Aisyah Journal of Informatics and Electrical Engineering
Universitas Aisyah Pringsewu

Journal Homepage
http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Penerapan Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) Kombinasi RC4 Berbasis Mobile Android

Agustinus Eko Setiawan[1], Alfredo Pasaribu[2], Rian Candra Pratama[3]
[1,3]Fakultas Teknologi dan Informasi, Universitas Aisyah Pringsewu
[2]Sistem Informasi, STMIK KUWERA
Email : tynuskicenk@gmail.com, Alfredopasaribu91@gmail.com

ABSTRACT

Steganografy is a technique to hide a message on digital image in order to make no one else realizing that in that imagery there are secret message , in the implementation of the steganografy we can use LSB algorithm or Least Significant Bit encrypted with the RC 4 cryptography method on android based mobile device. In this research we use an image file with jpg extension as an experiment and the insertion of message algorithm LSB with encryption RC 4 .We will insert message varying the number to cover image by using the android application studio. Research objectives we are design systems steganografy that can be concealing information into a medium of digital image .

Keywords: Steganography, LSB, Kriptografi, RC4, Image.

ABSTRAK

Steganografi merupakan sebuah teknik menyembunyikan pesan dalam citra digital dengan tujuan agar orang lain tidak menyadari bahwa dalam citra tersebut terdapat pesan rahasia, dalam penerapan steganografi dapat menggunakan algoritma (LSB) atau Least Significant Bit di enkripsi dengan kriptografi metode RC4 pada perangkat mobile berbasis Android. Dalam penelitian ini kami menggunakan file citra berekstensi JPG sebagai bahan percobaan dan penyisipan pesan menggunakan algoritma LSB dengan enkripsi RC4. Kami akan menyisipkan pesan yang bervariasi jumlahnya terhadap cover image dengan menggunakan aplikasi Android Studio. Tujuan penelitian kami adalah merancang sistem steganografi yang dapat menyembunyikan informasi kedalam suatu media berupa citra digital.

Keywords: Steganography, LSB, Kriptografi, RC4, Citra.

1. PENDAHULUAN

Dengan seiring berkembangannya kemajuan teknologi saat ini, membuat sebuah informasi sangat penting. Bahkan ada yang mengatakan bahwa masyarakat dunia kini sudah berada pada sebuah *"information-based society".* Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi yang ingin disampaikan tidak diterima oleh penerima,melainkan jatuh ditangan orang lain. Untuk mengatasi masalah keamanan informasi tersebut, metode yang bisa digunakan adalah ilmu steganografi dan ilmu kriptografi. Steganografi merupakan teknik menyembunyikan pesan atau informasi rahasia agar orang lain tidak menyadari keberadaan dari pesan yang disembunyikan. Teknik ini menggunakan wadah penampung seperti citra.

Seperti diketahui citra merupakan gambar pada bidang dua dimensi yang dihasilkan melalui proses digitasi. Saat ini peredaran citra di internet sangat banyak sehingga sulit untuk menemukan file asli citra tersebut. Untuk menjaga keaslian dari suatu citra, bisa jugamenggunakan steganografi. Jadi steganografi tidak hanya bisa digunakan untuk menyembunyikan pesan atau informasi, tetapi juga bisa digunakan sebagai proteksi hak cipta dan keaslian suatu citra.

Least significant bit merupakan metode untuk mengimplementasikan steganografi pada citra, yaitu dengan menggantikan bit-bit citra asli dengan bit-bit informasi yang akandisembunyikan, sehingga hasil keluaran akan sama dengan yang aslinya jika dilihat dengan kemampuan indera penglihatan manusia.

Berbeda dengan steganografi, kriptografi merupakan teknik penyandian data. Dengan teknik kriptografi data disandikan atau di enkripsi menjadi data rahasia sehingga data itu tidak akan berarti apa-apa bagi pihak yang tidak berwenang yang berhasil mengakses data tersebut. Data rahasia yang telah di enkripsi dan di terima oleh penerima dapat di ubah kembali atau dideskripsikan ke data asli sehingga dapat di pahami.

Penggabungan dua teknik keamanan data yakni kriptografi dansteganografi dengan metode *least significant bit* diharapkan mampu mengamankan data. Kriptografi berfungsi untuk mengenkripsikan data atau pesan, sedangkan steganografi berfungsi untuk menyisipkan pesan kedalam sebuah citra.

2. IDENTIFIKASI MASALAH

Masalah keamanan merupakan salah satu aspek tepenting dari sebuah komunikasi untuk berbagi suatu informasi atau pesan. Masalah keamanan seringkali kurang mendapatkan perhatian untuk melakukan pertukaran informasi. Bahkan kadang berada di urutan kedua, ketiga, atau di urutan terakhir dalam daftar hal-hal yang dianggap penting. Padahal informasi menentukan hampir setiap elemen dari kehidupan manusia. Informasi juga sangat penting artinya bagi kehidupan ini.

Apabila informasi yang sangat penting sampai dapat diketahui oleh pihak yang tidak berwenang maka rencana yang sudah dibuat dapat dengan mudah diketahui oleh pihak yang tidak berwenang.

3. PENELITIAN TERDAHULU

Pada penelitian Yusrian Roman Arubusman (2007), Teknik Informatika, Universitas Gunadarma, metode yang digunakan adalah penggunaan *audio* mp3 sebagai data masukan pembawa pesan rahasia. Dengan membagi media gambar data masukan dalam *frame*, teknik ini diharapkan dapat menyisipkan informasi rahasia ke dalam satu *frame maximum* sebanyak 1 bit sehingga perubahan yang terjadi tidak terlihat mencolok.

Metode proyek akhir ini membuktikan suatu teknik penyembunyian pesan rahasia dalam media *audio*. Hasil *file* keluaran yang dihasilkan oleh proyek akhir ini mengalami perubahan yang rendah, hal ini dibuktikan melalui besar rata-rata nilai *Signal-to Noise Ratio* sebesar 99.5 % yang artinya bahwa hanya terjadi kerusakan *audio* sebesar 0.5 % dalam setiap *file* hasil keluaran yang dibandingkan dengan *file* asli yang menjadi masukannya.

4. METODE PENELITIAN

A. Kriptografi

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

B. Steganografi

Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video.Sedangkan Steganografi LSB (*Least Significant Bit Insertion*) adalah dengan mengubah nilai Least Significant Bit Insertion pada *byte* intensitas piksel dengan teks yang ingin di sembunyikan.

Adapun jenis-jenis gambar yang dapat disisipi pesan dalam steganografi adalah sebagai berikut :

a. JPG / JPEG (*Joint Photographic Experts Assemble*)
   JPG adalah jenis data yang dikembangkan oleh Joint Photographic Experts Assemble (JPEG) yang dijadikan standar untuk para fotografer professional.

b. GIF (*Graphics Interchange Format*)
   GIF, sama seperti JPG, adalah format gambar yang sudah cukup lama digunakan dan salah satu yang umum dipakai di internet. GIF adalah kepanjangan dari Graphics Interchange Format. GIF secara alami adalah gambar dengan 8-bit warna, berarti mereka dibatasi oleh palet sebanyak

256 jenis warna, yang dapat dipilih dari model RGB dan disimpan ke *Color Look Up Tablet* (CLUT), atau sederhananya "*Color Table*". Mereka itu sejatinya adalah palet warna standar, seperti palet "*Web Safe*".Selain bisa transparansi, GIF juga mendukung animasi gambar yang membatasi tiap form nya pada 256 warna standar. Dan karena sifatnya yang tidak pecah-pecah, GIF bisa digunakan untuk menjaga baris dalam tipografi tetap rapi, dan juga bentuk-bentuk geometri.

c. PNG (Portable Network Graphics)

PNG adalah kepanjangan dari Portable Network Graphics. Dikembangkan sebagai alternatif lain untuk GIF, yang menggunakan paten dari LZW– algoritma kompresi. PNG adalah format gambar yang sangat baik untuk grafis internet, karena mendukung transparansi didalam perambah (browser) dan memiliki keindahan tersendiri yang tidak bisa diberikan GIF atau bahkan JPG. Bisa disebut sebagai salah satu format yang merupakan gabungan dari format JPG dan GIF. Untuk tipe ini mampu untuk gradiasi warna. Tipe file PNG merupakan solusi kompresi yang powerful dengan warna yang lebih banyak (24 bit RGB + alpha). Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (lossles compression). Kelebihan file PNG adalah adanya warna transparan dan alpha. Warna alpha memungkinkan sebuah gambar transparan, tetapi gambar tersebut masih dapat dilihat mata seperti samar-samar atau bening.

d. BMP (Bitmap)

Bitmap adalah representasi dari citra grafis yang terdiri dari susunan titik (pixel) yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu bit data (untuk gambar hitam putih) atau lebih (untuk gambar berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam gambar ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 1024×768).

e. TIFF (Tagged Image Format File)

TIFF merupakan format gambar terbaik dengan pengertian bahwa semua data dan informasi (data RGB, data CMYK, dan lainnya) yang berkaitan dengan koreksi atau manipulasi terhadap gambar tersebut tidak hilang. Format TIFF biasa digunakan untuk kebutuhan pencetakan dengan kualitas gambar yang sangat tinggi sehingga ukuran berkas untuk format ini biasanya sangat besar, karena dalam file ini gambar tidak dikompresi. Format ini mampu menyimpan gambar dengan kualitas hingga 32 bit. Format berkas TIFF juga dapat digunakan untuk keperluan pertukaran antar platform (PC, Macintosh, dan Silicom Graphic). Format ini juga mudah digunakan untuk transfer antar program. Sebuah pesan yang akan dikirimkan diubah terlebih dahulu menjadi kode biner dan dimasukkan ke dalam kode biner data lain yang menjadi media atau sampulnya. Lalu kedua kode biner tersebut

dikodekan sehingga menjadi satu kesatuan tanpa mengubah integritas media yang ditumpangi. Selanjutnya data tersebut dikirimkan dan diterima oleh si penerima pesan. Penerima pesan lalu mengkodekan kembali pesan tersebut sehingga pesan bisa dibaca.

C. Istilah-istilah dalam steganografi

1. *Embedding* Data
   Data *embedded* yang tersembunyi dalam suatu media membutuhkan dua *file.* Pertama adalah media asli yang belum dimodifikasi yang akanmenangani informasi tersembunyi. *File* kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa teks, baik itu plainteks, cipherteks, gambar, atau apapun yang dapat ditempelkan ke dalam *bit-stream*. Ketika dikombinasikan, maka akan menghasilkan stego dari media yang telah dijalankan proses *embedded*. Suatu stego-*key* (suatu password khusus) juga dapat digunakan secara tersembunyi, pada saat *decode* selanjutnya dari pesan.

2. *Covertext* atau *cover-object*
   Pesan yang digunakan untuk menyembunyikan embedded message.
3. *Stegotext* atau *stego-object*
   Pesan yang sudah berisi *embedded* message

4. *Encoding* Data
   Encoding adalah proses menempatkan urutan karakter tertentu (huruf, angka, tanda baca, dan simbol tertentu) ke dalam format khusus untuk transmisi yang efisien atau penyimpanan. Sebuah *encoder* mengambil data yang masuk bersamaan dengan beberapa metadata (seperti *signal* yang yang mengindikasikan apakah data mewakili data yang sesungguhnya atau *control character*) dan menghasilkan sebuah nilai yang sudah ter-*encode.*

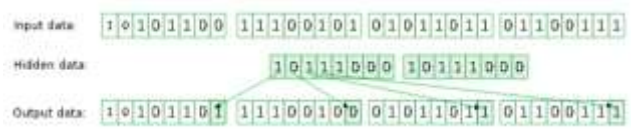
5. *Decoding* Data
   Decoding adalah proses yang berlawanan, konversi dari format yang disandikan kembali ke urutan asli dari karakter. *Encoding* dan *decoding* digunakan dalam komunikasi data, jaringan dan penyimpanan. Istilah *encoding* dan *decoding* sering digunakan dalam referensi untuk proses analog ke *digital* konversi dan *digital* ke analog konversi. Dalam pengertian ini dapat diterapkan pada segala bentuk data, termasuk teks, gambar, *audio, video*, multimedia, dan lain-lain.

D. Metode LSB (*Least Significant Bit*)

Least significant bit (LSB) merupakan salah satu teknik dalam steganografi. Teknik LSB yaitu menggantikan bit terakhir pada gambar dengan bit yang akan disembunyikan (pesan). Misalkan bit pada gambar dengan ukuran 3 pixel sebagai berikut:
(00111111 11101001 11001000)
(00111111 11001000 11101001)
(11000000 00100111 11101001).

Pesan yang akan disisipkan adalah karakter "A" yang memiliki biner 10000001, stego image yang akan dihasilkan adalah:
(00111111 11101000 11001000)
(00111110 11001000 11101000)
(11000000 00100111 11101001)

Ada dua teknik yang dapat digunakan pada LSB, yaitu penyisipan secara sekuensial dan secara acak. Penyisipan sekuensial dilakukan berurutan sedangkan penyisipan acak dilakukan dengan memasukan kata kunci (*stego key*).



Gambar 1. *Least Significant Bit*

E. Kriteria-Kriteria Penyembunyian Pesan

Beberapa kriteria yang harus diperhatikan dalam penyembunyian pesan adalah :

1. *Imperceptibility*
   Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio(misalnya berkas *mp3*, *wav*, *midi*, dan sebagainya), maka indera telinga tidak dapat mendeteksi perubahan pada audio *stegotext*-nya.

2. *Fidelity*
   Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya jika *covertext* berupa citra, maka penyisipan pesan menbuat *stego-text* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio (misalnya berkas *mp3*, *wav*, *midi*, dan sebagainya), maka audio *stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.

3. *Recovery*
   Pesan yang disembunyikan harus dapat diungkapkan kembali*(reveal)*. Karena tujuan steganografi *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stego-text* harus dapat diambil kembali untuk digunakan lebih lanjut.

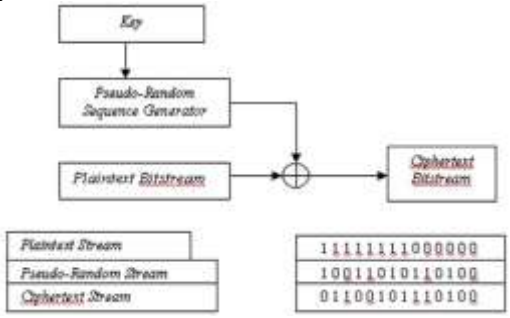
F. RC 4

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 Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali.

RC4 merupakan merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada variabel yang panjang. Algoritma ini tidak harus menunggu sejumlah input data tertentu.

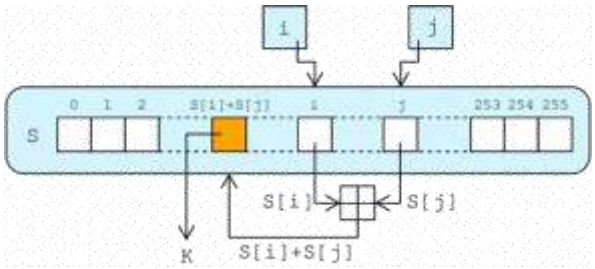
Algoritma RC4 memiliki dua fase, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup S-bit kunci (S merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah array, state dan kunci, dan sejumlah-S hasil dari operasi penggabungan. Operasi penggabungan ini terdiri dari pemindahan (swapping) byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3, begitu juga jika tujuh modulo empat maka akan dihasilkan nilai tiga. Variabel enkripsi dihasikan dari setup kunci dimana kunci akan di XOR-kan dengan plain text untuk menghasilkan teks yang sudah terenkripsi. XOR merupakan operasi logik yang membandingkan dua bit biner. Jika bernilai beda maka akan dihasilkan nilai 1. Jika kedua bit sama maka hasilnya adalah 0. Kemudian penerima pesan akan mendekripnya dngan meng XOR-kan kembali dengan kunci yang sama agar dihasilkan pesan dari plain text tersebut.

Untuk menunjukan cara kerja dari algoritma RC4, berikut dapat dilihat pada blok dibawah :



Gambar 10. Blok Diagram

algortima RC 4 secara umum



Gambar 11. Proses pembangkitan acak untuk kunci RC4

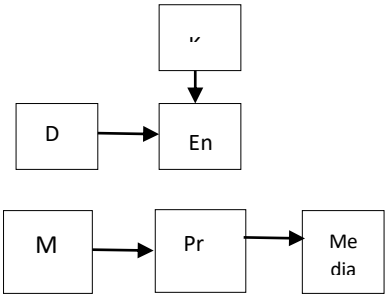
5. PEMBAHASAN

A. Analisis dan Perancangan

Proses perancangan menggunakan UML, perancangan sistem yang akan dilakukan meliputi tiga tahap, yaitu perancangan prosedural, perancangan

proses dan perancangan interface antarmuka.

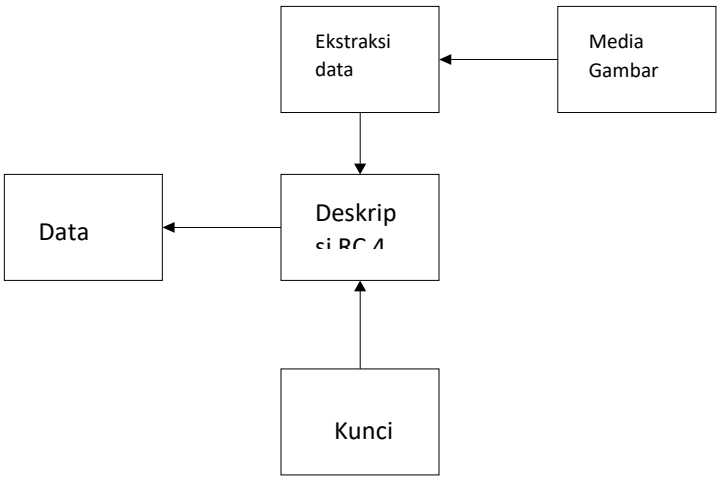
Perancangan prosedural ini berisi tentang flowchart dari aplikasi ini. Flowchart proses enkripsi bisa dilihat pada gambar 2.



Gambar 2.*Flowchart enkripsi*

Dari gambar 2 dapat dijelaskan, pertama kali sistem akan menampilkan menu encode, menampilkan form yang harus diisi untuk proses enkripsi, diantaranya file image, kunci, dan pesan yang akan di sembunyikan. Selanjutnya sistem akan mengecek ekstensi *image*. Selanjutnya sistem mengenkripsi kunci dan pesan. Selanjutnya hasil dari enkripsi akan di sembunyikan kedalam file dengan metode Steganografi LSB. Hasil dari proses diatas selanjutnya bisa diunduh dalam bentuk file gambar.

Sedangkan proses deskripsi bisa dilihat pada gambar 3.



Gambar 3.*Flowchart deskripsi*

Dari gambar 3 dapat dijelaskan, pertama kali sistem akan menampilkan menu decode, menampilkan form yang harus diisi untuk proses dekripsi, diantaranya file image dan kunci. Selanjutnya sistem akan mengecek ekstensi *image*dan kunci yang diinput. Selanjutnya sistem mengdeskripsipesan. Hasil dari proses diatas selanjutnya pesan bisa diunduh dalam bentuk file txt.

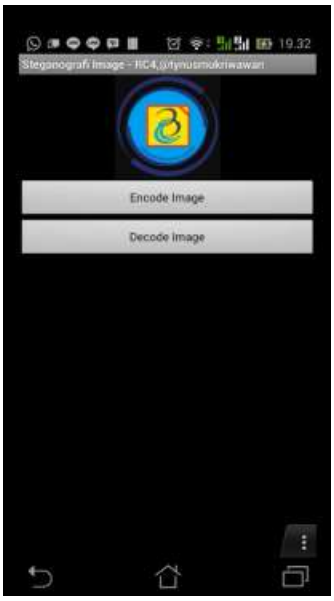
B. Implementasi

Implementasi adalah bermuara pada aktivitas, aksi, tindakan, atau adanya mekanisme suatu sistem. Implementasi bukan sekedaraktivitas, tetapi suatu kegiatan yang terencana dan untuk mencapai tujuan kegiatan [8].

Pengertian implementasi yang dikemukakan di atas,dapatdikatakan bahwa implementasi adalah bukan sekedar aktivitas, tetapisuatu kegiatan yang terencana dan dilakukan secara sungguh-sungguhberdasarkan acuan norma tertentu

untuk mencapai tujuan kegiatan. Olehkarena itu implementasi tidak berdiri sendiritetapi dipengaruhi oleh objekberikutnya.

1. Tampilan Awal
   Tampilan ini merupakan *homepage*yang berisi menu *encode* dan *decode* dimana *encode* untuk proses enkripsi file dan *decode* untuk proses deskripsi.



Gambar 7. Tampilan Awal / *Homepage*

2. Tampilan Encode
   Berikut ini adalah tampilan form proses *enkripsi*dari program yang memiliki fungsi steganografi berbasis web untuk diuji coba :

Gambar 8. Form Proses *enkripsi* file

3. Tampilan Decode
   Berikut ini adalah tampilan form proses *deskripsi*dimana hasil dari *deskripsi* ini adalah berupa txt yang isinya *message* yang sebelumnya sudah di *encode*:

Gambar 12. Form Proses *deskripsi* file

6. PENGUJIAN PROGRAM

1. Dalam percobaan ini, dilakukan pada media gambar yang akan disisipi oleh *file* data, Gambar 4.2 menunjukkan isi dari script Enkripsi RC 4 dalam *file* program java. Gambar 4.3 menunjukkan media gambar yang belum disisipi oleh *file* data. Gambar 4.4 menunjukkan media gambar yang sudah disisipi oleh *file* data. Gambar 4.5 menunjukkan isi dari Scritp Dekripsi RC 4

..

```
/***PROSES ENKRIPSI DENGAN RC4 */
String plainteks = editTextMessage.getText().toString();
String key= editTextKey.getText().toString();

//encryption
RC4 rc4 = new RC4(key.getBytes());
byte[] cipher = rc4.encrypt(plainteks.getBytes());
String chiper64= Base64.encodeToString(cipher, 1);
editTextMessageEncrypt.setText(chiper64);
/***END PROSES */
}
```

Gambar 4.2 : Script Enkripsi RC

Gambar 4.3 : Media Gambar Sebelum Disisipi Oleh *File* Pesan

Gambar 4.4 : Media Gambar Setelah Disisipi Oleh *File* Pesan

```
/***PROSES DEKRIPSI RC4 */
String k= editTextKey.getText().toString();
String chiper64= EditTextDecodedMessage.getText().toString();
//decryption
RC4 rc4d = new RC4(k.getBytes());
byte[] result = rc4d.decrypt(Base64.decode(chiper64.getBytes(), 1));
String pesan=new String(result);

editTextMessageDecrypt.setText(pesan);
/***END PROSES */
}
```

Gambar 4.5 : Script File Dekripsi RC 4

2. KESIMPULAN DAN SARAN

Berdasarkan analisa yang telah dilakukan mulai dari pengumpulan informasi, pemecahan masalah, hingga pengembangan serta pemanfaatan sistem ini, maka dapat ditarik bebrapa kesimpulan serta saran-saran yang perlu diperhatikan demi kelancaran sistem yang dibangun ini.

1. Kesimpulan

Berdasarkan uji coba sistem aplikasi yang telah dibangun maka dapat ditarik beberapa kesimpulan sebagai berikut:

a. Dengan adanya sistem ini, maka dapat melakukan pertukaran informasi dengan lebih aman, dimana informasi disisipi ke dalam media gambar.
b. Informasi akan menjadi lebih sulit untuk dipecahkan, dikarenakan sebelum proses penyisipan informasi, dilakukan proses enkripsi terlebih dahulu terhadap informasi tersebut.

2. Saran

Kemampuan sistem ini sebenarnya masih jauh dari sempurna, terlebih karena menggunakan metode *full* LSB (*Least Significant Bit*) dan tidak menggunakan *image compression* terhadap hasil dari media gambar yang telah disisipi oleh informasi. Oleh karena itu kedepannya disarankan untuk membuat dengan metode yang berbeda dimana posisi penyisipan informasi dapat secara acak dan menggunakan *image compression*, sehingga informasi yang disisipi dalam sistem ini menjadi lebih sulit untuk dipecahkan

3. DAFTAR PUSTAKA

[1] Arifanto, Teguh.2011.Membuat Interface Aplikasi Android Lebih Keren dengan LWUIT. Andi Publisher, Yogyakarta

[2] Sugeng Santoso, Padeli, Arisman. 2015. Steganografi Audio (Wav) Menggunakan Metode Lsb (Least Significant Bit). NS-CCIT RAHARJA 2015.

[3] Ghazali Moenandar Male, Wirawan, Eko Setijadi. 2012. Analisa Kualitas Citra Pada Steganografiuntuk Aplikasi E-Government. Prosiding Seminar Nasional Manajemen Teknologi XV.

[4] Putri Alatas. Implementasi Teknik Steganografi Dengan Metode Lsb Pada Citra Digital. Tugas Akhir. Jurusan Sistem Informasi, Fakultas Ilmu Komputer & Teknologi. Universitas Gunadarma.

[5] Caroline, Maureen Linda. 2011. Metode Enkripsi baru : Triple Transposition Vigènere Cipher. Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011.

[6] Prasetyo, Fahri Perdana. 2010. Steganografi Menggunakan Metode Lsb Dengan Software Matlab. Universitas Islam Negeri Syarif Hidayatullah

[7] Gupta, Shilpa., Geeta Gujrat, dan Neha Aggarwal. 2012. Enhanced Least Significant Bit algorithm For Image Steganography. *IJCEM*. 15(4): 2230-7893.

[8] Patel, Hardik. dan Preeti Dave. 2012. Steganography Technique Based on DCT Coefficients. *IJERA*. 2(1): 713-717