ISSN : 2503-054X
Vol 4 No: 1, April 2019

PENYISIPAN PESAN RAHASIA PADA CITRA GAMBAR DENGAN TEKNIK STEGANOGRAFI DAN ALGORITMA ASIMETRIS ENKRIPSI RIVEST SHAMIR ADLEMAN (RSA)

Dendi Prana Yudha
DPY@stmik-kharisma.ac.id
Program Studi Informatika STMIK Kharisma
Karawang, Indonesia

Kiki Ahmad Baihaqi
kikiahmad@ubpkarawang.ac.id
Program Studi Teknik Informatika
Universitas Buana Perjuangan
Karawang, Indonesia

Billy Ibrahim Hasbi
billy.ibrahimhasbi@gmail.com
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang,
Indonesia

ABSTRAK
Steganografi adalah seni menyembunyikan informasi dan upaya untuk menyembunyikan keberadaan informasi yang disematkan. Steganografi berfungsi sebagai sebuah cara yang lebih baik untuk mengamankan pesan dari pada kriptografi, steganografi menyembunyikan isi pesan bukan mengacak pesan. Pesan asli disembunyikan di dalam citra gambar sedemikian rupa sehingga perubahan yang terjadi pada gambar tidak dapat diketahui perbedaannya dengan gambar tanpa pesan. Pada penelitian ini dikombinasikan algoritma RSA yang digunakan untuk mengenkripsi pesan rahasia dan teknik LSB digunakan untuk menyembunyikan pesan terenkripsi dengan tujuan untuk menghasilkan stego file yang lebih aman dan lebih baik secara kualitas. Berdasarkan hasil implementasi dan pengujian citra gambar yang dihasilkan sistem memiliki nilai diatas 40 dB sehingga kualitas citra gambar stego file memiliki kualitas yang baik.

Kata kunci : Embedding Sistem, Steganografi, Kriptografi, RSA

1. PENDAHULUAN

Kriptografi dan Steganografi sudah dikenal luas sebagai suatu teknik yang digunakan untuk memanipulasi informasi atau pesan untuk diacak atau disembunyikan keberadaannya. Kriptografi adalah seni dan ilmu untuk menyimpan pesan secara aman. Steganografi adalah seni mentransmisikan data dengan cara disembunyikan agar keberadaan pesan tidak diketahui. Kata Steganografi merupakan kombinasi dari dua kata Yunani Kuno steganos berarti tertutup atau tersembunyi dan graphein berarti penulisan. Kriptografi adalah suatu teknik untuk mengacak pesan sehingga tidak mudah terbaca oleh orang yang tidak berhak sedangkan steganografi menyembunyikan pesan sehingga pesan tidak terlihat atau tertutup sehingga tidak diketahui keberadaannya. Kedua metode tersebut memberikan keamanan pada pesan yang ingin disampaikan. Penelitian ini bertujuan untuk mengkombinasikan kedua metode tersebut yaitu kriptografi dan Steganografi ke dalam satu sistem agar sebuah pesan dapat terjaga kerahasiaannya.

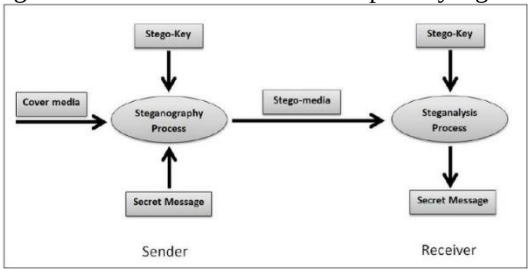
Selalu menjadi praktik yang baik untuk menggunakan Kriptografi dan Steganografi secara bersamaan untuk menambahkan beberapa lapisan keamanan. Dengan menggabungkan, enkripsi data bisa dilakukan dengan perangkat lunak kemudian menanamkan teks sandi dalam suara atau media lainnya dengan bantuan kunci steganografi. Kombinasi kedua metode akan meningkatkan keamanan data yang disematkan untuk pertukaran data yang tidak aman melalui saluran terbuka seperti internet.

Dari uraian di atas akan dilakukan pengacakan pesan rahasia yang disematkan pada citra gambar sebelum dikirimkan melalui transmisi data yang tidak aman seperti email, internet maupun media sosial.

2. METODE PENELITIAN

2.1 Steganografi

Steganografi secara teknis berarti pesan yang ditutupi atau pesan yang tersembunyi. Tujuan utama dari steganografi adalah untuk menutupi pesan pada media lain sehingga tidak memungkinkan pihak ketiga untuk mendeteksi keberadaan pesan yang dimaksud.

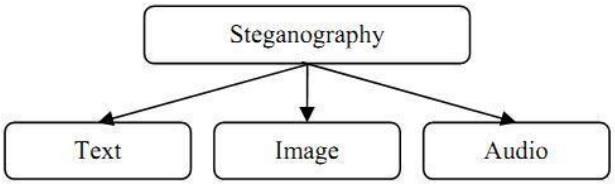


Gambar 1 Skema Steganografi

ISSN : 2503-054X
Vol 4 No: 1, April 2019

2.2. Media Steganografi

Tipe media yang digunakan untuk steganografi terbagi menjadi tiga kategori, teks, citra dan suara [1]



Gambar 2 Media Steganografi

Pada penelitian ini media steganografi yang digunakan adalah citra gambar. Menyembunyikan informasi dalam gambar merupakan teknik yang populer saat ini. Sebuah gambar dengan pesan rahasia di dalamnya dengan mudah dapat menyebar melalui World Wide Web atau di *newsgroup*. Untuk menyembunyikan pesan dalam gambar tanpa mengubah sifat yang terlihat, media penutup dapat diubah di dalam wilayah noisy dengan variasi warna yang lebih banyak, sehingga lebih sedikit perhatian pada daerah modifikasi tersebut. Metode yang paling umum digunakan pada media gambar adalah dengan Least Significant Bits atau LSB, masking, filtering serta transformasi pada gambar [2]. Teknik ini memiliki ingkat keberhasilan yang berbeda pada berbagai jenis berkas gambar. Metode penyisipan LSB bekerja dengan cara menyisipkan pesan dengan mengganti bit ke 8, 16 dan 24 pada representasi biner sebuah citra gambar. Berikut adalah contoh cara kerja LSB [3] representasi biner sebuah citra gambar sebagai berikut :

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111

Representasi biner huruf A adalah 01100101 apabila citra tersebut disisipkan pesan dengan huruf A maka dihasilkan :

00100110 11101001 11001001
00100110 11001000 11101000
11001000 00100111

Pada binary digit diatas pada bit ke-8, 16 dan 24 diganti dengan biner huruf A, dan hanya tiga bit rendah yang berubah (cetak tebal), sehingga menghasilkan gambar yang secara kasat mata sulit dibedakan antara citra gambar asli dengan citra gambar yang sudah disisipi pesan.

2.3. Terminologi dalam Kriptografi

Beberapa terminologi dalam kriptografi antara lain [4]:

A. Plainteks dan cipherteks

Pesan adalah suatu informasi atau data yang dapat dibaca dan dimengerti maknanya. Dalam kriptografi,pesan dapat disebut dengan plainteks (plaintext). Dalam kriptografi Pesan harus disandikan ke bentuk lain agar pesan tersebut tidak dapat mudah terbaca dan tidak mudah diketahui maknanya. Bentuk pesan yang sudah berubah bentuk disebut cipherteks. Cipherteks harus dapat ditransformasi kembali menjadi plainteks agar dapat terbaca dan diketahui maknanya.

B. Pengirim dan penerima

Pertukaran pesan atau data pada kriptografi melibatkan dua entitas. Entitas tersebut adalah pengirim dan penerima. Entitas bukan saja hanya manusia melainkan dapat berupa mesin maupun hal lainnya.

C. Enkripsi dan dekripsi

Enkripsi merupakan proses untuk merubah pesan rahasia yang dapat dengan mudah terbaca menjadi tidak mudah terbaca dengan cara mengacaknya melalui penyandian,

D. Kunci

Kunci (key) adalah parameter yang digunakan untuk proses enkripsi ataupun sebaliknya proses dekripsi. Kunci biasanya berupa string atau deretan bilangan. Pada penelitian ini kunci akan di *generate* secara otomatis oleh sistem, kunci yang digunakan adalah kunci privat dan kunci publik.

2.4. Algoritma RSA (Rivest, Shamir, Adleman)

RSA adalah sebuah algoritma enkripsi yang diambil berdasarkan singkatan nama depan 3 orang penemunya yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. Algoritma ini adalah algoritma enkripsi asimetris yang paling popular diantara algoritma lainnya [5]. Tingkat keamanan sangat tinggi karena tingkat kesulitan memfaktorkan bilangan bulat komposit yang besar [6]. Selama pemfaktoran bilangan komposit yang besar menjadi faktor-faktor prima belum ditemukan celahnya, maka keamanan algoritma kriptografi RSA ini tetap terjamin keamanannya dan akan sulit untuk dipecahkan.

ISSN : 2503-054X
Vol 4 No: 1, April 2019

A. Pembangkitan Kunci

Proses pembangkitan kunci dilakukan oleh pihak penerima data atau pesan, berikut proses yang berlaku pada pembangkitan kunci algoritma RSA.

1. Pilih dua buah bilangan prima acak yang sangat besar, p dan q. Untuk mendapatkan keamanan yang maksimal, bisa dipilih dua bilangan p dan q yang hampir sama besarnya.
2. Hitung n=p*q, dimana nilai n sebagai modulus.
3. Pilih e secara acak, yaitu bilangan bulat random dengan 1<e < φ (n), gcd (e, φ (n)) = 1. Φ(n) merupakan bilangan bulat positif kurang dari n danvrelatif prima terhadap n dengan φ (n) = (p-1)(q-1). Sehingga diperoleh pasangan kunci publik (e, n).
4. Hitung nilai d, dengan ed mod f(n) = 1 , pasangan kunci privatnya adalah (d, n).

Perhatikan bahwa d dan n juga relatif prima. Bilangan e dan n merupakan kunci publik, sedangkan d kunci privat. Dua bilangan prima p dan q tidak diperlukan lagi, namun p dan q kadang diperlukan untuk mempercepat perhitungan dekripsi.

B. Prosedur Enkripsi

Prosedur enkripsi pada Algoritma RSA adalah dengan mengubah plainteks menjadi cipherteks dengan mengikuti aturan berikut :

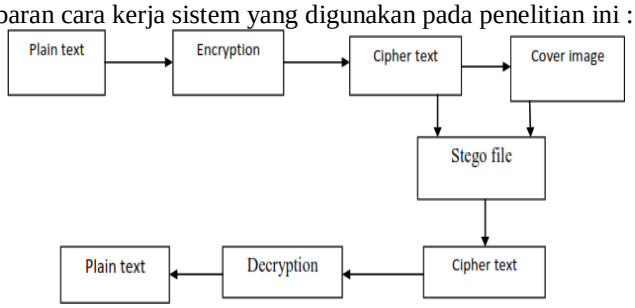
1. Bagi pesan menjadi beberapa kelompok mi, dengan i=1,2,…,| mi |=|n|-1.
2. Enkrip setiap kelompok dengan ci = mie mod n (ingat bahwa proses enkripsi dilakukan dengan menggunakan kunci publik).
3. Gabungkan setiap ci sehingga diperoleh cipherteks c.

C. Prosedur Dekripsi

Prosedur dekripsi merupakan kebalikan dari enkripsi, proses ini mengubah cipherteks menjadi plainteks, atau pesan asli. Prosedur dari proses dekripsi algoritma RSA adalah sebagai berikut :

1. Bagi cipherteks c ke dalam ci, dengan i=1,2,…, | ci |= |n|-1.
2. Dekrip setiap ci dengan mi = cid mod n (proses dekripsi menggunakan kunci privat).
3. Gabungkan setiap mi sehingga diperolah plainteks m

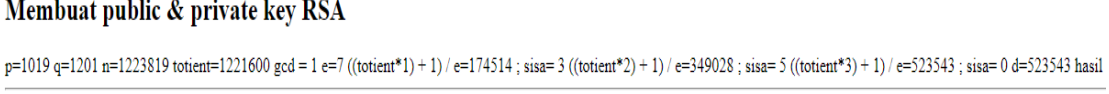
Berikut adalah gambaran cara kerja sistem yang digunakan pada penelitian ini :



Gambar 3 Alur Sistem

3. HASIL DAN PEMBAHASAN

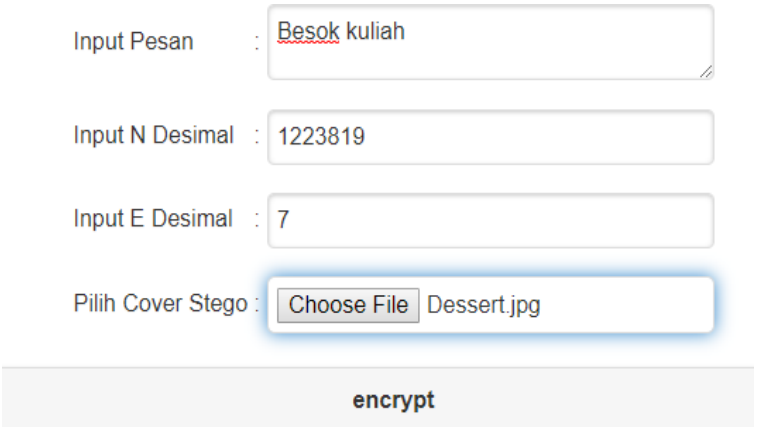
Sasaran dari penelitian ini adalah untuk mengimplementasikan dua teknik Steganografi dan Kriptografi untuk mengamankan pesan rahasia yang disisipkan pada sebuah citra gambar. Dalam makalah ini kami menerapkan algoritma LSB untuk steganografi dan Algoritma RSA untuk kriptografi. Pesan rahsia akan dienkripsi terlebih dahulu menggunakan algoritma RSA, selanjutnya pesan rahasia yang telah dienkripsi akan menjadi *chipper text*. *Chipper text* akan disisipkan ke gambar menggunakan teknik LSB, setelah itu gambar akan dikirim ke penerima menggunakan komunikasi publik seperti email, unggah ke situs web, maupun media social. Berikut ini adalah proses generate kunci privat dan kunci publik pada sistem yang telah dibuat :



Gambar 4 Proses Generate Kunci Privat dan Kunci Publik

Selanjutnya setelah proses pembangkitan kunci selesai, langkah selanjutnya adalah mengacak pesan rahasia menggunakan kunci yang telah dibuat dan menyisipkannya pada citra gambar dengan algoritma LSB, berikut ini adalah proses enkripsi dan penyisipan gambar pada sistem :

ISSN : 2503-054X
Vol 4 No: 1, April 2019

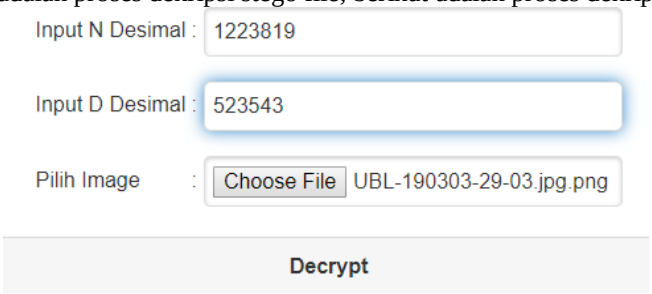


Gambar 5 Proses Penyisipan Pesan Rahasia

Setelah proses penginputan selesai, sistem akan menghasilkan stego file, stego file adalah citra gambar yang telah disisipkan pesan rahasia.

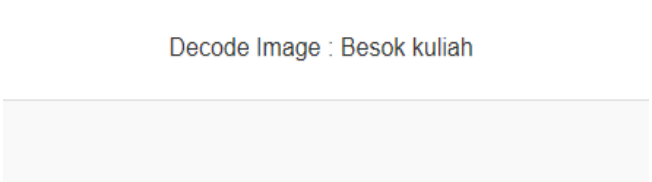
Gambar 6 Hasil Proses Penyisipan

Tahap selanjutnya adalah proses dekripsi stego file, berikut adalah proses dekripsi pada sistem



Gambar 7 Proses Dekripsi Stego File

Setelah proses dekripsi selesai sistem akan menguraikan pesan rahasia yang disisipkan pada citra gambar, berikut adalah hasil dekripsi yang dilakukan oleh sistem :



Gambar 8 Hasil Proses Dekripsi

Hasil yang diperoleh adalah sistem mampu mengembalikan pesan rahasia yang telah dienkripsi dan disisipkan pada citra gambar menjadi pesan asli yang telah didekrip seperti pesan yang disampaikan oleh pengirim. Untuk mengukur hasil kinerja dari sistem yang telah dibuat, penulis menguji hasil ctra gambar asli dibandingkan dengan citra gambar yang telah disisipkan pesan. Metode yang digunakan untuk menguji adalah PSNR dan MSE.

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal

ISSN : 2503-054X
Vol 4 No: 1, April 2019

yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (db). PSNR digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE (*Mean Square Error*). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi ; MSE adalah nilai error kuadrat rata-rata antara citra asli (cover-image) dengan citra hasil penyisipan (stego-image).

Nilai PSNR dibawah 30 dB mengindikasikan kualitas yang relatif rendah, dimana distorsi citra gambar yang telah dilakukan penyisipan terlihat jelas . Akan tetapi kualitascitra gambar yang tinggi berada pada nilai 40dB dan diatasnya (Cheddad, 2010).

Berikut adalah hasil pengujian yang telah dilakukan dengan alat bantu berupa aplikasi Matlab disajikan dalam bentuk tabel yaitu pada tabel 1 hasil pengujian.

Tabel 1 Hasil Pengujian

Citra	MSE	PSNR
Citra Uji 1	0.00	76.7791385 dB
Citra Uji 2	0.03	63.7171682 dB
Citra Uji 3	0.00	74.0187274 dB

Berdasarkan hasil pengujian didapatkan hasil bahwa citra gambar yang telah disisipkan pesan oleh sistem memiliki kualitas yang baik karena berada diatas angka 40 dB.

4. KESIMPULAN DAN SARAN

Berdasarkan implementasi dan pengujian yang telah dilakukan dapat diambil kesimpulan sebagai berikut :

1. Penelitian ini menghasilkan sebuah aplikasi yang dapat digunakan untuk menyisipkan pesan rahasia pada sebuah gambar.
2. Penggabungan algoritma LSB dan algoritma RSA untuk steganografi menghasilkan citra gambar yang memiliki kualitas baik berdasarkan pengujian MSE dan PSNR sehingga sulit dibedakan antara citra asli dan citra stego yang sudah disisipkan pesan.

Adapun saran yang dapat diberikan penulis adalah sebagai berikut :

1. Penelitian selanjutnya diharapkan dapat menggunakan kombinasi algoritma lain sehingga didapatkan hasil stego file yang lebih baik.
2. Membandingkan beberapa kombinasi algoritma untuk steganografi sehingga didapatkan kinerja sistem yang lebih baik.

DAFTAR PUSTAKA

[1] Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. *World Applied Programming*, (13), 191–195.

[2] Aboalsamh, H., Mathkour, H., Dokheekh, S., Mursi, M., & Ghazyassassa. (2008). An improved steganalysis approach for breaking the F5 algorithm. WSEAS Transactions on Computers, 7(9), 1447–1456.

[3] Das, Soumyendu, Subhendu Das, Bijoy Bandyopadhyay, & Sugata Sanyal. (2008) Steganography and Steganalysis: Different Approaches. International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1

[4] De Caro, A., & Iovino, V. (2011). jPBC: Java Pairing Based Cryptography. In Proceedings - IEEE Symposium on Computers and Communications (pp. 850–855).

[5] Hamdi, Mohamed. (2010), Architecture and Insecurity Issues of a Handheld Device. Journal of Security Engineering. Volume 6.

[6] Thomé, E. (2009). Abstracts of the CADO workshop on integer factorization. ACM SIGSAM Bulletin. http://doi.org/10.1145/1610296.1610298