tumpanginya tanpa mengubah data yang di tumpanginya tersebut sehingga data yang di tumpanginyasebelum dan sesudah peruses penymbunyian hampir sama.

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis [7]. Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak tak dapat dibaca dan keberadaan pesan sering dikenal [8].

Salah satu *cover image* yang dapat digunakan untuk menyembunyikan pesan adalah citra digital warna 24 bit. Setiap *pixel* pada citra warna 24 bit memiliki warna yang merupakan kombinasi dari tiga warna dasar *Red*, *Green*, *Blue* (RGB*)*. Sedangkan satu *pixel* citra warna 24 bit diwakili oleh tiga *byte*, dimana masing-masing *byte* merepresentasikan warna *Red*, *Green* dan *Blue*. Penyisipan pesan ke dalam *cover image* dinamakan *encoding*, sedangkan ekstraksi pesan dari *stego image* dinamakan *decoding.* Kedua proses memerlukan kunci rahasia (*stego key*), agar hanya pihak yang mempunyai kunci rahasia saja yang dapat melakukan penyisipan dan ekstraksi pesan. Proses *encoding* dan *decoding* diberikan dalam bentuk diagram pada gambar 1 berikut



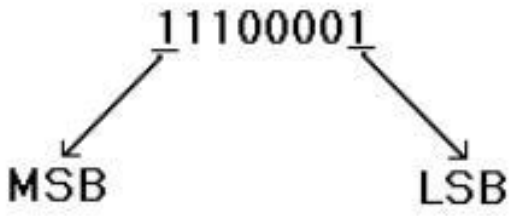
Gambar 2.1. Diagram penyisipan dan ekstraksi pesan

D. *Hill Cipher*

Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang menggunakan aritmetika modulo terhadap matriks. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m (matriks persegi) yang *invertible* dalam modulus p, sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan *dalam Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Proses enkripsi pada algoritma *Hill Cipher* dimulai dengan mengkonversikan *plaintext* kedalam angka sesuai dengan table korespondensi. Selanjutnya angka-angka tersebut dikelompokkan menjadi beberapa blok, dimana masing-masing blok terdiri dari m anggota sesuai dengan ordo matriks kunci K(mxm). Selanjutnya dicari *ciphertext* dengan C= K * P. Proses Dekripsi diawali dengan mengkonversikan *ciphertext* kedalam angka sesuai dengan table korespondensi. Seperti halnya pada proses enkripsi, angka-angka tersebut dikelompokkan menjadi beberapa blok dengan anggota masing-masing blok sebanyak m, lalu dicari *plaintext*nya dengan P = K-1 * C.

III. METODE PENELITIAN

Least Significant Bit adalah bit yang memiliki nilai terendah dalam barisan biner. Sedangkan bit yang memiliki nilai tertinggi disebut *Most Significant Bit*.



Gambar 3.1 MSB dan LSB

Pada file biasanya terdapat bit-bit LSB yang perannya tidak terlalu penting dan dapat diganti dengan informasi lain tanpa merusak file tersebut. Karena memanfaatkan bit-bit LSB, metode ini tidak digunakan pada media yang mengalami kompresi terutama jenis *lossy compression* karena akan menghilangkan bit-bit LSB tersebut. Penggunaan metode LSB umumnya tidak mengubah ukuran file dan bekerja dengan baik pada file gambar/audio yang memiliki resolusi/bit rate tinggi [9].

Dalam gambar digital, penggantian bit-bit LSB pada warna akan menyebabkan perubahan sebesar satu angka dari nilai sebelumnya. Perubahan ini tidak menimbulkan perubahan warna yang signifikan sehingga mata manusia sulit untuk mendeteksi perubahan yang terjadi. Metode LSB bekerja dengan memanfaatkan keterbatasan indera

ISBN: 978-602-60280-1-3

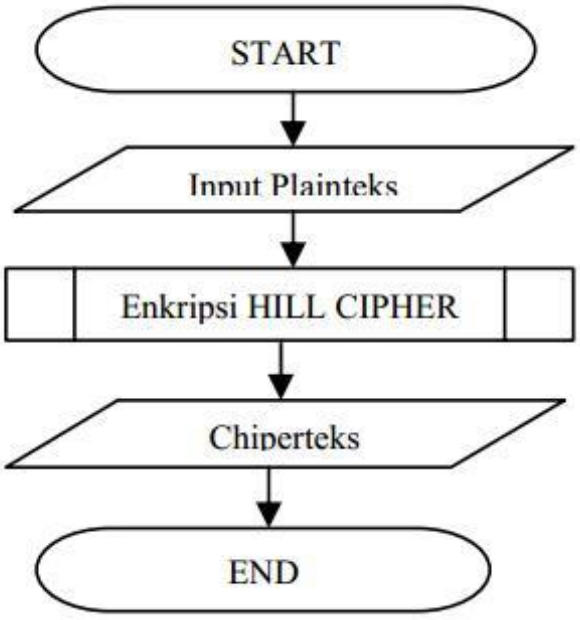
penglihatan manusia yang kurang peka terhadap perubahan warna tersebut. Pada penyisipan pesan dalam berkas bitmap 24-bit, terdapat 3 bit LSB yang dapat kita manfaat dari setiap pixel yaitu komponen Red, Green, dan Blue. Pesan yang akan disisipkan cenderung mempunyai panjang yang dinamis. Oleh karena kita membutuhkan sebuah header untuk menyimpan panjang pesan yang disisipkan. Misal: panjang pesan maksimal yang akan disisipkan adalah 255 karakter, maka kita membutuhkan header berukuran 1 byte atau 8 bit. Jadi, untuk menyisipkan huruf 'A' kita membutuhkan 3 piksel tambahan. Panjang pesan yaitu 1 karakter (biner: 00000001). Total piksel yang dibutuhkan adalah 6 piksel.

00100101	11101000	11001001
00100011	11001010	11101011
11001010	00100110	11101001
00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

Pixel setelah penyisipan: (8 bit pertama merupakan data *header)*

00100100	11101000	11001000
00100010	11001010	11101010
11001010	00100111	11101000
00100111	11101000	11001000
00100110	11001000	11101000
11001001	00100111	11101001

Dari contoh terlihat bahwa tidak semua nilai warna dari pixel mengalami perubahan. Dan untuk nilai warna yang mengalami perubahan hanya memiliki perbedaan sebesar satu angka dari nilai aslinya. Namun, penggunaan metode LSB membutuhkan media penyamaran yang cukup besar dalam menyembunyikan pesan [10].



Gambar 3.2. Flowchart Sistem Enkripsi

Pada gambar 3.2. menjelaskan tentang Proses kerja enkripsi.

IV. HASIL DAN PEMBAHASAN

Berikut ini adalah langkah-langkah penyandian pesan mengunakan kunci matriks 2x2, yaitu sebagai berikut :

1. Tahap pertama adalah menyiapkan Pesan dan Kunci Matriks.

$$\begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix}$$

2. Pesan dirubah menjadi kode dan matriks 2x2
3. Mengalikan matriks pesan dan matriks kunci
4. Matriks dirubah menjadi deret pesan
5. Kode pesan dirubah menjadi huruf (karakter)

Kemudian setelah proses enkripsi selesai dilakukan, maka untuk mendeskripsi *chipertext* menjadi pesan kembali sebenarnya hampir sama dengan cara enkripsi. Tetapi kunci yang digunakan harus di *invers* terlebih dahulu. Untuk lebih jelasnya tentang proses dekskripsi *chipertext* diatas, dibawah ini dijelaskan secara rinci tentang tahap-tahap deskripsi yang dimaksud yaitu :

1. Invers matriks kunci
2. Menyiapkan pesan chipper
3. *Chiper* dirubah menjadi kode dan matriks
4. Mengalikan matriks pesan *chiper* dengan *invers* matriks kunci
5. Matriks pesan dirubah menjadi deret kode
6. Kode dirubah menjadi pesan kembali dalam bentuk emoji

A. Analisa LSB *(Least Significant Bit)*

1. Menyiiapkan pesan
2. Pesan dirubah menjadi biner
3. Menyiapkan gambar dan mengetahui nilai RGB setiap pixel
4. Menyisipkan 1 bit pesan ke setiap bit ke-8 pada tiap-tiap warna pixel

B. Tampilan Program

Pada Tampilan ini berguna untuk melihat dan memahami bagaimana program berjalan. Dari tampilan ini diharapkan akan menambah pemahaman permbaca terhadap alur jalan dan prinsip kerja dari program steganografi dan enkripsi teks

1. Tampilan Menu Utama

Tampilan *Form* menu utama adalah jendela awal atau jendela untuk untuk menampung semua menu yang tersedia dalam program steganografi. Jendela ini keluar pertama kali saat program dijalankan dan juga rancangan jendela ini sangat sederhanya dengan hanya berisi beberapa menu yang dibutuhkan untuk steganografi to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

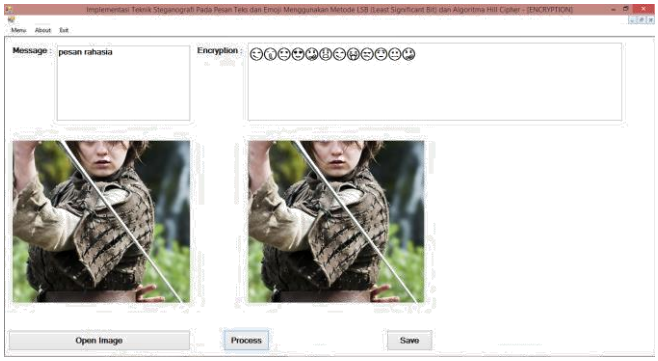
ISBN: 978-602-60280-1-3

Gambar 4.1. Tampilan Menu Utama

Pada gambar 4.1. terdapat beberapa menu diantaranya adalah Menu, About dan Exit.

2. *Form* Enkripsi

Tampilan *Form* Enkripsi adalah tampilan untuk menyisipkan pesan *chiper* kedalam citra gambar dengan dienkripsi terlebih dahulu. Dibawah terlihat bahwa gambar yang telah disispi pesan *chiper* tidak terlihat berubah oleh mata. Tetapi secara bit sebenarnya telah berubah beberapa.



Gambar 4.2. Tampilan *Form* Enkripsi

Gambar 4.2. merupakan tampilan dari hasil plainteks yang kemudian dienkripsi ke dalam emoji, selanjutnya emoji akan disisipkan ke dalam gambar.

3. *Form* Dekripsi

Tampilan ini berisi proses pengambilan pesan dari citra gambar, terlebhi dahulu gambar dimasukkan dengan mengklik tombol *Open Image* setelah itu dengan mengklik tombol *Process*, barulah pesan *chiper* didapat dan langsung dideskripsi kembali menjadi pesan utuh.

V. KESMPULAN

A. Kesimpulan

Dari penelitian ini maka dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Enkripsi teks dengan algoritma *hill chiper* adalah dengan mengubah masing-masing huruf teks menjadi matriks angka dengan memanfaatkan tabel kode yang telah ditentukan kemudian hasil perkalian antara matriks pesan dan kunci yang telah di modulus dengan 26 (duapuluh enam) diubah kembali menjadi urutan huruf dengan tabel kode. Setelah masing-masing huruf diacak atau dirubah, kemudian pesan atau huruf akan dirubah menjadi emoji. Untuk proses dekripsi sama seperti proses enkripsi, perbedaannya adalah matriks kunci di *invers* terlebih dahulu baru kemudian dilakukan perkalian dan modulus 26 hasil perkalian akan mengembalikan *chiper* ke bentuk pesan semula.
2. Dalam proses menerapkan *chipertext* yang telah dienkripsi dengan algoritma *hill chiper* ke dalam proses steganografi sama dengan menerapkan pesan biasa yang belum di sandikan atau dienkripsi, yaitu dengan mengubah pesan menjadi kode biner kemudian mengubah angka dari masing-masing piksel gambar menjadi imoji.

Untuk merancang sebuah sistem yang mampu menerapkan algoritma *hill chiper* dalam proses enkripsi dan menggunakan metode LSB dalam proses steganografi terlebih dahulu harus ditentukan kunci untuk enkripsi dan jumlah maksimal karakter yang digunakan serta jenis gambar yang digunakan. Kemudian untuk pembuatan aplikasi sesungguhnya dapat mengguanakan Visual Studio 2010 atau yang lebih tinggi

B. Saran

Untuk pengembangan penelitian ini, dapat diberikan beberapa saran sebagai berikut:

1. PenyisipankKarakter dapat lebih dari 66 karakter atau bahkan tidak terhingga.
2. Menggunakan warna dibawah 24 bit atau juga lebih dan dapat diterapkan pada gambar yang berekstensi .jpg, .png, .gif dan yang lainnya.
3. Menggunakan kuci matriks 3x3 atau lebih untuk enkripsi dengan algoritma *hill chiper*.
4. Menggunakan bahasa pemograman yang lebih populer lainnya serperti C++, C#, Python dan lainya.

Menggunakan algoritma lain dan memodifikasinya dengan algoritma tertentu

REFERENSI

[1] Ivan Nugraha. 2009. Studi dan perbandingan performasi algoritma simetri vigenere chipper binner dan hill chipper binner.

[2] Pramono. A dan Sujjada. A. (2009). Implementasi algoritma hill chiper sebagai media steganografi menggunakan metode LSB.

[3] Prasetyo, B. 2013. Kombinasi Steganpgrafi Bit Matching dan Kriptografi Des Untuk Pengamanan Data. Semarang: Universitas Diponegoro, Semarang

[4] Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. Yogyakarta: Penerbit Andi

[5] Schneier, Bruce. (1996). *Applied Cryptography* (2nd ed). New York : John Wiley & Son.

Menezes, Alfred, Paul C. Van Oorschot, Scott A. Vanstone. (1997). *Handbook of Applied Cryptography*. CRC Press

[7] Cox, I., Miller, M., Bloom, J., & Fridrich, J. &. (2008). *Digital Watermarking and STeganography 2nd Ed. Morgan Kaufmann*., MA.

[8] Kipper, G. (n.d). (2004). *Investigator's Guide to Steganography*, Florida: CRC Press LLC

[9] Ria, Gemita. (2010). Studi Perbandingan Steganografi pada Audio, Video dan Gambar. Bandung : Institut Teknologi Bandung

[10] Krenn, J. Robert. (2004). *Steganography and Steganalysis*. Diakses 1 Juli 2018, dari http://www.krenn.nl