INTECHNO Journal
INFORMATION TECHNOLOGY JOURNAL
Volume 1 No. 1 November 2018
e-ISSN: 2655-1438
p-ISSN: 2655-1632

HYBRID KRIPTOGRAFI - STEGANOGRAFI MENGGUNAKAN VERNAM CIPHER, VIGENERE CIPHER DAN LSB PADA PENGIRIMAN PESAN RAHASIA

Muh. Hutomo Perdana Putra[1)], Rizqi Sukma Kharisma, M.Kom[2)]

[1)] *Informatika Universitas AMIKOM Yogyakarta*
[1)]*Informatika Universitas AMIKOM Yogyakarta*
Email : hutomo8433@students.amikom.ac.id[1)],sukma@amikom.ac.id[2)]

Abstract

The development of science is very influential on the progress of the world of technologi. One of the emerging technologies is technology of information where the simplicity of finding the information quickly without concern on the limitation of the space and period, so that, in only a minute we are able to know the country's information. It would be a disadvantage if any information that is considered as a confidential information can be known by any parties, therefore to keep it save, a cryptographic and steganographic encryption technique is required. Cryptography, science and art to maintain the security of messages when messages are sent from one place to another that relies on mathematical techniques for dealing with information security. Steganography is the process of storing secret messages in the form of text in other forms so it is not easily known by others. Various kinds of steganography include hiding messages into image files, audio files, and video files.

The Vigenere and Vernam algorithms are the chosen algorithm to design an application that allows for cryptographic to encrypt the messages and the LSB algorithm is the chosen algorithm to insert the results of Crypto encryption messages into image files.

Keywords *– Cryptography, Steganography, Vigenere, Vernam, LSB, Web.*

Pendahuluan

Perkembangan ilmu pengetahuan sangat berpengaruh pada perkembangan dunia teknologi. Salah satu teknologi yang sedang berkembang adalah teknologi informasi yang dimana dengan kemudahan untuk mencari suatu informasi dengan cepat tanpa harus memperhatikan batasan ruang dan waktu sehingga dalam hitungan menit, kita dapat mengetahui informasi suatu negara. [2]

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi. [1]

Steganografi adalah proses menyimpan pesan rahasia berupa teks dalam bentuk lain sehingga tidak mudah diketahui oleh orang lain. Berbagai macam steganografi antara lain menyembunyikan pesan ke dalam file gambar, file audio, dan file video. [4]

Berdasarkan pada analisa diatas, maka penulis akan membahas mengenai bagaimana cara mengamankan suatu pesan dengan menggunakan algoritma Vernam Cipher, Vigenere Cipher pada Kriptografi dan algoritma LSB (Least Significant Bit) pada Steganografi.

Berdasarkan latar belakang yang peneliti tulis, ditentukan beberapa rumusan masalah, yaitu : Bagaimana menggabungkan (hybrid) teknik Kriptografi dan teknik Steganografi pada sebuah pesan rahasia?

Batasan masalah yang diterapkan pada aplikasi enkripsi pesan ini adalah sebagai berikut:

Algoritma yang di terapkan pada teknik Kriptografi adalah Vernam Cipher dan Vigenere Cipher, sedangkan teknik Steganografi adalah LSB (Least Significant Bit).

Aplikasi yang akan dibangun berbasis website. Menggunakan file gambar sebagai output pesan. Aplikasi menggunakan bahasa pemrograman PHP.

Adapun tujuan yang ingin dicapai dari penelitian ini adalah : Merancang sebuah aplikasi enkripsi dengan gabungan kriptografi dan steganografi. Membuat pesan pengirim menjadi aman terenkripsi. Mencoba untuk kobinasikan dua Teknik kemanan Kriptografi dan Steganografi.

Metode Penelitian yang digunakan pada penelitian ini adalah :

1. Studi Literatur

   Sebelum memulai penelitian ini terlebih dahulu peneliti akan mencoba untuk mempelajari literatur melalui buku, jurnal, artikel, makalah maupun situs internet yang membahas tentang kriptografi dan steganografi.

2. Analisis dan Perancangan Sistem

   Pada tahap ini penulis akan melakukan

analisis SWOT terhadap aplikasi sesuai dengan batasan masalah dan tujuan yang akan dicapai dari pengujian aplikasi kriptografi dan steganografi, setelah itu dilakukan perancangan flowchart serta interface dan perancangan sistem.

3. Implementasi Sistem

Pada tahap ini akan dilaksanakan pengkodean (coding) dengan merancang interface website terlebih dahulu menggunakan HTML dan CSS dan proses sistem dengan Java Script dan PHP pada aplikasi untuk meng-enkripsi pesan.

4. Pengujian Sistem

Pada tahap pengujian sistem, peneliti akan mencoba aplikasi yang telah dibangun apakah sudah sesuai dengan algoritma yang diterapkan yaitu penggabungan kriptografi dan steganografi pada pesan.

5. Penyusunan Laporan

Dalam tahap ini dilakukan penyusunan laporan hasil dari analisis dan perancangan aplikasi dalam format penulisan penelitian.

Tinjauan Pustaka

Kriptografi berasal dari Bahasa Yunani, menurut Bahasa dibagi menjadi dua yaitu, kripto dan graphia, kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain.

Dalam perkembangannya kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dan tangan digital dan keaslian pesan dengan sidik jari digital. [1]

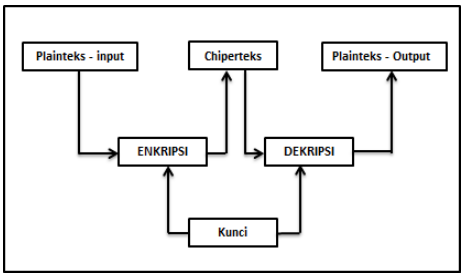
Menguraikan hasil analisis kualitatif dan/atau kuantitatif dengan penekanan pada jawaban atas permasalahan.

Isi dari pembahasan ini memuat segala sesuatu tentang kegiatan yang dilakukan dalam makalah. Mulai dari konsep, perancangan, hipotesis (bila ada), percobaan, data pengamatan, hasil dari data pengamatan yang ada.

Isi didukung dengan gambar dan tabel yang dirujuk dalam naskah. Jenis – jenis Algoritma Kriptografi

1. Algoritma Simetris

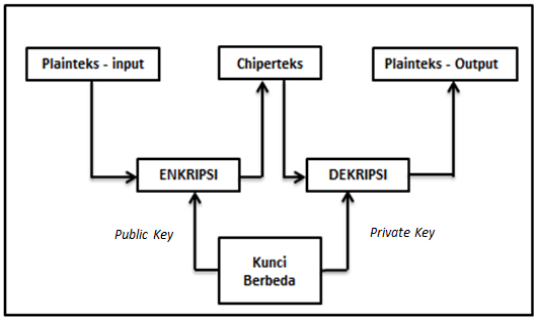
Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya, contoh : Alice ingin mengirimkan pesan x dengan aman menggunakan saluran umum kepada Bob. Alice menggunakan kunci x yang sebelumnya telah disepakati oleh Alice dan Bob. Untuk mengirim pesan e x (x) kepada Bob, dia akan mendeskripsikan teks-kode yang diterima dengan kunci yang sama dengan yang digunakan untuk memperoleh akses ke pesan yang diterima Begitu juga sebaliknya.



Gambar 1 Skema Algoritma Simetris

2. Algoritma Asimetris

Algoritma asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satunya lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya satu orang saja yang memiliki kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirmkan



Gambar 2 Skema Algoritma Asimetris

3. Vigenere Cipher

Vigenere chiper merupakan salah satu algoritma klasik dengan teknik subtitusi. Nama vigenere diambil dari seorang yang bernama Blaise de Vigenere, Vigenere Chiper mungkin adalah contoh terbaik dari chiper alphabet- majemuk manual,

Rumus Enkripsi Vigenere :
$Ci=(Pi + Ki) \bmod 26$
Rumus Dekripsi Vigenere :
$Pi=(Ci + Ki) \bmod 26$

Dimana :
Ci = Nilai desimal karakter chiperteks ke-1
Pi = Nilai desimal karakter plainteks ke-1
Ki = Nilai Desimal karakter kunci ke-1

4. Vernam Cipher

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma ini merupakan algoritma berjenis symmetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit

key. Algoritma Vernam cipher diadopsi dari one-time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, Vernam Cipher merupakan versi lain dari one-time pad cipher. [3]

Dalam proses enkripsi,cipherteks diperoleh hamper sama dengan metode vigenere tapi mempunyai perbedaan dibagian proses key.

5. Steganografi

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi "rahasia" di dalam suatu informasi lainnya. Steganografi mempunyai sejarah yang hamper sama dengan kriptografi, keduanya banyak digunakan terutama pada zaman perang. Steganografi dapar dipelajari lebih jauh dalam.

Beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik Steganography antara lain adalah :

a. Teks

Dalam algoritma Steganography yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik NLP sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.

b. Audio

Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.

c. Citra

Format pun paling sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma Steganography untuk media penampung yang berupa citra.

d. Video

Format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

LSB (*Last Significaant Bit*)

Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Hingga saat ini sudah banyak dikemukakan oleh para ilmuwan metode-metode penyembunyian data. Metode yang paling sederhana adalah metode modifikasi LSB (Least Significant Bit Modification). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai ilustrasi, di bawah ini dijelaskan metode modifikasi LSB untuk menyisipkan watermark pada citra (gambar) digital.

Misalnya pada byte 11010010, bit 1 yang pertama (digarisbawahi) adalah bit MSB dan bit 0 yang terakhir (digarisbawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab penggantian hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut di dalam gambar menyatakan warna tertentu, maka perubahan satu bit LSB tidak mengubah warna tersebut secara berarti. Lagi pula, dan ini keuntungan yang dimanfaatkan, mata manusia tidak dapat membedakan perubahan yang kecil. Misalkan segmen pixel-pixel citra sebelum penambahan bit-bit watermark adalah

0011001110100010 11100010
01101111

Misalkan data rahasia (yang telah dikonversi ke sistem biner) adalah 0111. Setiap bit dari watermark menggantikan posisi LSB dari segmen data citra menjadi:

0011001010100011 11100011
01101111

Hasil dan Pembahasan

Telah dilakukan Analisis SWOT sebagai berikut :

1. Kekuatan (Strenghts)

Kekuatan adalah sumber daya, keterampilan, atau keungulan-keungulan lain yang berhubungan dengan para pesaing perusahaan dan kebutuhan pasar yang dapat dilayani oleh perusahaan yang diharapkan dapat dilayani. [5]

2. Kelemahan (Weakness)

Kelemahan adalah keterbatasan atau kekurangan dalam sumber daya, keterampilan, dan kapabilitas yang secara efektif menghambat kinerja perusahaan. Keterbatasan tersebut dapat berupa fasilitas, sumber daya keuangan, kemampuan manajemen dan keterampilan pemasaran dapat meruoakan sumber dari kelemahan perusahaan.

3. Peluang (Opportunities)

Peluang adalah situasi penting yang mengguntungkan dalam lingkungan perusahaan. Kecendrungan-kecendrungan penting merupakan salah satu sumber peluang, seperti perubahaan teknologi dan meningkatnya hubungan antara perusahaan dengan pembeli atau pemasokk merupakan gambaran peluang bagi perusahaan.

4. Ancaman (Threats)

Ancaman adalah situasi penting yang tidak menguntungan dalam lingkungan perusahaan. Ancaman merupakan pengganggu utama bagi posisi sekarang atau yang diinginkan perusahaan. Adanya peraturan-peraturan pemerintah yang baru atau yang

direvisi dapat merupakan ancaman bagi perusahaan.

Kebutuhan Fungsional yang diperlukan pada sistem ini adalah :

1. Pengguna dapat menentukan public kunci dengan bebas asalkan kedua pihak mengetahuinya.
2. Pengguna dapat menggunakan gambar apa aja sebagai media penyembunyian pesan.
3. Pengguna dapat melakukan dekripsi pesan yang telah dienkripsi sebelumnya pada aplikasi.

Sedangkan Kebutuhan Non-Fungsional yang diperlukan adalah:

1. Kebutuhan *Hardware*

Tabel 1 Kebutuhan *Hardware*

Hardware	**Spesifikasi**
CPU (*Central Processing Unit*)	Intel Core I5 @1.60GHz ~2.3GHz
RAM (*Random Access Memory*)	4GB RAM
Harddisk	Seagate 1TB

2. Kebutuhan *Software*

Tabel 2 Kebutuhan *Software*

Software	**Spesifikasi**
Operating system	Windows 10 Pro 64 bit
Text Editor	Sublime Text 3
Web Server	XAMPP V3.2.2
Brwoser	Google Chrome
Bahasa Program	HTML, CSS 3,PHP

Interfaces atau antarmuka yang diperlukan pada sistem ini adalah:

1. Halaman *Home*

Halaman utama (home) merupakan halaman yang pertama kali akan dilihat oleh pengunjung saat pengunjung mengakses website ini.

Gambar 3 Halaman Home

2. Halaman Enkripsi

Pada Enkripsi User memasukkan pesan rahasia, key, dan gambar apapun diform tersebut, gambar boleh berformat jpg atau png. Setelah itu klik button Encode dan akan menghasilkan gambar dengan pesan didalamnya.

Gambar 4 Halaman Enkripsi

3. Halaman Dekripsi

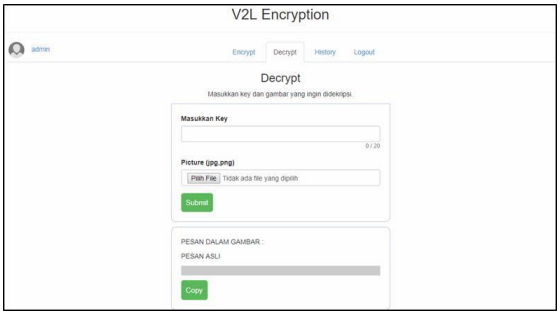
Halaman dekripsi pesan dibuat untuk menerjemahkan pesan yang telah dienkripsi sebelumnya agar dapat dimengerti isi dari pesan yang telah dikirmkan oleh pengirim sebelumnya

Gambar 5 Halaman Dekripsi

Telah dilakukan pengujian system dengan beberapa katagori :

1. Pengujian Waktu Penyisipan Pesan

Pengujian ini bertujuan untuk mengetahui berapa lama proses penginputan kedalam file gambar berformat jpg dan png.



Tabel 3 Pengujian Waktu Eksekusi p dan q Enkripsi

p	**q**	**Ukuran file**	**waktu**
49	11	244kb	0,69 detik
138	9	523kb	0,95 detik
151	7	76kb	0,08 detik

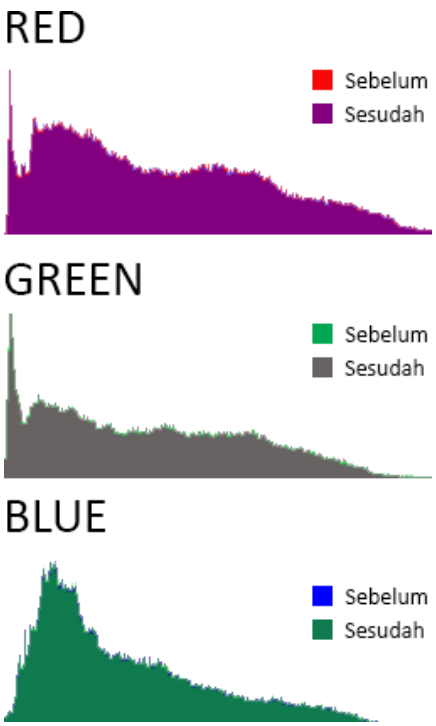
Tabel 4 Pengujian Waktu Eksekusi Dekripsi

p	**q**	**Ukuran file**	**waktu**
49	11	244kb	0,04 detik
138	9	523kb	0,05 detik
151	7	76kb	0,02 detik

Analisis Perbedaan Gambar dengan Histogram dilakukan bertujuan untuk melihat perbedaan histogram entitas warna sebelum dan sesudah penyisipan pesan, terlihat perbedaan grafik yang sedikit antara sebelum dan sesudah, ini membuktikan bahwa gambar tak dapat diketahui apakah sudah disisipi pesan atau tidak karena hanya mempunyai sedikit perubahan pada histogram

e-ISSN: 2655-1438
p-ISSN: 2655-1632

warnanya.



Gambar 6 Histogram warna RGB sebelum dan sesudah disisipkan pesan

Kesimpulan dan Saran

Dari hasil pembahasan sebelumnya maka dapat disimpulkan bahwa :

1. Aplikasi web V2L berhasil menggabungkan dan mengimplementasikan antara Teknik Kriptografi dan Teknik Steganografi.
2. Aplikasi web V2L berhasil mengamankan pesan dengan gabungan Teknik. Hal ini dibuktikan penyisipan yang sudah disisipkan ke gambar dan dapat diambil kembali dari gambar tersebut.
3. Proses penyisipan pesan ke dalam gambar hanya dengan file gambar berupa format *jpg, *jpeg, *png.
4. Hasil gambar masukan dan keluaran dimana gambar sebelum di enkripsi dan sesudah di enkripsi tidak mempunyai perbedaan dari segi warna maupun ukuran px gambar, sehingga orang lain tidak akan tahu bahwa ada pesan di dalam gambar tersebut.
5. File gambar masukan dan hasil keluaran memiliki jumlah ukuran file yang berbeda, dikarenakan file format apapun yang dimasukkan akan dikonversi menjadi format *png.

Pada penulisan skripsi ini tentu masih banyak kekurangan yang mungkin dapat disempurnakan lagi oleh pengembang berikutnya, sehingga terdapat beberapa saran yang bisa menjadi pertimbangan agar website V2L nantinya menjadi lebih baik lagi, diantaranya :

1. Website V2L dapat ditambahkan algoritma-algoritma simetri lainnya sebagai proses enkripsi pesannya.
2. Tampilan Website yang mungkin dapat dibuat lebih menarik.
3. V2L hanya bisa meng-enkripsi pesan berupa huruf saja, sehingga kedepannya bisa ditambahkan berupa angka dan simbol-simbol.
4. Key yang tidak ditentukan lagi antara pengirim dan penerima, melainkan key yang dimasukkan akan di enkripsi juga sehingga penerima jika ingin dekripsi pesan tidak memasukkan key lagi.

Daftar Pustaka

[1] D. Ariyus, Kriptografi Keamanan Data dan Komunikasi, Yogyakarta: Graha Ilmu, 2006.
[2] D. Ariyus, Pengantar Ilmu KRIPTOGRAFI Teori, Analisis, dan Implementasi, Yogyakarta: Andi, 2008.
[3] W. H. Encyclopedia, Gilbert Vernam, Virginia: World Heritage Encyclopedia, 2004.
[4] E. Zam, Anti Privacy : Melacak, Membajak & Membobol Data Rahasia, Jakarta Selatan: Mediakita, 2013.
[5] F. Rangkuti, Analisis SWOT Teknik Membedah Kasus Bisnis, Jakarta: PT. Gramedia Pustaka Utama, 2006.