JURNAL ILMIAH FLASH
Vol. 5 No. 1, Halaman: 05 - 09
Juni 2019

APLIKASI KRIPTOGRAFI ALGORITMA RIVEST-SHAMIR-ADLEMAN DAN RIVEST CODE 4 PADA STEGANOGRAFI CITRA METODE LEAST SIGNIFICANT BIT

Reza Naftali Pahlawan[1], Rocky Y. Dillak[2], Jemsrado Sine[3]
PoliteknikNegeriKupang
Jl. Adisucipto – Penfui Kupang NTT
E-mail: rezapahlawan152@gmail.com

Abstrak

Aplikasi Kriptografi Algoritma Rivest-Shamir-Adleman Dan Rivest Code 4 Pada Steganografi Citra Metode Least Significant Bit Merupakan salah satu aplikasi yang digunakan untuk mengamankan pesan dari sumber kepada tujuan. Aplikasi ini meningkatkan tingkat kerahasian data agar tetap terjaga keamanannya dari pihak lain yang tidak diinginkan. Aplikasi ini menggunakan algoritma kriptografi Rivest-Shamir-Adleman yang di padukan dengan Algoritma Kriptografi Rivest Code 4 serta Steganografi Citra Metode Least Significant Bit

Kata kunci: Aplikasi, Kriptografi, Steganografi.

PENDAHULUAN

Perkembangan media perentara komunikasi kini semakin beragam. Dalam perkembanganya, informasi yang dikirim melalui berbagai media komuniasi menjadi hal yang sangat penting. Beragam aplikasi pengirim pesan teks seperti social media menjadi layanan yang sering digunakan untuk saling bertukar informasi. Walaupun terlihat praktis namun keamanan pesan yang dikirim melalui layanan tersebat masih belum begitu aman, dan masih dapat dicuri pesannya dari pihak lain yang tidak berwenang, terlebih lagi jika informasi yang dikirmkan merupakan informasi yang sangat rahasia dan hanya boleh diketahui oleh pihak tertentu, seperti password, nomor pin, atau rahasia perusahaan yang tidak boleh diketahui pihak ketiga. Oleh karena itu dibutuhkan suatu metode untuk meningkatkan kerahasian, keamanan dan keaslian informasi tersebut. Untuk itu dalam meningkatkan keamanan sebuah pesan dapat menggunakan Teknik kriptografi dan steganografi.

Kriptografi sendiri adalah seni atau ilmu untuk mengamankan isi pesan yang disandikan atau dienkripsi sedemikian rupa sehingga tidak diketahui apa isi pesan tersebut. Algoritma simetris dan asimetris merupakan dua algoritma yang digunakan dalam proses pengamanan data. Algoritma simetris merupakan algoritma yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi, sedangkan algoritma asimetris menggunkan dua kunci berbeda dalam proses enkrpsi dan dekripsi pesan. Sedangakan, Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (**R**ivest—**S**hamir—**A**dleman). Termasuk algrotma asimetri karena mempunyai dua kunci, yaitu kunci publik dan kunci privat. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Sedangkan, RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi. Algoritma kriptografi *Rivest Code* 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc *(RSADSI)* yang berbentuk *stream chipper*. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest, Shamir, dan Adleman).

Sedangkan, Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Sedangkan, metode LSB (least significant bit) adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu mengubah bit redundan *cover image* yang tidak berpengaruh signifikan dengan bit dari pesan rahasia

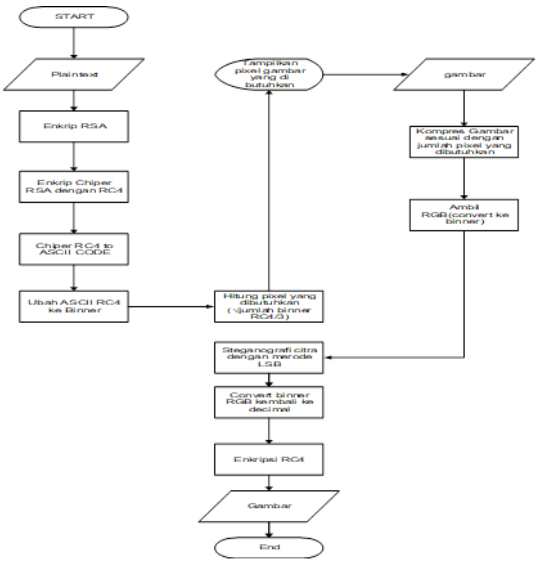
Berdasarkan uraian yang telah disampaikan maka penulis tertarik untuk

membuat program yang dapat melakukan kryptografi dan steganografi secara bersamaan berbasis web serta akan dijadikan oleh penulis sebagai suatu topik dalam penulisan tugas akhir dengan judul "Aplikasi Kriptogtafi Dengan Algoritma Rivest–Shamir–Adleman Dan Rivest Code 4 Serta Steganografi Citra Dengan Metode Least Significant Bit".

METODE PENELITIAN

Aplikasi Kirptografi Algoritma Rivest-Shamir-Adlmeman Dan Rivest Code 4 Pada Steganografi Citra Metode Least Significant Bit di kerjakan pada Politeknik Negeri Kupang. Bahan yang digunakan adalah sebuah laptop dengan spesifikasi : intel core i3, 4gb Ram ddr4. Harddisk 1 TB.

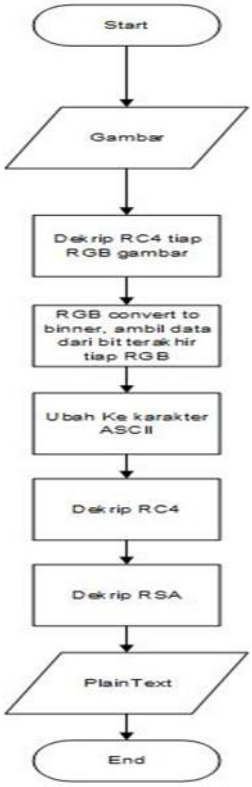
A. Flowchart Enkripsi
Flowchart ini menggambarkan tentang bagaimana Aplikasi melakukan proses enkripsi terhadap sebuah pesan.



Gambar 1. Flowchart Enkripsi

Pada Gambar 1 Pengguna melakukan proses enkripsi yang diawali saat pengguna melakukan inputan berpa plainteks, setelah itu plainteks akan di enkripsi dengan algoritma Berlapis yaitu Algoritma Rivest-Shamir-Adleman dan Rivest Code 4 setelah itu sistem akan menghitum jumlah pixel minimum dari citra gambar agar diinputkan oleh pengguna selanjutnya. Selanjutnya maka pengguna akan menginput file citra sesuai dengan ketentuan pixel sebelumnya, setalah pengguna melakukan inputan maka system akan melakukan proses steganografi dengan metode Least Significant Bit pada file citra tersebut dengan menyisipkan plainteks yang telah dienkripsi berlapis sebelumnya.Setelah proses steganografi selesai maka file citra yang telah disteganografi tersebut akan di enkripsi kembali menggunakan algorima Rivest Code 4 sehigga menghasilkan sebuah output yaitu file citra yang telah dienkripsi tersebut.

B. Flowchart Dekripsi
Flowchart ini menggambarkan tentang bagaimana Aplikasi melakukan proses dekripsi untuk mengambil sebuah pesan.



Gambar 2. Flowchart Dekripsi

Pada Gambar 2 Penguuna Melakukan proses dekripsi yang diawali saat pengguna memasukan sebuah file citra kemudian sistem akan melakukan proses Dekripsi pada gambar tersebut dengan menggunakan Algoritma Rivest Code 4 setelah itu sistem akan mengambil pesan yang telah disteganografikan dan melakukan dekripsi berlapis kepada pesan tersebut dengan menggunakan algoritma Rivest Code 4 dan Rivest-Shamir-Adleman. Selah itu sistem akan menghasilkan sebuah output yaitu sebuah plainteks.

HASIL DAN PEMBAHASAN

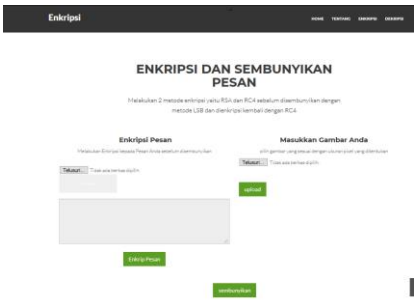
A. Tampilan Aplikasi

Gambar 3. Halaman Home

Pada menu tampilan halaman ini hanya terdapat tampilan berupa website statis yang penuli gunakan agar aplikai ini lebih menarik

Gambar 4. Halaman Tentang

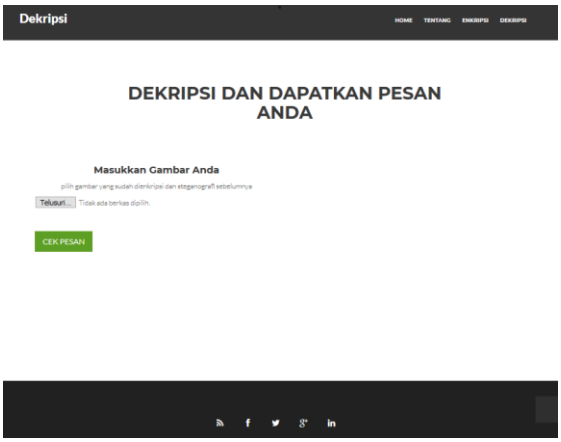
Pada menu tampilan halaman ini hanya terdapat tampilan berupa website statis yang penuli gunakan agar aplikai ini lebih menarik



Gambar 5. Halaman Enkripsi

Halaman Enkripsi adalah halaman yang melakukan enkripsi dan steganografi dimana halaman ini 4 buah button ,1 text area dan 2 input type file. Dimana komponen tersebut berfungsi untuk :

1. Input Type File Telusuri digunakan untuk mengambil file doc
2. Button Upload di bawah Telusuri digunakan untuk megupload File Docx yang dipilh Sebelumnya
3. Text area digunakan untuk menampilkan pesan yang diambil dari file docx
4. Input type file untuk melakukan inputan berupa file citra
5. Button Enkripsi Pesan berfungsi untuk melakukan enkripsi RSA dan RC4 pada pesan,
6. Button Upload berfungsi untuk mengupload gambar ke dalam sistem aplikasi ini
7. Button Sembunyikan berfungsi untuk menyembunyikan pesan ke dalam gambar dan mengenkripsi gambar dengan algoritma RC4 setelahnya



Gambar 6. Halaman Dekripsi

Halaman Dekripsi adalah halaman yang melakukan Dekripsi dan pengambilan pesan dari gambar yang telah diupload pengguna dimana halaman ini memiliki berapa komponen utama yaitu 1 buah button ,1 text area dan 1 input type file. Dimana komponen tersebut berfungsi untuk :

1. Text area digunakan untuk menampilkan pesan yang telah berhasil diambil dari gambar dan didekripsi oleh aplikasi ini
2. Input type file untuk melakukan inputan berupa file citra
3. Button Cek Pesan Berfungsi untuk mengupload gambar dan melakukan proses dekripsi dan pengambilan pesan dari gambar yang diupload.

B. Input

Adapun Beberapa Inputan yang diperlukan adalah sebagai berikut :

1. File txt yang digunakan untuk menginput pesan
2. Citra gambar dengan tipe jpg ,png, jpeg yang digunakan untuk proses steganografi

C. Output

File Output yang dikeluarkan bertipe .doc yang akan menyimpan plainteks yang dimasukkan oleh sumber .

D. Pengujian

Tabel 1. Pengujian

No	Jumlah Karakter	Ukuran Pixel Gambar Yang Dibutuhkan	Besaran Gambar	Waktu Enkripsi (/detik)	Waktu Dekripsi (/ detik)
1	1.000	116*116	400*400 (12,6Kb)	0.103540	0.093851
2	2.000	164*116	400*400 (12,6Kb)	0.1864280	0.162804
3	3.000	200*200	400*400 (12,6Kb)	0.28751611	0.300282
4	4.000	231*231	400*400 (12,6Kb)	0.40236496	0.359488
5	5.000	259*259	400*400 (12,6Kb)	0.44199776	0.439706
6	6.000	283*283	400*400 (12,6Kb)	0.54461002	0.533524
7	7.000	306*306	400*400 (12,6Kb)	0.65423583	0.584797
8	10.000	366*366	400*400 (12,6Kb)	0.96410298	0.914968
9	40.000	731*731	3840*2160 (626Kb)	3.58524703	3.250519
10	60.000	895*895	3840*2160 (626Kb)	5.81995511	5.006398

PENUTUP

A. Kesimpulan

Berdasarkan analisis dam perancangan dari aplikasi kriptografi algoritma Rivest-Shamir-Adleman dan Rivest Code 4 Pada Steganografi Citra Metode Least Significant Bit, maka dapat disimpulkan benerapa hal sebagai berikut :

1. Aplikasi ini memiliki tingkat keamanan yang cukup tinggi karena menggunakan algoritma kriptografi berlapis
2. Aplikasi ini dapat digunakan dengan baik sebagai salah satu alternatif pengaman data degan pengaman yang lebih tinggi dan akurat

B. Saran

Aplikasi ini masih dapat dikembangkan dengan menambahkan beberapa hal yang membantu pengguna dalam mengamankan data :

1. Aplikasi ini kiranya nanti dapat dimanfaatkan dalam pengaman data pada database sebuah sistem informasi
2. Aplikasi ini kirinya dapat dikembangkan sehingga menambah kualitas pengamanan data yang lebih akurat dan tepat
3. Aplikasi ini kiranya dapat dikembangkan agar dapat menerima inputan selain berupa file txt dan file citra gambar selain jpg, jpeg ,png , dan gif
4. Aplikasi ini kiranya dapat dikembangkan dengan melakukan enkripsi langsung pada header file sehingga tidak memakan waktu yang lama

UCAPAN TERIMAKASIH

Penelitian ini dapat dilaksanakan karena bantuan Pembimbang Penulis yaitu Bapak Rocky Y. Dillak, ST., M.Sc Selaku Pembimbing I Penulis Serta Bapak Jemsrado Sine, ST., M.Eng Selaku Ketua Jurusan Teknik Elektro Dan Pembimbing II Penulis.

DAFTAR PUSTAKA

[1]. Ali Ridho Barakbah, Tita Karlita, A. S. A. (2013) Logika dan algoritma.
[2]. Arifin, R., & Oktoviana, L. T. (2013). Implementasi Kriptografi Dan Steganografi Menggunakan Algoritma RSA Dan Metode LSB. Jurnal Dinamika Informatika, 2(Mei), 1–7.
[3]. Ariyus, Dony. (2006). Kriptografi Keamanan Data dan Komunikasi.Yogyakarta: Graha Ilmu,.
[4]. Email, D., Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk, 3(2), 253–258.
[5]. Kromodimoeljo, S. (2009). Teori & Aplikasi Kriptografi. SPK IT Consulting.
[6]. Munir, R. (2004). Diktat Kuliah : IF5054 Kriptografi Steganografi Dan Watermarking.
[7]. Suryani, K. N. (2009). Algoritma Rc4 Sebagai Metode Enkripsi.

[8]. Zebua, T., & Ndruru, E. (2017). PENGAMANAN CITRA DIGITAL BERDASARKAN MODIFIKASI ALGORITMA RC4, 4(4), 275–282. https://doi.org/10.25126/jtiik.201744474