E-ISSN: 2528 - 6544
P-ISSN: 2620 - 3383
Vol.3 No.1 Agustus 2018

Technomedia Journal

iLearning Journal Center (iJC)

Technomedia Journal (TMJ)
Vol.3 No.1 Edisi Agustus 2018
E-ISSN: 2528 – 6544
P-ISSN: 2620 – 3383

Perancangan Aplikasi Steganografi Dengan Teknik LSB dan AlgoritmaRC4 & Base64 Encoding

Oleh Soleh, S.Kom.,M.MSi[1]
Fifit Alfiah M.Kom[2]
Budi Yusuf[3]

Dosen Sistem Informasi STMIK Raharja[1], Dosen Teknik Informatika STMIK Raharja[2],Mahasiswa STMIK Raharja Jurusan Teknik Informatika[3]
Jl. Jend. Sudirman No. 40, Modern Cikokol, Tangerang
E-mail: oleh.soleh@raharja.info[1]; fifitalfiah@raharja.info[2]; budiyusuf@raharja.info[3]

ABSTRAK

Penyembunyian pesan rahasia dengan cara menyisipkan pesan ke dalam sebuah file gambar atau lebih sering dikenal dengan istilah steganografi adalah pengembangan dari kriptografi. Kriptografi adalah ilmu penyembunyian pesan dengan cara mengenkripsi pesan tersebut ke dalam bentuk acak yang sulit dibaca. Pesan rahasia yang disembunyikan dengan steganografi ini tidak menarik perhatian karena pesan tersebut hanya disisipkan ke dalam sebuah file. Beberapa metode algoritma steganografi menggunakan sebuah kombinasi untuk melakukan tugas penyembunyian pesan rahasia. Metode yang digunakan adalah metode LSB (Least Significant Bit), algoritma RC4 dan Encoding Base64. Metode ini menggabungkan teknik steganografi dengan teknik kriptografi. Pesan dienkripsi terlebih dahulu sebelum disisipkan ke dalam sebuah file. Tujuan penelitian ini adalah untuk sebagai pengetahuan dalam bidang keamanan data didunia maya berbasis mobile application. Karena penerapan pada teknik ini digunakan untuk masyarakat umum terutama pemerintah, perusahaan, atau sekelompok orang tertentu yang saling bertukar informasi penting seperti password, rahasia perusahaan, data orang penting, informasi tentang musuh di lapangan, atau data – data sensitif lainnya secara aman tanpa orang lain mengetahuinya.

Kata kunci : *Steganografi, Kriptografi, LSB, algoritma RC4, Base64 Encoding*

ABSTRACT

The concealment of secret messages by inserting messages into an image file or more commonly known as steganography is the development of cryptography. Cryptography is the science of hiding messages by encrypting them into random forms that are difficult to read. This hidden secret message with steganography does not attract attention because the message is simply inserted into a file. Some steganographic algorithm methods use a combination to perform the task of hiding secret messages. The method used is the method of LSB (Least Significant Bit), RC4 algorithm and Base64 Encoding. This method combines steganography techniques with cryptographic techniques. The message is encrypted before being inserted into a file. The purpose of this study was to be a knowledge in the field of virtual world data security based on mobile applications. Because the application of this technique is used for the general public, especially the government, companies, or certain groups of people who exchange important information such as passwords, company secrets, important person data, information about enemies in the field, or other sensitive data safely without anyone else know it.

Keywords: *Steganography, Cryptography, LSB, RC4 algorithm, Base64 Encoding*

PENDAHULUAN

Perkembangan teknologi informasi sangat berpengaruh akan pentingnya dalam mendapatkan informasi. Perkembangan teknologi juga mempermudah orang berkomunikasi, dalam bentuk mengirim pesan dan menerima pesan. Dengan adanya internet, pengiriman pesan menjadi lebih cepat dan mudah. Bahkan hasil survey yang dilakukan oleh APJII (Asosiasi Penyelenggara Jaringan Internet Indonesia) di tahun 2016, mengungkapkan lebih dari 80 juta orang pengguna internet di indonesia yang menggunakan layanan email untuk mengirim pesan.

Data dari Security Threat Report pada tahun 2013, Indonesia berada diurutan pertama dalam daftar sepuluh besar yang dianggap sebagai negara paling berisiko mengalami serangan IT Security. Dan data dari Kemenkominfo pada tahun 2013, ada 36, 6 juta insiden serangan *cyber crime* di Indonesia. Banyaknya jumlah serangan *hacker, cracker,* dan *carder* menjadi ancaman kejahatan didunia maya seperti pada layanan email, media sosial, maupun aplikasi *messenger*, ataupun mengirim data secara *peer-to-peer* melalui jaringan bluetooth, maupun jaringan wireless. Pemerintah, perusahaan ataupun sekelompok orang yang ingin saling bertukar informasi penting atau mengirim data rahasia seperti *password*, rahasia perusahaan, data orang penting, informasi tentang musuh di lapangan, atau data – data sensitif lainnya menjadi khawatir dan sangat merugikan terhadap kejahatan tersebut, yang membuat pengiriman informasi menjadi terhambat dan sangat merugikan.

Keamanan informasi menjadi hal yang penting agar pesan tersebut tidak dapat dicuri, tetapi hal itu sulit dihindari jika pesan tetap dapat dicuri dengan memanfaatkan celah pada suatu sistem pengiriman pesan melalui email, media sosial, dan aplikasi messenger seperti pada teknik SS7 (Signalling System No.7) dengan memanfaatkan sistem sinyal pada pengiriman pesan. Pencuri dapat mengganti isi pesan atau pesan tersebut disimpan untuk keperluan di masa mendatang.

Ada banyak teknik untuk menghindari kejahatan tersebut, salah satu caranya adalah dengan menyembunyikan pesan ke dalam suatu pesan lain. Teknik ini disebut dengan teknik steganografi. Teknik menyembunyikan pesan pada pesan lain untuk menghindari kecurigaan pada saat data dicuri. Dengan teknik ini pesan dapat disembunyikan tanpa ada orang lain sadar bahwa ada pesan rahasia didalamnya dan penggabungan teknik kriptografi dalam mengenkripsi pesannya. Mengirim pesan melalui layanan email, media sosial, dan aplikasi messenger tentunya menjadi lebih aman menggunakan penggabungan teknik tersebut. Hal inilah yang mendorong penulis melakukan penelitian dengan perkembangan di era digital ini dalam mengatasi permasalah tersebut melalui informasi data yang nantinya dapat menjadi perbandingan dengan teknik pencegahan pencurian data yang lainnya.

Berdasarkan latar belakang diatas, maka penulis mengambil rumusan masalah untuk dapat membantu penulisan dalam mencapai tujuan penelitian yaitu penampilan pesan yang telah dimasukkan pesan dengan sebelumnya pesan yang akan dikirim dienkripsi terlebih dahulu lalu disisipkan ke dalam suatu *file* gambar dengan metode LSB (*Least Significant Bit*) sebelum dikirim melalui layanan email, media sosial maupun aplikasi *messenger*.

Adapun batasan yang dapat ditentukan penulis dalam penelitian ini , antara lain :

1. Data yang digunakan berupa data teks, file gambar *archive* rar.
2. Metode yang digunakan dalam teknik steganografi adalah metode LSB (Least Significant Bit).
3. Algoritma kriptografi yang digunakan adalah algoritma RC4 dan Base 64 Encoding.

Tujuan utama dalam penulisan penelitian ini adalah memperoleh pengetahuan penggabungan antara teknik kriptografi dengan metode algoritma RC4 dan algoritma Base64 Encoding dan teknik steganografi LSB (Least Significant Bit) melalui perancangan sistem yang berbasis *mobile application* untuk menjadi perbandingan antara teknik pencegahan pencurian data lainnya.

PERMASALAHAN

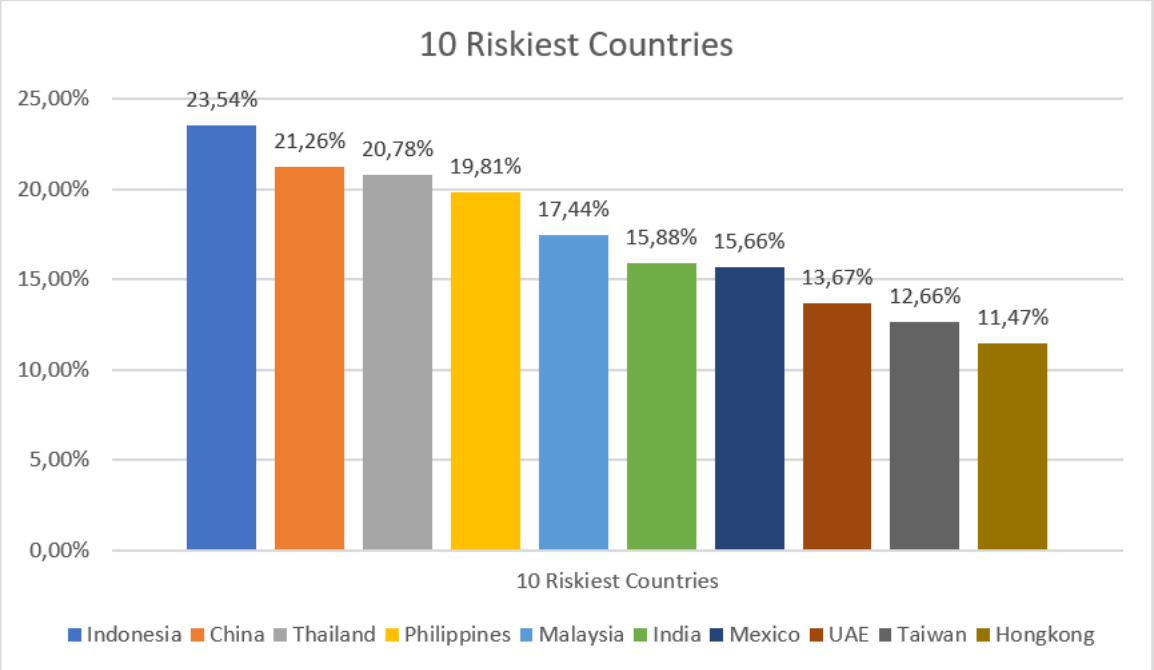


Diagram 1. 10 Negara-negara paling berisiko
(**Sumber :** Security Threat Report 2013)

Indonesia menjadi negara yang paling berisiko terpapar dari ancaman serangan malware dan keamanan dalam berinternet mencapai 23,54%. Dan data dari Kemenkominfo

E-ISSN: 2528 – 6544
P-ISSN: 2620 – 3383

pada tahun 2013, ada 36,6 juta insiden serangan cyber crime di Indonesia. Hasil survei diatas menunjukkan perlu adanya suatu bentuk pengamanan dalam berselancar didunia maya. Dengan resiko yang cukup tinggi dan tingginya angka kejahatan serangan pada dunia maya maka keamanan data sangat diperlukan untuk menjamin kerahasian data. Jika ingin mengirim data penting yang bersifat rahasia diperlukan suatu sistem khusus untuk menjamin kerahasian data saat pengiriman berlangsung.

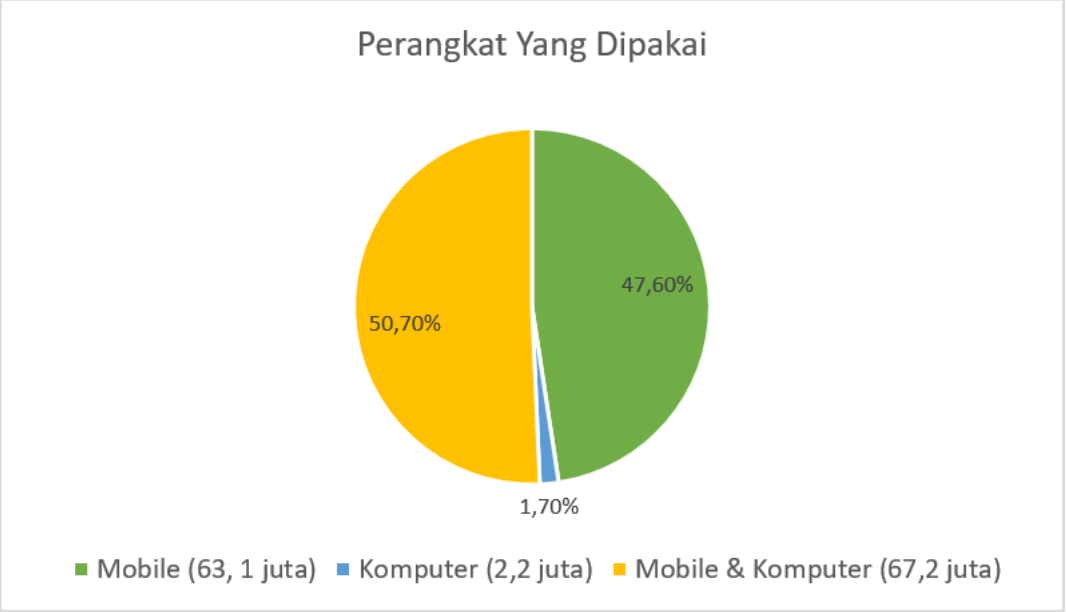


Diagram 2. Perangkat yang dipakai
(**Sumber :** Penetrasi & Perilaku Pengguna Internet 2016, APJII)

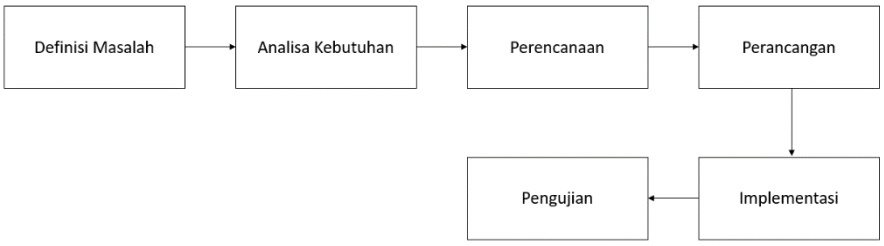
Hasil survei APJII pada tahun 2016 menunjukkan bahwa 63,1 juta menggunakan perangkat mobile untuk beraktivitas di internet, sedangkan 67,2 juta menggunakan mobile dan komputer untuk berselancar, dan 2,2 juta pengguna internet hanya menggunakan komputer. 84,6 juta pengguna internet telah menggunakan smartphone untuk mengirim email dan 46,4 juta menggunakan komputer personal maupun laptop. Sedangkan pada tahun yang sama pengguna media sosial telah mencapai 129,4 juta jiwa.

Berdasarkan data survei diatas dapat dilihat dengan banyaknya pengguna internet melalui perangkat mobile atau komputer dan dengan banyaknya pengguna internet yang mengirim email baik melalui smartphone ataupun komputer personal maupun laptop. Dengan permasalahan dan berdasarkan data diatas, maka penulis memutuskan untuk membuat aplikasi keamanan informasi yang dapat diakses melalui smartphone.

METODOLOGI PENELITIAN

Meliputi rancangan penelitian, teknik pengumpulan data, dan teknik analisis data,yang diuraikan secara singkat. Serta penambahan *literature review* yang berisikan serangkaian

penelitian yang relevan dengan topik atau tema penelitian yang diambil,



Gambar 1. Metode Penelitian

Keterangan :

1. Definisi Masalah yaitu mencari data-data yang berkaitan dengan masalah yang sedang terjadi untuk mengetahui letak permasalahannya lebih detail untuk selanjutnya di analisa untuk pemecahan masalahnya.
2. Analisa Kebutuhan, setelah mencari data dan mengetahui letak permasalahannya selanjutnya menganalisa apa saja yang dibutuhkan untuk pemecahan masalah tersebut.
3. Perencanaan, hasil dari analisa kebutuhan kemudian dibuat suatu konsep perencanaan aplikasi steganografi dengan teknik LSB dan algoritma RC4 & base64 encoding dalam menyelesaikan masalah berdasarkan data.
4. Perancangan sistem, konsep yang telah terbentuk lalu diaplikasikan ke dalam perancangan sistem sesuai dengan konsep yang telah direncanakan.
5. Implementasi, apabila langkah-langkah sebelumnya telah dilaksanakan dengan benar maka langkah selanjutnya yaitu melakukan penerapan sistem yang telah dirancang sebelumnya.
6. Pengujian, langkah ini dilakukan untuk mengetahui apakah sistem telah berjalan dengan benar sesuai dengan perencanaan di awal.

Berikut ini adalah daftar literature review yang digunakan dalam penelitian ini :

1. Penelitian yang dilakukan oleh Harianto Antonio dengan judul yaitu "Studi Perbandingan Enkripsi Steganografi Dengan Menggunakan Metode Least Significant Bit Dan End Of File". Penelitian ini membahas tentang menganalisa perhitungan waktu penyembunyian pesan, ukuran data, analisa keamanan, dan analisa ketahanan dengan cara membandingkan antara metode *least significant bit* dan *end of file*.
2. Penelitian yang dilakukan oleh Suriski Sitinjak,Yuli Fauziah, Juwairiah dengan judul yaitu "Aplikasi Kriptografi File Menggunakan Algoritma Blowfish". Penelitian ini membahas tentang mengenkripsi file (*plaintext*) dalam bentuk teks, gambar, suara, video, juga *archieve* seperti .zip dan .rar menggunakan metode kriptografi algoritma blowfish dengan implementasi menggunakan Visual Basic 6.0.
3. Penelitian yang dilakukan oleh Jane Irma Sari, Sulindawaty, Hengki Tamando Sihotang dengan judul yaitu "Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (LSB)". Penelitian ini membahas tentang menyembunyikan pesan teks pada citra

digital dengan menggunakan algoritma Hill Cipher untuk melakukan enkripsi dan deskripsi dengan menggunakan matriks berukuran m x m dan metode Least Significant Bit sebagai penyisipan pesannya.

4. Penelitian yang dilakukan oleh Taronisokhi Zebua, Eferoni Ndruru dengan judul yaitu "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4". Penelitian ini membahas tentang mengamankan citra digital dengan menggunakan teknik kriptografi modifikasi algoritma RC4 dengan modifikasi yang dilakukan menambahkan blok initial vector pada proses enkripsi dan deskripsi.
5. Penelitian yang dilakukan oleh Marta Darma Putra, Mardhiya Hayaty dengan judul yaitu "Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 Dan RC4". Penelitian ini membahas tentang mengenkripsi gambar menggunakan perpaduan antara algoritma base64 dan RC4.
6. Penelitian yang dilakukan oleh Shuliang Sun, Yongning Guo dengan judul "A Novel Image Steganography Based on Contourlet Transform and Hill Cipher". Penelitian ini membahas tentang penyembunyian pesan melalui gambar yang sudah diproses steganografi dengan berdasarkan *transform contourlet* menyediakan representasi multi-skala dan multi-arah pada sebuah gambar dan algoritma matriks *hill chipher*.
7. Penelitian yang dilakukan oleh Khanna Tiara, Fella Megita Putri, Henni Triyani dengan judul "Optimalisasi Single Sign On Untuk Meningkatkan Sistem Keamanan OJRS+". Penelitian ini membahas tentang sistem *single sign on* pada sebuah website OJRS+ sebagai fasilitas untuk mempermudah dalam melakukan batal tambah jadwal rencana studi secara online yang memberikan rasa aman dan mudah dalam menggunakannya.

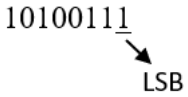
Setelah melakukan peninjauan terhadap 7 *Literature Review*, didapat kesimpulan bahwa telah banyak penelitian mengenai sistem keamanan data baik dengan teknik steganografi maupun dengan teknik steganografi. Sedangkan perbedaan yang dilakukan penulis pada penelitian ini ialah menggabungkan teknik steganografi metode LSB (*Least Significant Bit*) dengan teknik kriptografi metode algoritma RC4 dan algoritma Base64 Encoding berbasis mobile application. Selain merancang sistem penulis juga memberi pengetahuan tentang hasil yang diperoleh setelah perancangan sistem tersebut untuk mengetahui hal-hal apa saja yang dapat mendukung perancangan sistem tersebut.

HASIL DAN PEMBAHASAN

Menurut Frank Y. Shih, steganografi digital bertujuan menyembunyikan informasi digital kedalam bentuk informasi digital lainnya sehingga seseorang dapat menyembunyikan informasi dan mencegah pendeteksian karena informasi rahasia disembunyikan dalam sebuah informasi. Tidak seperti kriptografi, yang membuat pesan terlihat acak dan dapat menimbulkan kecurigaan, steganografi menyembunyikan tanpa orang lain menyadarinya karena pesan tersebut "bersembunyi" dibalik pesan lainnya.

E-ISSN: 2528 – 6544
P-ISSN: 2620 – 3383

Pada penyembunyian datanya menggunakan metode LSB (*Least Significant Bit*) dengan mengganti bit-bit data pada *cover* di dalam citra gambar dengan bit-bit data rahasia. Perubahan yang dilakukan dalam metode LSB adalah susunan bit didalam sebuah *byte* (1 *byte* = 8 bit) yang paling kanan.

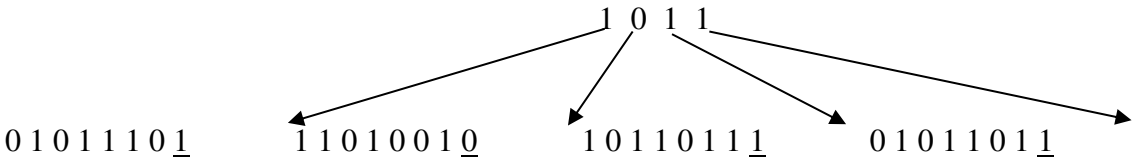


Gambar 2. *Least Significant Bit*

Misalkan pada bit suatu citra gambar sebelum perubahan bernilai :

0 1 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 1 1 0 0 1 0 1 1 0 1 1

Bit data rahasia yang akan disembunyikan bernilai :



Menurut Jonathan Katzis dan Yehuda Lindell, kriptografi berhubungan dengan mekanisme untuk memastikan integritas, teknik untuk bertukar *secret-key*, protokol untuk mengautentifikasi pengguna, pelelangan dan pemilihan elektronik, dan uang digital. Kriptografi modern melibatkan studi teknik matematika untuk mengamankan informasi digital, dan perhitungan terdistribusi.

Algoritma RC4 menggunakan inisialisasi S-Box dengan panjang 4 byte pada mode 4 byte, dengan memakai array S[0]=0, S[1]=1, S[2]=2, S[3]=3, sehingga akan didapatkan array S yaitu : 0 1 2 3.

Masukkan plaintext : H A L O, dengan key : 2537

Algoritma RC4 menggunakan sistem sandi *state*, yaitu larik byte berukuran 256 yang termutasi dan tercampur oleh kunci.

Array S
0 1 2 3
Array K
2 5 3 7

Inisialisasi i dan j dengan 0 kemudian dilakukan KSA untuk membuat *state-array* terlihat acak.

i = 0
j = (0 + S[i] + K [0 mod 4]) mod 4
= (0 + 0 + 2) mod 4 = 2
Swap (S[n],S[n])

n digantikan dengan array s yang diacak. Selanjutnya dilakukan proses PRGA yang dilakukan sebanyak jumlah karakter yaitu 4. Hal ini untuk pengoperasian XOR untuk setiap karakter pada plainteks.

Array S
1 2 0 3
Inisialisasi
i = 0
j = 0
Iterasi 1
i = (0 + 1) mod 4 = 1
j = (0 + S[i]) mod 4 = (0+ 2) mod 4 = 2
swap (S[n],S[n])
1 0 2 3
K1 = S[(S[n]+S[n]) mod 4] = S[2 mod 4] = 2
K1 = 00000010

Setelah menemukan kunci dari setiap karakter selanjutnya operasi XOR antara plainteks dengan kunci yang dihasilkan. Proses XOR pada enkripsi akan menghasilkan pesan yang sudah teracak.

HURUF	KODE ASCII (Binary 8 bit)
H	01001000
A	01000001
L	01001100
O	01001111

Tabel 1. Kode ASCII Plainteks

Pada tabel 1 merupakan tabel dari kode ASCII dengan bilangan biner 8 bit pada setiap karakter. Kode ASCII ini berfungsi sebagai plainteks yang nantinya akan digabungkan dengan proses XOR pada enkripsi akan menghasilkan pesan yang sudah teracak.

	H	**A**	**L**	**O**
Plainteks	01001000	01000001	01001100	01001111
Key	00000010	00000011	00000010	00000010
Chipherteks	01001010	01000010	01001110	01001101
	J	**B**	**M**	**N**

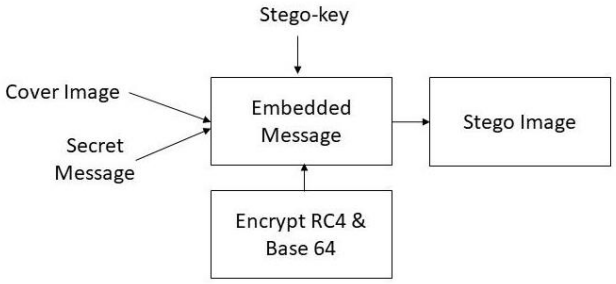
Tabel 2. Proses XOR Enkripsi

Pada tabel 2 adalah proses enkripsi plainteks, key, chipherteks yang akan diproses dengan metode XOR. Proses ini akan mendapatkan nilai acak yang merupakan hasil dari enkripsi.

Menurut Marta Darma Putra dan Mardhiya Hayaty, algoritma base64 adalah teknik konversi pencodean radix-64, teknik ini merupakan pemetaan untuk merubah input numeric kebentuk karakter sebagai hasilnya. Masukkan karakter yang diubah kedalam ke dalam bentuk bilangan ASCII yang selanjutnya didapatkannya nilai biner tersebut, kemudian nilai biner tersebut digabungkan dan dikelompokkan kedalam 1 kelompok mengandung 6 bit. Tiap-tiap kelompok dipetakan untuk diubah menjadi karakter yang berdasarkan pada set karakter base64.

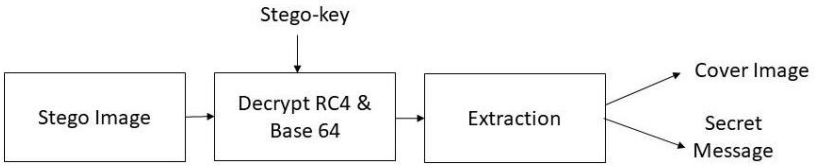
Perancangan Alur Kerja Sistem

Perancangan alur kerja sistem untuk menentukan alur proses dalam steganografi, berikut alur dari proses enkripsi steganografi seperti terlihat pada gambar 3 dibawah ini.



Gambar 3. Alur Proses Enkripsi Steganografi

Dalam gambar 3 dijelaskan alur dari proses enkripsi steganografi dalam aplikasi steganografi. Dimana sebelum melakukan enkripsi, *cover image* menjadi sampul dari pesan rahasia yang akan disembunyikan. *Secret message* akan dienkripsi oleh sistem, yang nantinya pesan tersebut akan menjadi bilangan acak yang sulit untuk dibaca. Pengenkripisian ini menggunakan algoritma RC4 dan Base64 yang secara otomatis *secret message* yang dimasukkan akan menjadi bilangan acak dan harus memasukkan *stego-key* untuk menjadi kunci mengembalikkan pesan tersebut.



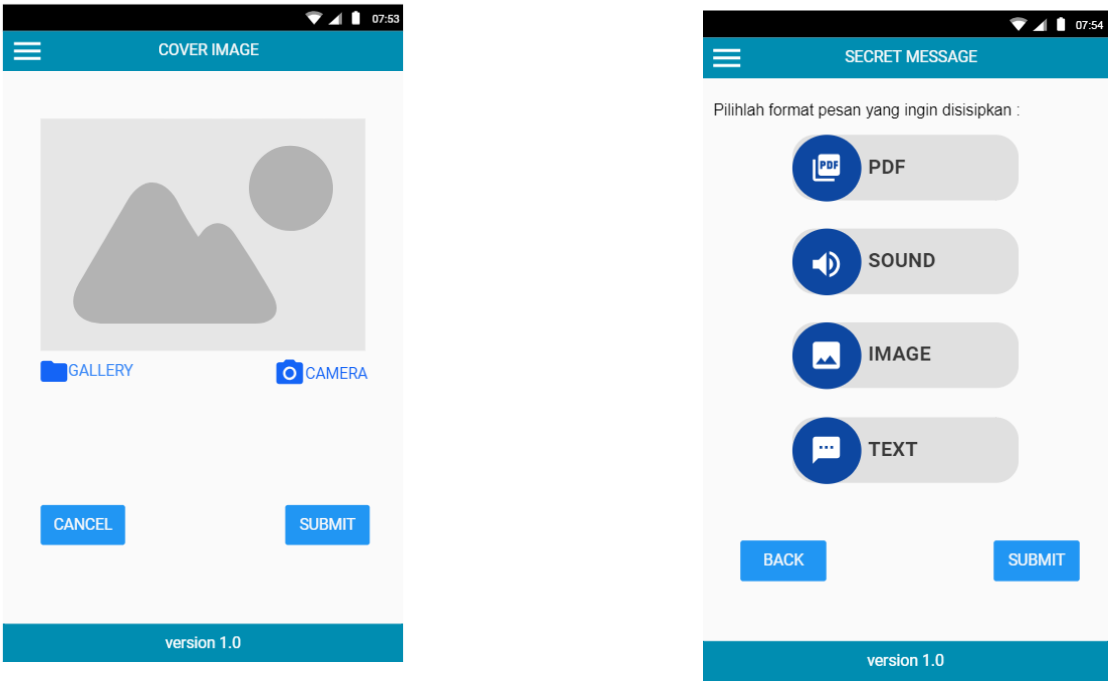
Gambar 4. Alur Proses Dekripsi Steganografi

Dalam gambar 4 dijelaskan alur dari proses dekripsi steganografi dalam aplikasi steganografi. Dimana ketika mendekripsi *stego image* yang terdapat pesan rahasia didalamnya, sebelum dipisahkan antara cover image dan message harus memasukkan *stego-key* terlebih dahulu untuk mengembalikkan pesan yang terlihat acak. Setelah *stego-key* yang dimasukkan telah benar maka sistem secara otomatis akan memisahkan *cover image* dengan *secret message*.

Pada tahap implementasi sistem penelitian ini adalah melakukan implementasi sistem aplikasi steganografi, interface yang digunakan oleh user dimulai dari implementasi sampai dengan fungsional sistem. Tampilan halaman Home sebagai menu utama untuk menggunakan sistem aplikasi steganografi ini. Tampilan home tersebut seperti terlihat pada gambar 5 dibawah ini.

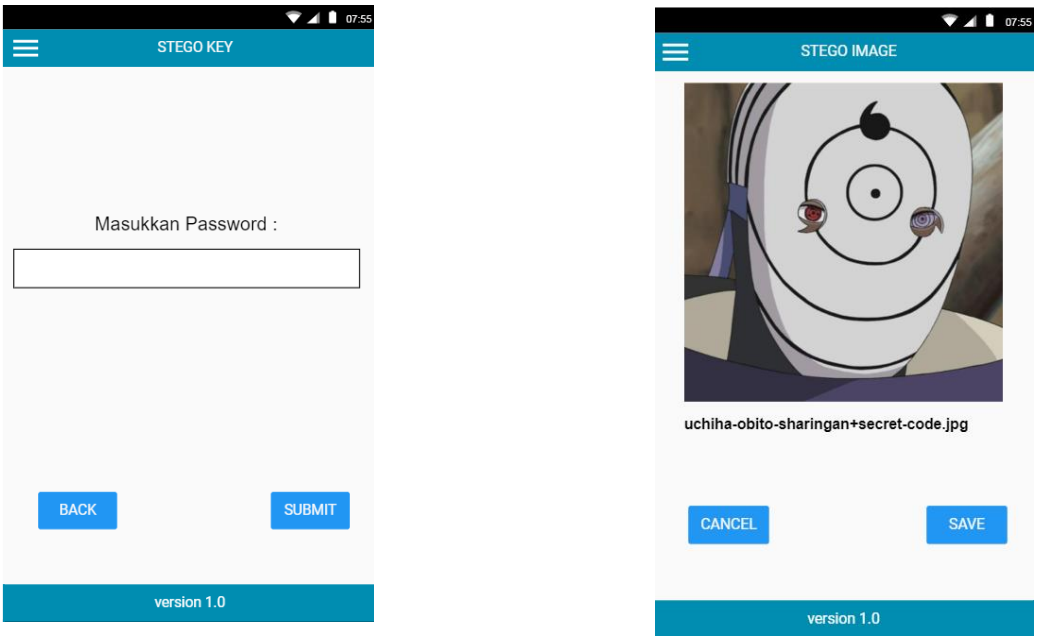
Gambar 5. Tampilan Home

Sesuai tampilan diatas ada 2 pilihan fitur, yaitu *encode* dan *decode*. Fitur *encode* ini digunakan untuk membuat *stego image* atau membuat steganografi dengan *cover image* yang akan disisipkan *secret message*. *Secret message* akan dienkripsi menjadi bilangan acak dan dikunci. Fitur *decod*e adalah kebalikan dari fitur *encode* yaitu untuk memisahkan stego image menjadi *cover image* dan *secret message* yang telah dienkripsi sebelumnya.



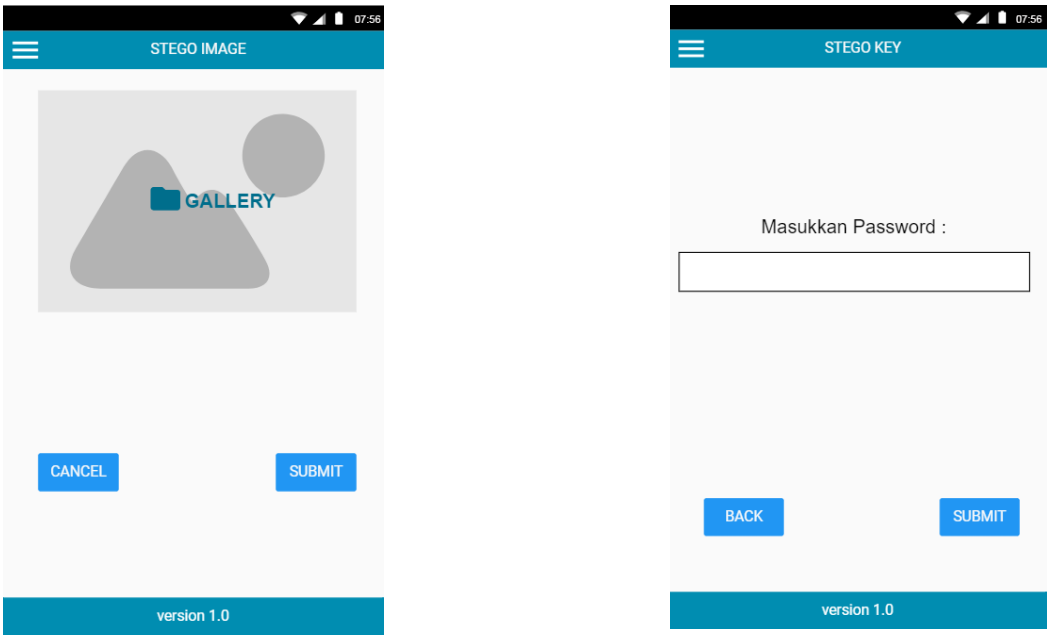
Gambar 6. Tampilan input cover image dan secret message pada fitur encode

Selanjutnya jika memilih fitur *encode*, maka user akan diarahkan ke tampilan *cover image* untuk memasukkan sampul gambar yang akan menutupi secret message. User dapat memilih apakah ingin memasukkan gambar lewat *gallery* handphonenya atau langsung mengambil gambar lewat kameranya. Selanjutnya user diwajibkan memilih format *secret message* mana yang akan disisipkan pada *cover image*. Sebelum mendapatkan hasil *stego image*, user akan diarahkan pada tampilan *stego key*, seperti gambar 7 dibawah ini.



Gambar 7. Tampilan stego key dan stego image pada fitur encode

Berdasarkan gambar 7 diatas, *user* diwajibkan untuk memasukkan *password* untuk menjadi kunci pada *secret message* yang telah dienkripsi tersebut. Selanjutnya, sistem akan melakukan proses steganografi dengan menyisipkan *secret message* yang telah dienkripsi sebelumnya dan *cover image*. Setelah itu maka akan muncul gambar yang telah disisipkan *secret message* dan *user* dapat menyimpan hasil *stego image*. Untuk memisahkan antara *cover image* dan *secret message*, pilih fitur *decode* pada tampilan *home* seperti terlihat pada gambar 5 diatas.



Gambar 8. Tampilan stego image dan stego key pada fitur decode

Sesuai pada tampilan gambar 8 diatas, pada fitur *decode user* diarahkan untuk memasukkan gambar yang berisi *secret message* didalamnya. Setelah mendapatkan gambarnya, sistem akan secara otomatis memisahkan *cover image* dengan *secret message*. Selanjutnya user akan diarahkan untuk memasukkan *password* yang fungsinya untuk mengembalikan *secret message* yang terlihat acak. Dan pesannya akan terlihat seperti pada gambar 9 dibawah ini.

Gambar 9. Tampilan extraction pada fitur decode

Berdasarkan gambar 9 diatas, terlihat *secret message* yang telah dipisahkan dari *cover image*. Isi dari *secret message* ini akan terlihat jelas sesuai dengan yang dikirim oleh si pengenkripsi pesan. Selanjutnya akan dilakukan pengujian pengiriman gambar yang sudah disisipkan pesan steganografi. Pengujian dilakukan dengan tiga *type* gambar dan bmp, jpg, png sebagai *cover image*. Dan tiga type data berformat doc, pdf, dan rar sebagai *secret message*.

Tabel 3. Pengujian ukuran gambar

No	Cover Image	Secret Message	Ukuran Cover Image	Ukuran Secret Message	Ukuran Enkripsi	Status (Berhasil/Gagal)
1	a.bmp	secret-code001.doc	1.020 KB	80 KB	328 KB	Berhasil
2	b.jpg	secret-code002.pdf	24,8 KB	538 KB	734 KB	Berhasil
3	c.png	Secret-code003.rar	377 KB	3,76 KB	409 KB	Berhasil

Tabel 4. Analisa hasil pengiriman, penerimaan, dan mendekripsi stego image

No	Aplikasi	Sent (Berhasil/Gagal)	Receive (Berhasil/Gagal)	Decode (Berhasil/Gagal)
1	Email	Berhasil	Berhasil	Berhasil

2	Messenger	Berhasil	Berhasil	Berhasil
3	Facebook	Berhasil	Berhasil	Gagal
4	Whatsapp	Berhasil	Berhasil	Berhasil
5	Hangouts	Berhasil	Berhasil	Berhasil
6	Bluetooth	Berhasil	Berhasil	Berhasil
7	ShareIt	Berhasil	Berhasil	Berhasil

Setelah proses pengenkripsian, lalu dilakukan pengujian terhadap beberapa aplikasi terlihat pada tabel 4. Aplikasi tersebut diuji dengan cara mengirimkan dan juga penerimaan *cover image* yang bertipe bmp, jpg, png (tabel 3) pada masing-masing aplikasi tersebut. Setelah berhasil dilakukan pengiriman, *cover image* tersebut lalu di decode untuk mengetahui hasil *secret message*.

KESIMPULAN

Berdasarkan dari perancangan dan pengujian pada sistem aplikasi steganografi dengan teknik steganografi *Least Significant Bit* (LSB) dan pengabungan algoritma kriptografi RC4 dan Base64 Encoding, penulis dapat diambil kesimpulan sebagai berikut :

1. Penyisipan secret message pada cover image aman dan tidak terlihat secara kasat mata atau tidak terlihat perbedaannya secara penglihatan mata.
2. Secret message terlihat aman karena telah dienkripsi menggunakan algoritma kriptografi RC4 dan Base64 Encoding yang menjadikan secret message terlihat acak.
3. Gambar yang telah menjadi stego image selanjutnya harus ke proses dekripsi untuk memisahkan antara cover image dan secret message, dan untuk mengembalikkan secret message kebentuk semula.
4. Pengujian aplikasi steganografi dengan fitur encode dan decode berhasil dijalankan. Dan dilanjutkan ke pengiriman, penerimaan ke layanan email, media sosial, maupun aplikasi *messenger*. Yang ternyata ada beberapa pengujian gagal dilakukan karena gambar sudah tidak lagi menjadi stego image.

SARAN

Berdasarkan dari pembahasan yang telah diuraikan sebelumnya, penulis dapat menyimpulkan saran sebagai berikut :

1. Pengembangan terhadap steganografi saat penyembunyian pesan sehingga tidak terlihat dan tidak mengubah ukuran file dan image aslinya.
2. Pengembangan terhadap gambar yang telah disembunyikan dan dienkripsi dapat di *compress* agar ukurannya menjadi lebih kecil sehingga tidak memakan banyak ruang memori.

DAFTAR PUSTAKA

[1] Shih, F. Y., 2008, *Digital Watermaking and Steganography*, CRC Press, New York.

[2] Katz, J., dan Lindell, Y., 2014, *Introduction to Modern Cryptography,* Vol 1, Ed. 2, CRC Press, New York.

[3] [Antonio, H. (2013). Studi Perbandingan enkripsi steganografi dengan menggunakan metode least significant bit dan end of file. JustIN (Jurnal Sistem dan Teknologi Informasi), 1(2), 132-137.

[4] Sitinjak, S., Fauziah, Y., & Juwairiah, J. (2015, July). Aplikasi Kriptografi File Menggunakan Algoritma Blowfish. In Seminar Nasional Informatika (SEMNASIF) (Vol. 1, No. 3).

[5] Sari, J. I., & Sihotang, H. T. (2017). Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB). Jurnal Mantik Penusa, 1(2).

[6] Zebua, T. (2018). Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4.

[7] Putra, M. D. (2018). ENKRIPSI DAN DEKRIPSI GAMBAR DENGAN MENGGUNAKAN PERPADUAN ALGORITMA BASE64 DAN RC4. SEMNASTEKNOMEDIA ONLINE, 6(1), 2-14.

[8] Sun, S., & Guo, Y. (2015). A Novel Image Steganography Based on Contourlet Trans-form and Hill Cipher. Journal of Information Hiding and Multimedia Signal Processing, 6(5), 8891897.

[9] S.Kom, M.T.I, K., Putri, F., & Triyani, H. (2017). Optimalisasi Single Sign On Untuk Meningkatkan Sistem Keamanan OJRS+. Technomedia Journal, 1(2), 61-75.