



ANALISIS KEAMANAN PESAN MENGGUNAKAN METODE *STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB)*

Andrian Kaspari

Program Studi Teknik Informatika,
Fakultas Teknik,
Universitas Islam Kuantan Singingi, Indonesia
Jl. Gatot Subroto KM. 7 Kebun Nenas, Desa Jake, Kab. Kuantan Singingi
E-mail : andriankaspari@gmail.com

ABSTRAK

Seiring perkembangan zaman, komputer berubah menjadi sebuah alat yang dapat mempermudah segala aktifitas manusia. Untuk dapat menjadi manusia yang unggul dimasa kini dan masa yang akan datang, salah satunya adalah mampu menguasai dan mengikuti trend perkembangan teknologi komputer. Pada era informasi digital, *steganografi* merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan. Oleh karna itu, pada penelitian ini penulis akan mengembangkan sistem yang dapat menyembunyikan pesan dalam *ekstensi .txt* didalam file yang lain.

Kata Kunci : Keamanan pesan, Metode *Steganografi, Least Significant Bit*

1. PENDAHULUAN

Seiring perkembangan zaman, komputer berubah menjadi sebuah alat yang dapat mempermudah segala aktifitas manusia. Untuk dapat menjadi manusia yang unggul dimasa kini dan masa yang akan datang, salah satunya adalah mampu menguasai dan mengikuti *trend* perkembangan teknologi komputer. Siapa yang dapat menyangka bahwa teknologi komputer berkembang dengan pesat, dan juga menjadi salah satu bagian yang cukup vital dalam kehidupan sehari-hari. Pada awalnya komputer digunakan layaknya menghitung, karena kata komputer sendiri berasal dari kata "*to compute*" yaitu untuk menghitung. Seiring waktu pun teknologi komputer yang dikembangkan bukan hanya sekedar mesin penghitung tapi juga mesin yang dapat memproses data. Data yang awalnya berjumlah kecil dan algoritma yang sederhana, perlahan semakin besar dan kompleks. Melihat perkembangan itu, jika disadari setiap masa waktu, memiliki *trend* perkembangan teknologi komputer yang berbeda sesuai dengan keadaan masa zaman saat itu. Hal tersebut dikarenakan kemampuan teknologi komputer yang berbeda-beda pula. Komputer pada awalnya adalah sebetuk mesin yang sangat besar. Semakin kompleks kemampuannya, maka semakin besar pula ukuran komputer tersebut. Bahkan mampu mengisi setengah ruangan kamar kita. Pada saat itu aplikasi atau sistem operasi pilihannya hanyalah sedikit dengan kemampuan yang terbatas pula. *Steganografi* merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan suatu informasi. *Steganografi* dapat digolongkan sebagai salah satu bagian dari ilmu komunikasi. Pada era informasi digital, *steganografi* merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan. Oleh karna itu, pada penelitian ini penulis akan



mengembangkan sistem yang dapat menyembunyikan pesan dalam ekstensi .txt didalam file yang lain.

2. METODE PENELITIAN

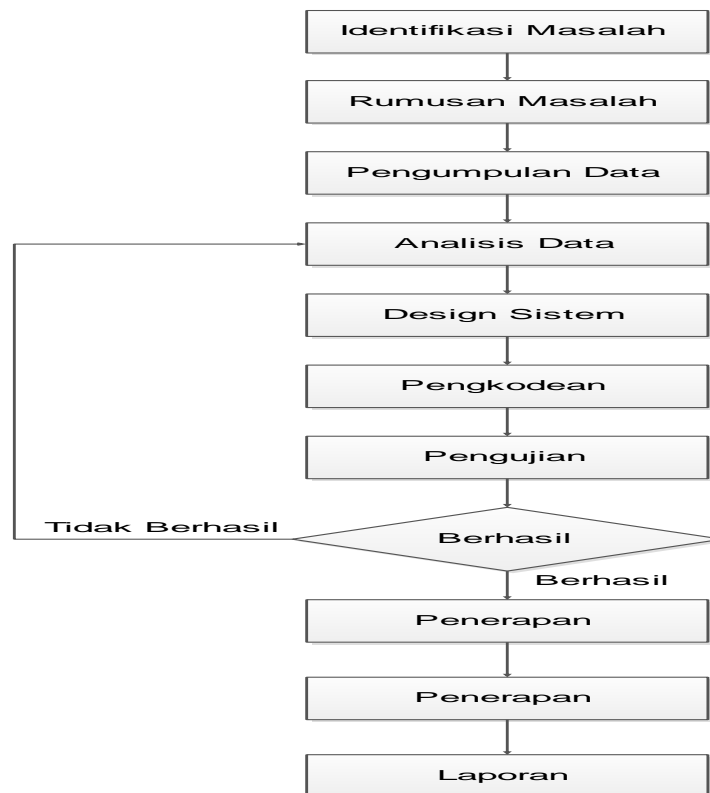
2.1 Teknik Pengumpulan Data

Dalam penulisan penelitian ini penulis melakukan teknik pengumpulan data dengan cara antara lain :

- Observasi, meneliti langsung objek penelitian.
- Wawancara, yaitu penulis melakukan wawancara dengan pihak yang bersangkutan untuk mendapatkan informasi dan data tersebut.
- Studi literature yaitu mendapatkan data dengan cara mencari sumber-sumber penelitian terdahulu seperti didapat dari jurnal, buku-buku dan teori-teori yang berkaitan dengan penelitian yang sedang dilakukan.

2.2 Rancangan Penelitian

Dalam melakukan penelitian ada beberapa tahapan yang dilaksanakan dengan sistematis. Rangkaian tahapan akan diuraikan pada gambar berikut :



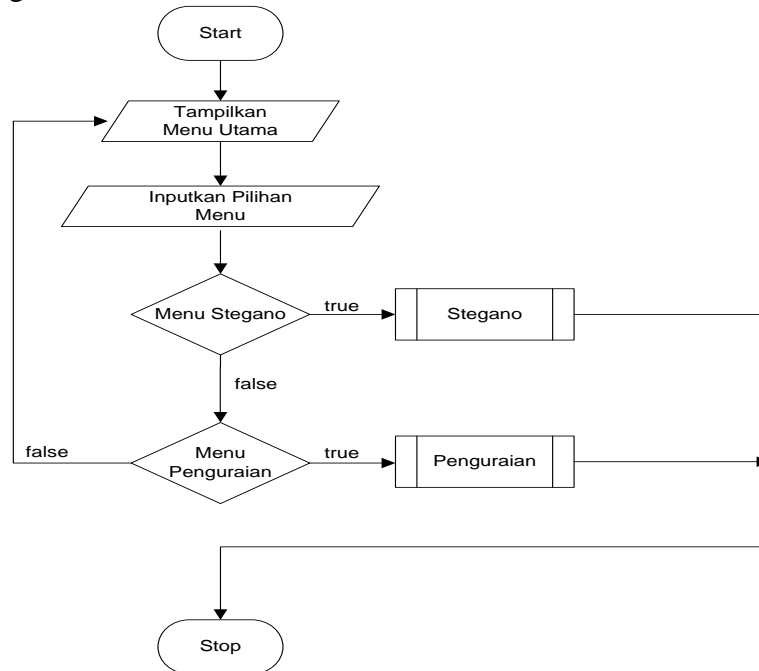
Gambar 1. Rancangan Penelitian

3 HASIL DAN PEMBAHASAN

3.1 Flowchar Program Utama Sistem

Gambar dibawah ini adalah alur program pada sistem yang sedang dikembangkan. Diagram tersebut menjelaskan alur dimulai nya program, proses yang terjadi dalam program,

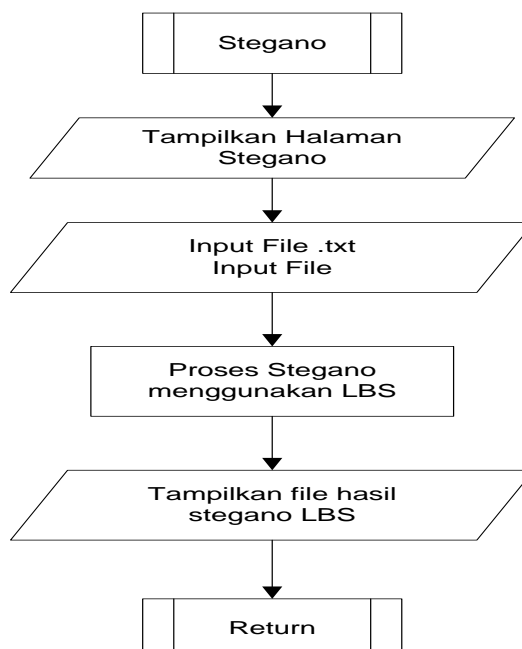
menu yang disediakan program dan hasil yang dikeluarkan program. Untuk lebih jelasnya dapat dilihat pada gambar berikut :



Gambar 2. Flowchart Program Utama Sistem

3.2 Flowchar Program Proses Steganografi (Encode)

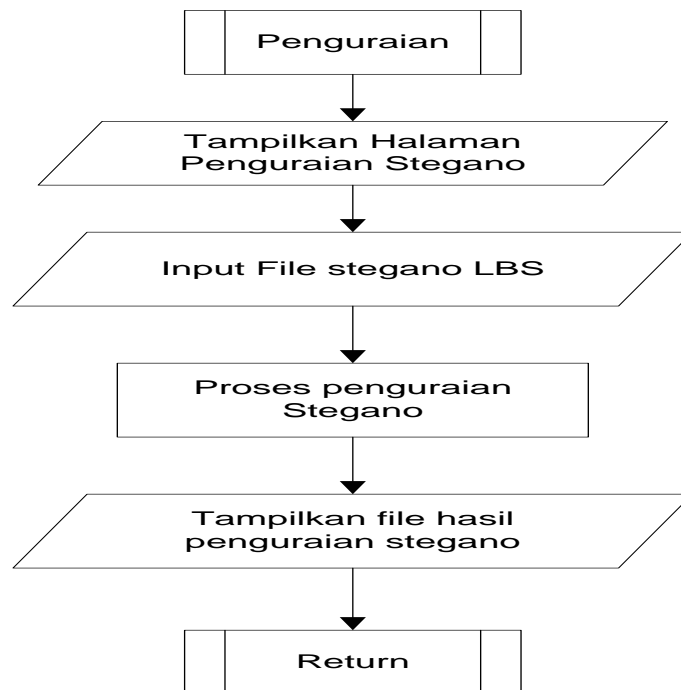
Gambar dibawah ini merupakan uraian alur program pada *flowchar* utama. Diagram ini menjelaskan jalannya sistem yang sedang dikembangkan saat proses *steganografi (Encode)*. Dimana pada proses ini sistem akan menggabungkan pesan dan file tempat pesan tersebut disembunyikan. Proses steganografi ini menggunakan metode LSB pada penerapannya. Agar lebih mudah untuk memahami dapat melihat flowchart steganografi pada gambar berikut :



Gambar 3. Flowchart Program Proses Steganografi (Encode)

3.3 Flowchart Program Penguraian (Decode)

Gambar dibawah ini merupakan penguraian flowchar utama pada proses penguraian pesan (Decode). Pada proses ini dijelaskan bahwa pesan yang telah digabungkan dengan file lain (Encode) dapat diuraikan kembali sehingga pesan yang disembunyikan didalam file lain dapat terbaca. Untuk lebih jelasnya dapat melihat diagram berikut ini:



Gambar 4. Flowchart Program Penguraian File Steganografi (Decode)

Berikut merupakan tabel pengujian sistem yang dilakukan pada aplikasi yang sedang dikembangkan.

3.4 Pengujian Sistem

Tabel 1. Pengujian Pada Halaman Data Encode

No	Jenis Pengujian	Yang Diharapkan	Keterangan
1.	Menguji form dengan mengosongkan form dan menekan tombol buton	Sistem memperingatkan untuk mengisi form kosong	Berhasil
2.	Menekan tombol <i>Choose File</i>	Sistem menampilkan menu dialog untuk mencari file yang akan di upload.	Berhasil
3.	Button Reset	Sistem secara otomatis menghapus semua isi form.	Berhasil
4.	Tombol <i>Encode</i>	Sistem melanjutkan proses encode menggunakan LSB	Berhasil
5.	Tombol <i>Save</i>	Sistem menyimpan data hasil <i>Encode</i> .	Berhasil



Tabel 2. Pengujian Pada Halaman *Decode*

No	Jenis Pengujian	Yang Diharapkan	Keterangan
1.	Menguji form dengan mengosongkan form dan menekan tombol buton	Sistem memperingatkan untuk mengisi form kosong.	Berhasil
2.	Button Reset	Sistem secara otomatis menghapus semua isi form.	Berhasil
3.	Button Decode	Sistem memproses penguraian encode dan menampilkan pesan dibalik gambar	Berhasil

Dari pengujian *black box* yang telah dilakukan pada sistem yang sedang dikembangkan, maka diperoleh kesimpulan bahwa sistem telah lulus uji *black box* karena semua hasil yang diharapkan dapat terpenuhi oleh sistem.

3.5 Tampilan Hasil Program

Pada tahap ini penulis mengimplementasikan hasil rancangan yang telah dibuat. Implementasi merupakan proses pembuatan perangkat lunak dari tahap perancangan atau desain ke tahap pengkodean yang akan menghasilkan perangkat lunak yang telah dirancang sebelumnya. Adapun hasil dari implementasi dari aplikasi yang telah dikembangkan adalah sebagai berikut:

1) Tampilan Halaman *Input Data Encode*

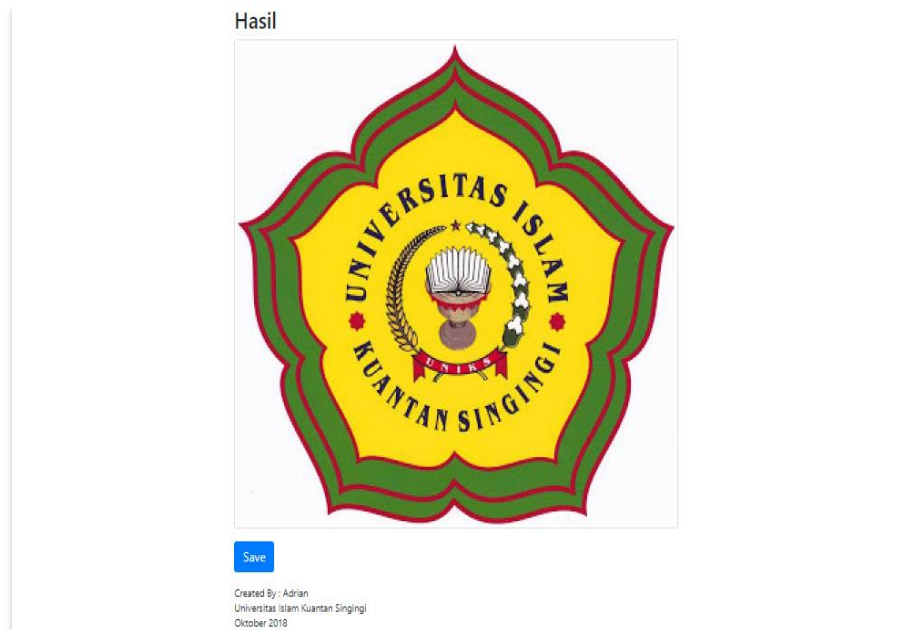
Berikut ini adalah tampilan menu *Input Data Encode* pada aplikasi yang sedang dikembangkan:

Gambar 5. Tampilan Halaman *Input Data Encode*



2) Tampilan Halaman Hasil *Encode*

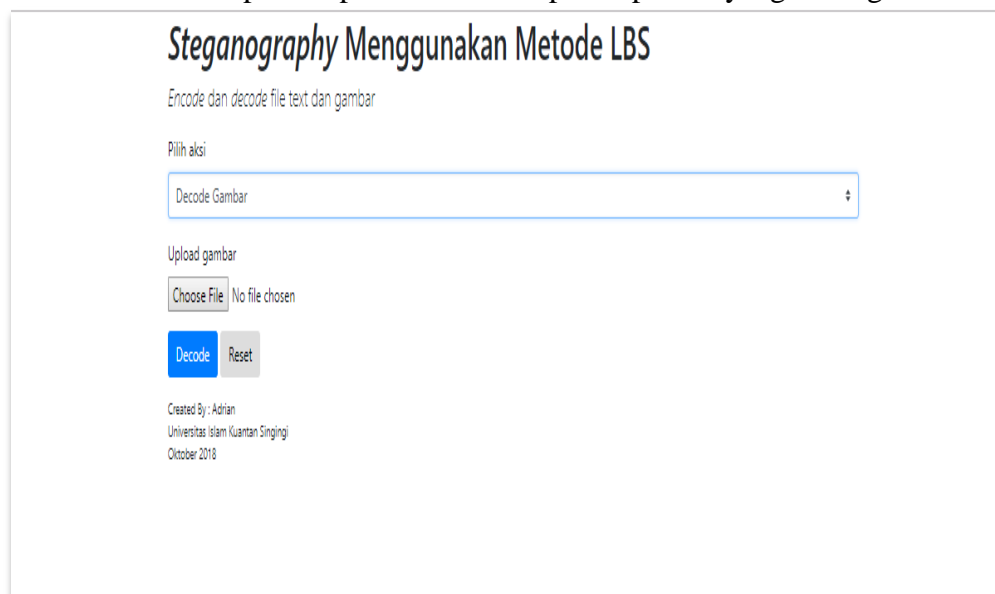
Berikut ini adalah tampilan halaman hasil *encode* pada aplikasi yang sedang dikembangkan:



Gambar 6. Tampilan Halaman Hasil Encode

3) Tampilan Halaman Input Data *Decode*

Berikut ini adalah tampilan input data *decode* pada aplikasi yang sedang dikembangkan :



Gambar 7. Tampilan Halaman Decode

4) Tampilan Halaman Hasil *Decode*

Berikut ini adalah tampilan halaman hasil *decode* pada aplikasi yang sedang dikembangkan:



Gambar 8. Tampilan Halaman Hasil *Decode*

4 PENUTUP

4.1 Kesimpulan

Berdasarkan dari uraian yang telah disampaikan diatas, maka penulis mengambil kesimpulan sebagai berikut:

1. Telah berhasil membangun sistem analisa keamanan data menggunakan *steganografi* dengan metode LSB.
2. Metode LSB efektif untuk menyembunyikan pesan teks kedalam file gambar dengan ekstensi *.jpg*.
3. Ukuran gambar hasil encode menggunakan metode *steganografi* berubah menjadi lebih besar dari gambar dasar.

DAFTAR PUSTAKA

Agung Suryahadiningrat Kusumanegara, Bambang Hidayat, Nur Andini. "Analisis Keamanan Pesan Menggunakan Teknik Steganografi Modified Enhanced Lsb Dan Four Neighbors Dengan Teknik Kriptografi Chaining Hill Cipher". ISSN 2085-4218.

Anggraini, Y; Sakti, D.V.S.Y., 2014. "Penerapan steganografi metode End Of File (EOF) dan Enkripsi metode Data Encryption Standard (DES) pada aplikasi pengamanan data gambar berbasis java programming". Konferensi Nasional Sistem Informasi 2014 (KNSI 2014). STMIK Dipanegara Makassar, 27 Februari – 01 Maret 2014.

Aryasanti, A., & Hardjianto, M. (2014). "Model Pengamanan Berkas Bank Soal Dengan Metode Steganografi LSB dan Kompresi. Jurnal TICOM", II (2), 127-135.

B. S. Champakamala, K. Padmini, and D. K. Radhika, "Least Significant Bit algorithm for image steganography" International journal of Advanced Computer Technology, vol. 3, no. 4, pp. 34-38, 2014.



- Bonifacius Vicky Indriyono."Implementasi Sistem Keamanan File Dengan Metode Steganografi Eof Dan Enkripsi Caesar Cipher". Vol. 06 No. 01 (2016) 1–16.
- David, A. Murtado, Utin Kasma. "Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode Least Significant Bit". Vol. 2, No. 1, Januari 2012.
- Department of Computer & Information System Engineering, 2012. "Practical Workbook: Information Theory". 4th edition. Karachi, Pakistan: NED University of Engineering & Technology".
- E. R. Hidayat, dan K. Hastuti. "Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak secara Kuantitatif dan Visual" Jurnal Techno.Com, vol. 12, no. 3, pp. 157-167 , 2013.
- F. A. Antika, A. B. Purba, dan U. T. Lenggana. "Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit 3-3-2 Bit Berbasis Android" Skripsi, STMIK Kharisma Karawang, 2016.
- Hernawandra, S. Supriyadi, and U. T. Lenggana, "Aplikasi Steganografi Menggunakan LSB 4 Bit Sisipan dengan Kombinasi Algoritme Substitusi dan Vigenere Berbasis Android" Jurnal Teknologi dan Sistem Komputer, vol. 6, no. 2, Apr. 2018. doi: 10.14710/jtsiskom.6.2.2018.44-50, [Online].
- M. F. Syawal, D. C. Fikriansyah, dan N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher dan Metode LSB," Jurnal TICom, vol. 4, no. 3, pp. 91-99, 2016.
- Seftyanto, D.; Apriani, M.; Haryanto, T., 2012. "Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi". Seminar Nasional Matematika dan Pendidikan Matematika. Jurusan Pendidikan Matematika FMIPA UNY 10 November 2012. Yogyakarta.
- Sembiring, S., 2013. "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File". Pelita Informatika Budi Darma, IV (2). ISSN : 2301-9425.
- Wandani, H.; Budiman, M.A; Sharif, A., 2012. "Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem". Jurnal Alkharizimi, 1 (1).
- Wasino; Rahayu, T.P; Setiawan., 2012." Implementasi Steganografi Teknik End Of File Dengan Enkripsi Rijndael. Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012)". Yogyakarta, 10 Maret 2012. ISSN: 2089-9815.
- Wawan Setiawan, Juwairiah, Herry Sofyan,"Aplikasi Keamanan Pesanmenggunakan Algoritma Steganografi Dan Kriptografi". Vol. 8, No. 2, JANUARI 2012: 129 – 140