Aplikasi Kriptografi dan Steganografi Menggunakan Metode Least Significant Bit (LSB) dan One Time Pad (OTP)

Ali Mahmudi, Sandy Nataly Mantja, Achmad Rozikin

Abstract - **With the development of technology, especially in the IT field, the more developed also the current exchange of information using internet technology. Security of information transmitted via the Internet network is a must to maintain the confidentiality and originality of the information. Technology to maintain the security of the information used in this paper is a cryptography and steganography. Application cryptography to secure information on the text, then the information is hidden in digital images. So that only users who have a lock / unlock passwords only, can read the message in greeting such information.**

Keyword : Steganography, cryptography, least significant bit, the one-time pad

Abstrak - Dengan semakin berkembangnya teknologi, khususnya teknologi di bidang IT, maka semakin berkembang pula arus pertukaran informasi dengan menggunakan teknologi internet. Keamanan informasi yang dikirimkan melalui jaringan internet adalah suatu keharusan untuk menjaga kerahasiaan dan keorisinalitas suatu informasi. Teknologi untuk menjaga keamanan informasi yang digunakan pada makalah ini adalah kriptografi dan steganografi. Aplikasi kriptografi untuk mengamankan informasi pada teks, yang kemudian informasi tersebut disembunyikan pada citra digital. Sehingga hanya pengguna yang memiliki kunci/sandi pembuka saja, dapat membaca pesan disalam informasi tersebut.

Keywords: Steganografi, kriptografi, least significant bit, one time pad

I. PENDAHULUAN

1.1 Latar Belakang

Kriptografi terdiri dari kata kripto dan grafi. Kata kripto bermakna rahasia dan grafi bermakna menulis.Kriptografi adalah teknologi untuk menyembunyikan pesan secara rahasia dengan cara mengaburkan pesan tersebut[1]. Kriptografi berguna untuk mengubah suatu informasi menjadi informasi lain, sehingga hanya orang penerima informasi saja yang mengetahui isi dari informasi yang sebenarnya.

Metode kriptografi yang cukup populer adalah metode *One Time Pad* (OTP)[2]. Metode ini menggunakan sebuah kunci atau pad yang digunakan untuk enkripsi dan dekripsi.

Steganografi adalah teknik untuk menyembunyikan suatu informasi dalam suatu informasi lain[3]. Metode steganografi yang cukup popular adalah metode *Least Significant Bit* (LSB). Metode LSB menyembunyikan pesan dengan cara mengganti notasi biner paling kanan, biner dengan nilai penting paling rendah yang disebut *least significant bit,* dengan bit pesan yang ingin ditanamkan[3]. Dengan teknik ini, informasi dapat disembunyikan dengan memodifikasi bit yang paling tidak berpengaruh pada citra.

Penggunaan dua teknik sekaligus, yakni teknik steganografi dan teknik kriptografi, dapat membuat informasi akan semakin sulit dipecahkan. Teknik yang dilakukan adalah dengan melakukan kriptografi pada informasi, kemudian dilanjutkan dengan teknik steganografi untuk menyembunyikan pesan pada citra digital.

Manuscript received March 08, 2016. This work was supported in part by Computer Science Department Institut Teknologi Nasional Malang..

Ali Mahmudi was with Computer Science Departement of ITN, Malang, Indonesia (corresponding author email amahmudi@hotmail.com)

Sandy Nataly Mantja was with Computer Science Department of ITN Malang.

Achmad Rozikin Mantja was with Computer Science Department of ITN Malang.

II. LANDASAN TEORI

2.1 *Kriptografi Metode One Time Pad*

Metode *One Time Pad* (*OTP*) adalah salah satu metode kriptografi yang cukup dikenal. Metode ini[4] ditemukan oleh G. Vernam dan Major Joseph Mauborgne. Prinsip kerja ,metode ini adalah dengan mengkombinasikan masing masing karakter pada *plaintext* dengan satu karakter pada kunci.

Metode *one time pad* yang modern, tidak mengguakan pad kertas, tapi media yang digunakan adalah barisan angka[5]. Jika kunci tersebut benar-benar acak, digunakan hanya sekali, serta terjaga kerahasiannya dengan baik, maka metode penyandian OTP ini sangat kuat dan sangat susah dipecahkan.

Persamaan untuk melakukan proses enkripsi terhadap pesan *P* dengan menggunakan kunci *K* danmenghasilkan cipher *C* adalah

$$Ci = (Pi + Ki) mod\ 26$$

Sedangkan persamaan untuk mendekripsikan adalah

$$Pi = (Ci - Ki) mod\ 26$$

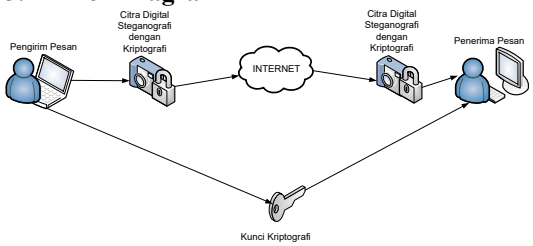
2.2 Steganografi Metode Least Significant Bit

Least significant bit (LSB) adalah bit pada bagian dari barisan data biner (berbasis dua) yang mempunyai nilai paling kecil. Letak LSB di posisi paling kanan dari barisan bit.

Pada steganografi, metode *Least Significant Bit* adalah metode subtitusi pada posisi bit paling kanan pada notasi binary, digantikan dengan bit informasi yang akan diselipkan. Penyembunyian informasi dilakukan dengan mengganti bit-bit paling kecil (LSB) dengan bit-bit informasi yang dirahasiakan[6].

III. PERANCANGAN APLIKASI

3.1 Blok Diagram



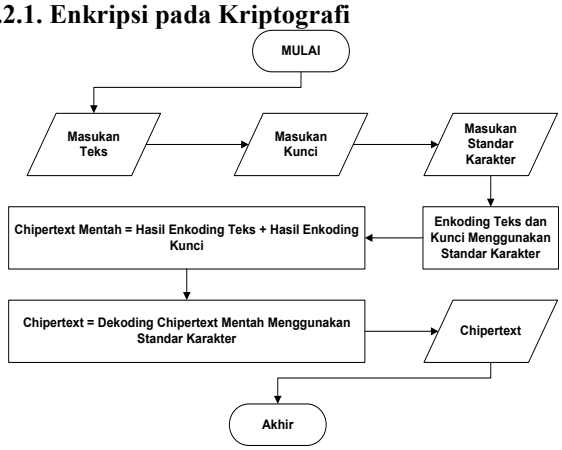
Gambar 1. *Blok Diagram Sistem*

Blok diagram sistem adalah gambaran dari sistem yang akan dibuat. Pada gambar 1 adalah gambaran dari sistem yang akan dibuat. Pada skenario blok diagram sistem ada 2 pelaku yaitu pengirim pesan dan penerima pesan. Pengirim pesan akan menggunakan citra digital yang telah disisipi dengan pesan yang telah terenkripsi dengan menggunakan media internet. Kemudian penerima pesan menerima citra digital yang telah disisipi pesan terenkripsi tersebut. Untuk membuka informasi yang disisipkan oleh pengirim pesan, maka penerima memerlukan kunci kriptografi untuk melakukan dekripsi informasi. Oleh karna itu pengirim pesan dapat mengirimkan kunci kriptografi kepada penerima pesan dengan menggunakan cara yang berbeda bisa melalui protokol lain atau media lain selain internet.

3.2 Diagram Alir

Diagram alir menjelaskan proses berjalannya program, berikut adalah beberapa diagram alir pada aplikasi steganografi dengan kriptografi.

3.2.1. Enkripsi pada Kriptografi

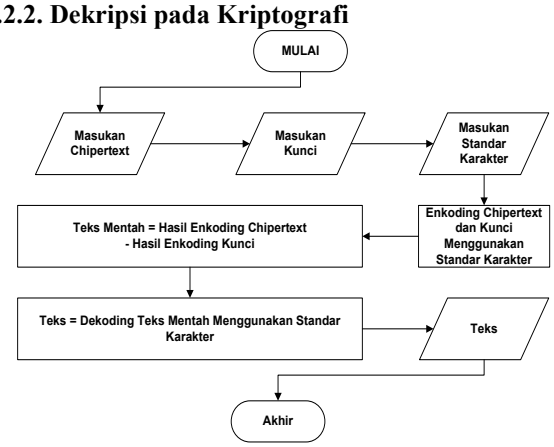


Gambar 2 *Diagram alir proses enkripsi*

Gambar 2 adalah gambar dari diagram alir proses enkripsi data menggunakan metode *One Time Pad.* Penjelasan dari gambar 2 adalah sebagai berikut

1. Pengguna memasukan teks yang akan dienkripsi.
2. Pengguna memasukkan kunci enkripsi.
3. Pengguna memasukkan standar karakter sebagai acuan untuk enkoding dan dekoding pesan atau kunci direpresentasikan menjadi angka.
4. Proses enkoding pesan dan kunci menggunakan standar karakter masukan pengguna. Sehingga pesan dan kunci direpresentasikan sebagai angka.
5. Proses penambahan hasil enkoding kunci dan hasil enkoding pesan sehingga menghasilkan *chipertext* mentah.
6. Melakukan dekoding *chipertext* yang berupa angka desimal menjadi deret karakter menggunakan karakter standar pengguna.
7. Menampilkan hasil berupa *chipertext.*

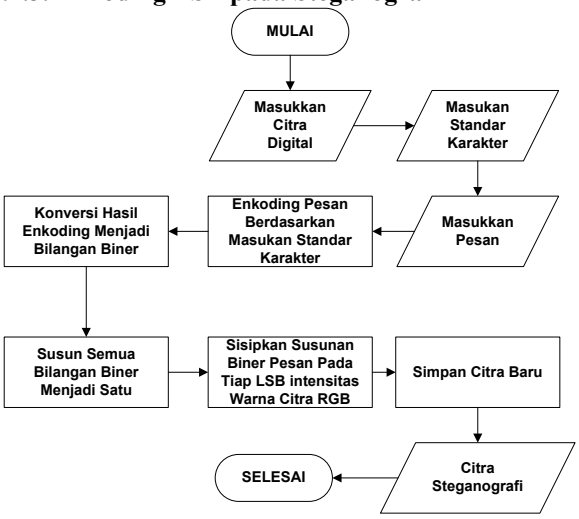
3.2.2. Dekripsi pada Kriptografi



Gambar 3 *Diagram alir proses dekripsi*

Gambar 3 adalah gambar dari diagram alir proses dekripsi data menggunakan metode *One Time Pad.* Diagram alir dekripsi adalah kebalikan dari diagram alir enkripsi.

3.2.3. Enkoding LSB pada Steganografi



Gambar 4. *Diagram alir proses enkoding pesan menggunakan LSB*

Gambar 4 adalah diagram alir proses enkoding pesan ke citra digital menggunakan metode *Least Significant Bit.* Penjelasan dari gambar 4 adalah sebagai berikut

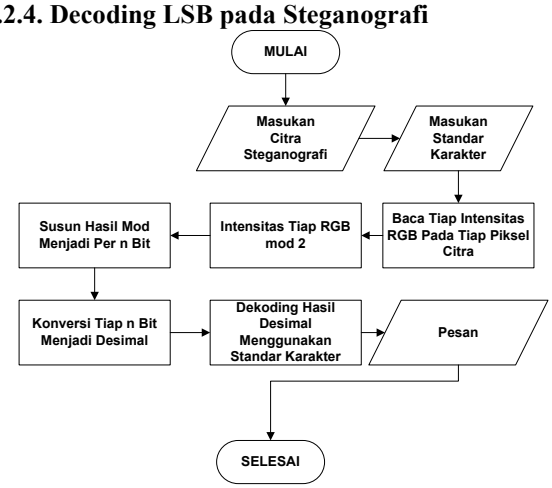
1. Pengguna memasukkan citra digital yang akan disisipi dengan pesan.
2. Pengguna memasukkan standar karakter pengguna yang akan digunakan untuk melakukan proses enkoding dan dekoding deret karakter.
3. Pengguna akan memasukkan pesan yang akan disisipkan pada citra digital.
4. Proses enkoding pesan yang dimasukkan pengguna menggunakan standar karakter pengguna. Yaitu

proses merepresentasikan pesan yang berupa teks atau deretan karakter menjadi deretan angka.

5. Konversi hasil representasi angka enkoding pesan menjadi bilangan biner.
6. Susun semua pesan yang telah dikonversi menjadi biner menjadi satu paket *bit.*
7. Sisipkan tiap *bit* dari paket *bit* yang telah dibuat pada citra digital, hingga deret *bit* terakhir
8. Simpan citra baru yang telah disisipi dengan pesan tiap intensitasnya.
9. Citra steganografi yang telah disisipi pesan.

.

3.2.4. Decoding LSB pada Steganografi



Gambar 5. *Diagram alir proses dekoding pesan menggunakan LSB*

Gambar 5 adalah gambar dari diagram alir proses dekoding pesan yang ada dalam citra digital untuk melihat pesan pada citra digital. Diagram alir decoding adalah kebalikan dari diagram alir encoding.

IV. HASIL

Gambar 6 adalah gambar dari tampilan menu utama aplikasi steganografi dengan kriptografi menggunakan metode *LSB* dan *One Time Pad.* Pada *form* ini terdapat 2 tombol yang akan mengarahkan penggunakan ke 2 fungsi utama aplikasi ini. Yaitu tombol enkripsi dan tombol dekripsi. Tombol enkripsi akan mengarahkan pengguna ke *form* yang digunakan untuk melakukan proses steganografi dengan kriptografi. Sedangkan tombol dekripsi akan mengarahkan pengguna pada *form* yang digunakan untuk membaca pesan stagano yang telah terenkripsi pada citra digital.

Gambar 6. *Menu utama Aplikasi*

Gambar 7 *Enkripsi dan enkoding*

Gambar 7 adalah tampilan awal dari *form* enkripsi. *Form* ini memiliki fungsi untuk melakukan proses steganografi dengan kriptografi. Proses pertama yang harus dilakukan untuk membuat citra steganografi dengan kriptografi adalah dengan memasukkan citra awal yang ingin disisipi pesan.

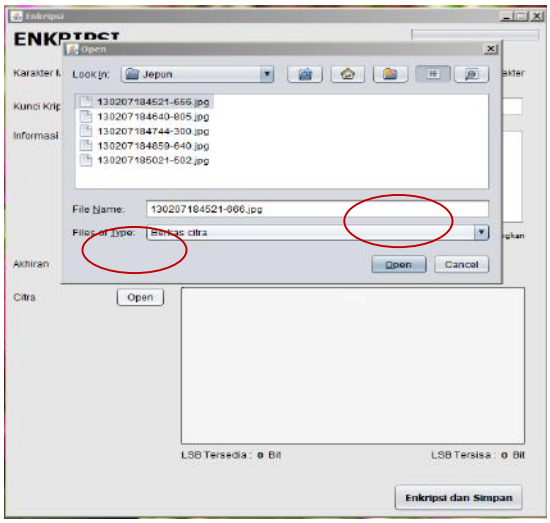
Gambar 8 adalah proses pemilihan citra yang akan disisipi pesan. Pada aplikasi ini, berkas citra yang dapat dipergunakan hanyalah jpg, jpeg, bmp, gif, dan png. Citra yang dipilih, kemudian muncul pada kotak gambar di dalam aplikasi, seperti ditunjukkan dalam gambar 9.

Pada saat citra muncul pada kotak citra maka secara otomatis muncul perhitungan LSB tersedia dan LSB Tersisa. LSB Tersedia adalah jumlah total bit LSB yang dapat disisipi pada citra digital tersebut, yang dihitung dengan persamaan

LSB Tersedia = Width x Height x 3

Proses perkalian dengan 3 dikarenakan pada citra digital terdapat 3 intensitas warna yaitu R, G dan B yang tiap LSB dari intesitas tersebut akan digunakan untuk menyisipkan informasi. LSB Tersisa adalah sisa LSB jika disisipi informasi, yang dihitung dengan persamaan berikut ini

LSB Tersisa = LSB Tersedia –
(Jumlah Karakter * Bit per karakter)



Gambar 8. *Proses membuka citra*

Gambar 9 *Citra yang telah dibuka*

Gambar 9 adalah hasil pemilihan citra. Citra yang dipilih akan muncul pada *image box* aplikasi.

Tiap penambahan informasi berupa teks maka jumlah LSB tersisa akan berkurang. Dikarenakan belum ada informasi yang diketik pada *text area* informasi makan jumlah LSB tersedia sama dengan LSB tersisa, namun ketika adalah perubahan informasi penambahan atau pengurangan maka jumlah LSB tersisa akan berubah.

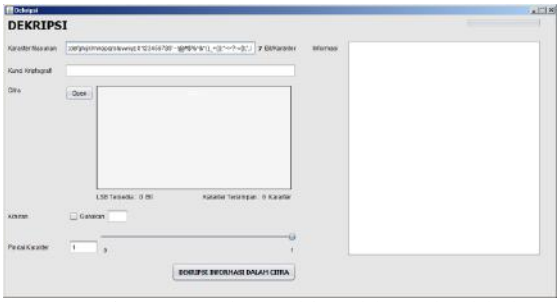
Gambar 10. *Menentukan standar karakter dan kunci kriptografi*

Gambar 10 menunjukkan proses pengguna menentukan karakter masukan dan kunci kriptografi. Karakter masukkan digunakan untuk melakukan proses enkoding dan dekoding dari informasi ke dalam bentuk angka. Sedangkan kunci kriptografi digunakan untuk proses enkripsi informasi. Karakter yang ada pada kunci kriptografi harus ada pada deret karakter masukkan.

Gambar 11 *Menyisipkan informasi berupa teks*

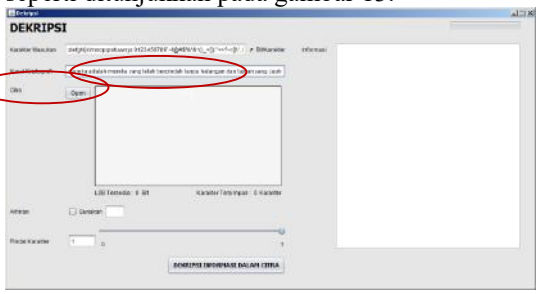
Gambar 11 adalah proses pengguna memasukkan informasi berupa teks yang akan disimpan pada gambar. Teks informasi dapat berupa paragraf yang panjang, namun penggunaan *tab* dan *enter* akan dihilangkan pada saat menyimpanan informasi ke citra.

Jika informasi ditambahkan, maka akan mengurangi LSB tersedia. LSB tersedia mengindikasikan jumlah sisa LSB yang masih dapat digunakan setelah informasi ditambahkan. Jika nilai LSB Tersisa menunjukan nilai kurang dari 0 maka informasi telah memenuhi jumlah LSB.



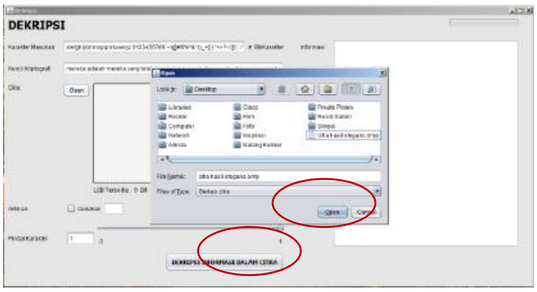
Gambar 12 *Tampilan awal form dekripsi dan dekoding*

Gambar 12 adalah tampilan awal dari menu *form* dekripsi dan dekoding. Proses awal yang harus dilakukan untuk melakukan dekripsi dan decoding adalah memasukkan karakter masukan dan kunci steganografi, seperti ditunjukkan pada gambar 13.

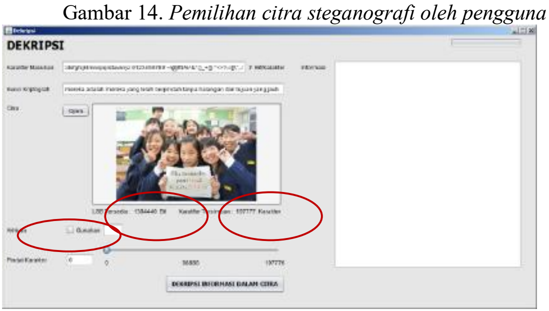


Gambar 13 *Penentuan kunci kriptografi dan karakter masukan*

Langkah selanjutnya adalah memilih citra steganografi, seperti ditunjukkan gambar 14 dan 15.



Gambar 14. *Pemilihan citra steganografi oleh pengguna*



Gambar 15 *Tampilan setelah pemilihan gambar*

Selanjutnya pengguna dapat menentukan jumlah karkater yang ingin dipindai dari citra digital tersebut. Semakin banyak jumlah karakter yang dipindai maka proses dekoding dan dekripsi akan semakin lama. Gambar 16 adalah hasil proses dekoding dan dekripsi informasi dalam citra tanpa menggunakan akhiran.

Gambar 16. *Hasil proses dekripsi informasi dalam citra*

V. PENGUJIAN

Pengujian dilakukan untuk menguji aplikasi yang telah dibuat dan menguji keluaran citra digital yang telah diproses steganografi dengan kriptografi.

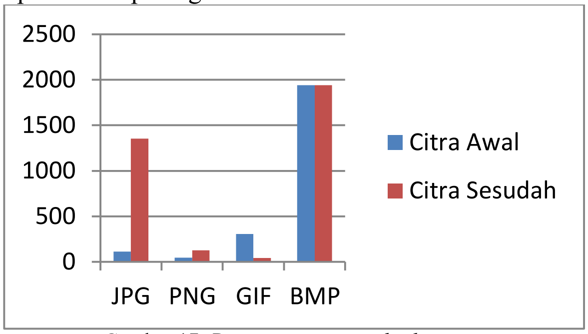
5.1. Pengujian Steganografi

Proses pengujian steganografi digunakan untuk menguji hasil citra digital yang telah disisipi dengan informasi yang terenkripsi dengan menggunakan proses steganografi *LSB.*

Tabel dibawah ini adalah tabel perbandingan hasil ukuran citra sebelum dan sesudah disisipi dengan informasi steganografi.

Nama Citra	Ukuran Sebelum	Ukuran Sesudah	Stegano
jepang.jpg	113 Kb	1,354 Mb	Ya
ranger_belato.png	48 Kb	126 Kb	Tidak
alam.gif	306 Kb	42 Kb	Tidak
belato_bg.bmp	1,94 Mb	1,94 Mb	Ya

Dari hasil pengujian tersebut, dapat diketahui bahwa beberapa citra tersebut tidak dapat dibaca kembali pesan yang disisipkan. Hal ini dikarenakan perbedaan format citra. Format cita yang masih dapat dibaca informasinya adalah JPG dan BMP sedangkan format citra PNG dan GIF tidak dapat lagi membaca informasi yang disisipkan. Grafik perubahan ukuran citra digital dapat dilihat pada gambar 17.



Gambar 17. *Diagram pengujian berkas citra*

5.2. Pengujian Kriptografi

Pengujian ini dilakukan untuk menguji proses kriptografi pada aplikasi yang telah dibut. Pada proses kriptografi ini, pertama-tama kita akan mendefinisikan masukan yaitu sebagai berikut.

No	Kunci Kriptografi	Informasi
1	aaaaaaaaaa	1234567890123456789012345678901234567890123456789012345678900
2	1234567890	abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz
3	abcdefghij	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
4	xxxxxxxxxx	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
5	aaaaaaaaaa	cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc

Kemudian informasi dan kunci tersebut kita enkripsi dan akan menghasilkan *chipertext.*

No	Kunci Kriptografi	Chipertext
1	aaaaaaaaaa	123456789012345678901234567890123456789012345678901234567890 01234567890
2	1234567890	13579~@$^9~@$^*)+}:*)+}:<?79~3579~@$^*)@$^*)+}:<?+}:3579~@$79~@$^*)+}^*)+}:<?=
3	abcdefghij	abcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghijabcdefghij

4	xxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxx xxxxxxxx
5	aaaaaaaaaa	ccccccccccccccccccccccccc ccccccccccccccccccccccccc ccccccccccccccccccccccccc ccccccccccccccccccccccccc ccccccccccccccccc

Pada tabel diatas dapat diketahui bahwa hasil *chipertext* akan menghasilkan deretan yang menyerupai informasi awal jika menggunakan kunci deretan "a" sebanyak 10 kali. Sedangkan pada informasi yang menggunakan kunci deretan angka, dapat menghasilkan *chipertext* yang tidak menyerupai informasi awal.

Pengujian ini membutikan bahwa, kekuatan dari kriptografi dengan menggunakan metode OTP adalah pada keacakan kunci. Semakin acak kunci, maka semakin baik metode kriptografi ini untuk mengacak informasi. Panjang kunci pada kriptografi metode OTP dapat disesuaikan dengan jumlah informasi yang dimasukkan sehingga probabilitas terbentuknya huruf akan semakin banyak.

VI. PENUTUP

6.1 Kesimpulan

Berdasarkan hasil pembuatan dan pengujian aplikasi steganografi dengan kriptografi dengan menggunakan metode OTP dan LSB. Dapat ditarik kesimpulan sebagai berikut:

1. Pesan yang akan disisipkan pada citra digital dengan metode LSB, terlebih dahulu akan di enkripsi dengan metode OTP.
2. Enkripsi metode OTP dilakukan dengan menambahkan informasi dengan kunci kriptografi. Namun terlebih dahulu tiap karakter informasi dan tiap karakter kunci kriptografi direpresentasikan sebagai angka dengan melakukan proses enkoding.
3. Steganografi LSB pada citra digital dilakukan dengan mengganti tiap bit LSB intensitas RGB citra dengan bit bit pesan yang telah dikonversi menjadi bilangan biner.

6.2 Saran

Berikut ini adalah beberapa saran yang dapat dijadikan bahan pertimbangan dalam pengembangan aplikasi steganografi, yaitu:

1. Penambahan format pesan selain teks yang dapat disisipkan pada citra digital. Dapat berupa berkas teks, document, excel atau berkas lainnya.
2. Penambahan pilihan format gambar saat penyimpanan berkas citra hasil steganografi agar citra dapat disimpan selain menjadi format citra BMP.
3. Penambahan format berkas yang dapat disisipi dengan steganografi. Sehingga tidak hanya citra digital yang dapat disisipi pesan.

DAFTAR PUSTAKA

[1] Christof Paar, dan Jan Pelzl. 2009. *Understanding Cryptography*. Springer Science & Business Media.

[2] Buchmann, Johannes. 2013. *Introduction to Cryptography*. Springer Science & Business Media.

[3] Kipper, Gregory. 2003. *Investigator's Guide to Steganography.* CRC Press.

[4] Duwi Astutik, Amelia. 2010. *ALGORITMA ENKRIPSI ONE TIME PAD UNTUK SISTEM PENGAMANAN ACCESS DATABASE SERVER MENGGUNAKAN BAHASA PEMPROGRAMAN VISUAL BASIC*. Skripsi Sarjana Pada Universitas Negeri Semarang.

[5] Garfinkel, Simson. 1995. *PGP: Pretty Good Privacy*. O'Reilly Media, Inc

[6] Hidayat, Wildan. 2010. *PERLINDUNGAN PESAN RAHASIA PADA CITRA DIGITAL MENGGUNAKAN METODE LEAST SIGNIFICANT BIT STEGANOGRAFI.* Skripsi Sarjana Pada Universitas Sumatra Utara.

ISSN 1978-161X
Volume 8 Nomor 1 Maret 2016

MATICS

Jurnal Ilmu Komputer dan Teknologi Informasi

(Journal of Computer Science and Information Technology)

MATICS	Volume 8	Nomor 1	Halaman 1- 43	Maret 2016	ISSN 1978-161X

ISSN 1978-161X
Volume 8 Nomor 1 Maret 2016

MATICS

Jurnal Ilmu Komputer dan Teknologi Informasi
(Journal of Computer Science and Information Technology)

Jurnal MATICS berisi kumpulan publikasi ilmiah yang dihasilkan dari aktifitas penelitian di bidang Teknik Informatika. Jurnal ini terbit dua kali setahun, yaitu pada bulan Maret dan September, dan diterbitkan oleh Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang.

Alamat Redaksi *(Editorial Office)*
Jurusan Teknik Informatika
Fakultas Sains dan Teknologi, Universitas Islam Negeri (UIN) Maulana Malik Ibrahim
Jl. Gajayana 50 Malang 65144 – Indonesia

ISSN 1978-161X
Volume 8 Nomor 1 Maret 2016

MATICS

Jurnal Ilmu Komputer dan Teknologi Informasi
(Journal of Computer Science and Information Technology)

DAFTAR ISI