RANCANG BANGUN IMPLEMENTASI STEGANOGRAFI AUDIO MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB) DENGAN KOMBINASI ALGORITMA *BLOWFISH*

Irtafa Masruri, Mungki Astiningrum

Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang
JL. Soekarno-Hatta No. 9 Malang 65141, Indonesia
irtafamasruri@gmail.com, mungki_astiningrum@polinema.ac.id

Abstrak

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan melalui media jaringan/internet. Teknik kriptografi dan stegano-grafi dapat digunakan untuk memberi perlindungan keamanan pada pesan rahasia. Penggabungan teknik kriptografi algoritma Blowfish yang diintegrasikan ke dalam steganografidengan metode Least Significant Bit(LSB) diharapkan dapat melindungi pesan rahasia.

Penelitian ini bertujuan untuk mengkombinasikan teknik kriptografi Blowfish yang terintegrasi dengan metode steganografi, untuk memberikan proteksi ganda pada pesan rahasia di dalam sebuah audio digital. Hasil dari penelitian ini adalah sebuah aplikasi yang telah berhasil mengkombinasikan kriptografi dan steganografi.

Pada aplikasi ini dapat menyembunyikan file text dan gambar ke dalam audio digital berformat mp3 dan wav. Aplikasi ini dapat di jalankan pada sistem informasi windows. Oleh sebab itu diperlukan pengembangan yang dapat di gunakan di berbagai sistem informasi.

Kata kunci: Blowfish, Least Significant Bit, Audio, Kriptografi, Steganografi

1. Pendahuluan

Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu.

Turut berkembang pula kejahatan yang memanfaatkan teknologi dengan berbagai teknik. Tanpa adanya jaminan keamanan, maka orang lain dapat dengan mudah mendapatkan informasi yang dikirimkan melalui jaringan/internet. Dengan demikian keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran informasi melalui jaringan/internet.

Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan dari orang yang tidak berkepentingan. Teknik steganografi dan kriptografi termasuk dalam teknik pengamanan informasi. Kriptografi akan menyamarkan pesan atau informasi dalam bentuk text bermakna menjadi text yang tidak bermakna. Sedangkan steganografi tidak menyamarkan informasi melainkan menyembunyikannya ke dalam media yang tidak dapat di duga oleh orang biasa, sehingga tidak menimbulkan suatu kecurigaan kepada orang yang melihatnya.

Keamanan dari suatu teknik kriptografi (cryptosystem) biasanya terletak pada kerahasaiaan pada beberapa kunci yang dijadikan sebagai ciphertext pada algoritma kriptografi tersebut. Meskipun mempunyai kemungkinan jangkauan kunci yang sangat luas tetapi keberadaan informasinya masih terlihat, hal ini menyebabkan kemungkinan informasi dipecahkan menjadi semakin besar.

Keamanan dari suatu teknik steganografi biasanya terletak pada penyembunyian informasi rahasia ke dalam informasi lain dengan tingkat perubahan informasi yang telah disisipi oleh informasi rahasia sangat sedikit, sehingga pesan rahasia benar benar tersamarkan. Tetapi jika informasi yang telah disisipi pesan rahasia diketahui maka pesan rahasia akan dapat dengan mudah terbaca.

Dalam hal ini penulis mencoba menerapkan teknik kriptografi dan digabungkan dengan teknik steganografi untuk memberi keamanan lebih pada informasi rahasia. Teknik kriptografi menggunakan algoritma blowfish.

2. Landasan Teori

2.1 Steganografi

Steganografi adalah seni atau ilmu untuk menyamarkan sebuah pesan/data rahasia ke dalam data atau media *digital* yang tampaknya biasa saja, sehingga keberadaan pesan rahasia itu sulit diketahui (Eko Arryawan, 2010). Informasi rahasia yang disisipkan dapat berupa teks, gambar, dan file lainnya.

Steganografi berasal dari Bahasa Yunani yaitu "*steganos*" yang artinya tulisan tersembunyi. Steganografi bukan hal yang baru dan sudah dikenal sejak zaman Romawi dan Yunani kuno. Teknik ini

diterapkan pada zaman dahulu dengan cara menuliskan pesan di kepala budak lalu menunggu rambut dari budak itu tumbuh sehingga cukup untuk menutupi psan yang tertulis di kepalanya. Setelah itu budak itu dikirim kepada orang yang dituju dimana rambutnya akan dicukur sehingga pesan itu dapat terlihat dan dibaca oleh penerima pesan.

2.1.1 Terminologi Steganografi

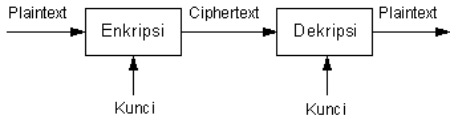
- *Embedding Data*
  Data embedded adalah data/pesan rahasia yang disembunyikan dalam suatu media digital.
- *Covertext atau cover-object*
  Media digital yang digunakan untuk menyembunyikan embedded data.
- *Stegotext atau stego-object*
  Media digital yang sudah disisipi oleh embedded data.

2.2 *Audio* Steganografi

Cara untuk mengaplikasikan steganografi pada file audio terdiri dari beberapa cara yang lazim digunakan, antara lain dengan cara mengganti atau menambahkan bit.

2.3 Kriptografi

Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula.



Gambar 1. Skema Enkripsi dan Dekripsi

2.4 *Blowfish*

Algoritma Blowfish merupakan algoritma kriptografi modern kunci simetris berbentuk cipher block yang berarti selama proses enkripsi dan dekripsi, Blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang yaitu 64-bit dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok. Algoritma yang dibangun ini dapat mengenkripsi file (plaintext) dalam bentuk teks, gambar, suara, video, juga archieve seperti .zip dan .rar.

Algoritma Blowfish terdiri atas dua bagian, yaitu ekspansi kunci dan enkripsi data :

- **Ekspansi Kunci**

Tentukan nilai dari S-box dan P-aray. Setelah itu lakukan Ekspansi kunci, yaitu XOR-kan P1 dengan 32-bit awal kunci, XOR-kan P2 dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR-kan dengan bit-bit kunci. Atau jika disimbolkan :

P1 = P1 $\oplus$ K1, P2 = P2 $\oplus$ K2, P3 = P3 $\oplus$ K3, . . . P14 = P14 $\oplus$ K14, P15 = P15 $\oplus$ K1, . . . P18 = P18 $\oplus$ K4. Lakukan hal yang sama pada ke 4 buah *S-box*.

- **Enkripsi Data**

Bagi 64-bit data masukan menjadi dua bagian masing-masing terdiri dari 32-bit : XL, XR. Kemudian lakukan langkah berikut :

For i = 1 to 16:
XL = XL Xor P(i)
XR = F(XL) Xor XR
Tukar XL dan XR

Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir. Kemudian lakukan langkah berikut:

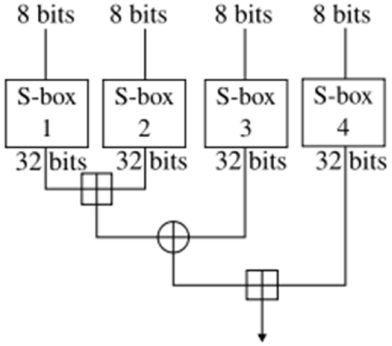
XR = XR Xor P(17)
XL = XL Xor P(18)

Kemudian satukan kembali XL dan XR. Ulang proses diatas sampai data ter-enkripsi seluruhnya.

Pada proses di atas telah dituliskan adanya fungsi F(XL). Fungsi F(XL) adalah bagi XL menjadi empat bagian a, b, c, d masing-masing terdiri dari 8-bit. Kemudian masukkan ke dalam rumus berikut:

$F(XL) = ((S1,a + S2,b \bmod 2^{32}) \text{ XOR } S3,c) + S4,d \bmod 2^{32}$

Untuk lebih memahami fungsi F, prosesnya dapat di lihat pada gambar berikut :



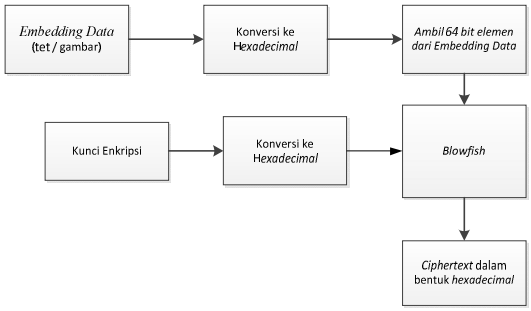
Gambar 2. Fungsi F dalam *blowfish*

3. Perancangan Sistem

3.1 Gambara Umum Sistem

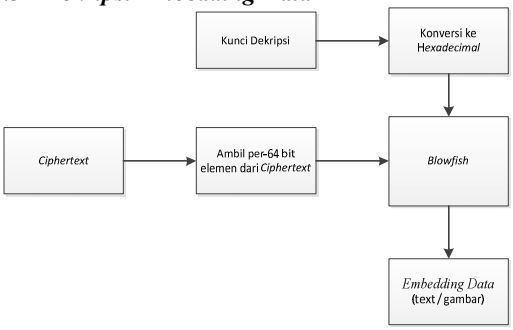
Gambar 3. Gambaran Umum Sistem

3.2 *Enkripsi Embedding Data*



Gambar 4. Diagram block enkripsi *Embedding Data*

3.3 *Dekripsi Embedding Data*



Gambar 5. Diagram block deskripsi *Embedding Data*

3.4 Penerapan Blowfish

Pada bagian ini akan membahas perancangan untuk pengimplementasian metode ini ke dalam sistem sebagai berikut:

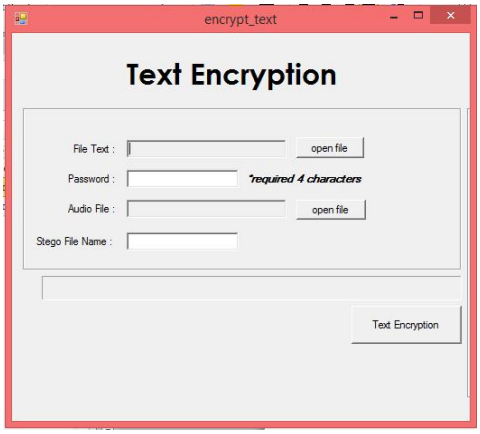
Gambar 6. Tahapan Enkripsi Input Data pada Blowfish

4. Implementasi

4.1 Implementasi Program

Implementasi program yaitu tampilan hasil dari penerapan sistem yang telah dibuat, sesuai dengan perancangan yang telah dilakukan dengan hasil berupa tampilan aplikasi sebagi berikut:

Implementasi Sistem Informasi *Steganografi* ini dilakukan menggunakan bahasa pemrograman VB.net.



Gambar 7. Halaman Enkripsi *text*

Gambar 8. Halaman Enkripsi Image

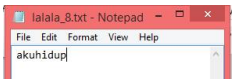
Kedua gambar diatas adalah halaman untuk melakukan proses enkripsi sejaligus penyisipan ke dalam *cover-object*. Perbedaannya adalah antara file yang disisipkan, text dan gambar.

5. Pengujian dan Pembahasan

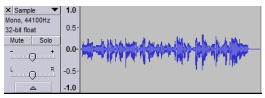
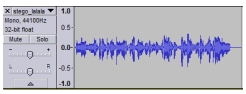
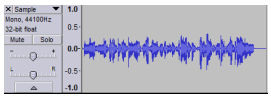
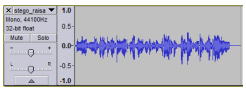
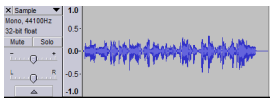
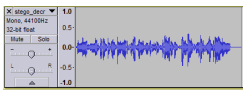
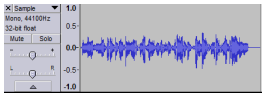
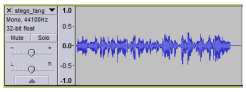
5.1 Pengujian Kesesuaian Data

Pengujian terhadap kesesuaian data dilakukan untuk mengetahui apakah *embedding data* yang berhasil di ambil dari *stego-audio* bersesuaian dengan *embedding data* yang disisipkan. Kriteria pengujian adalah *embedding data* yang berhasil di ambil dari *stego-audio* sesuai dengan *embedding data* yang disisipkan.

Tabel 1. *Embedding Data*

Cover-audio	*Stego-audio*	*embedding data*
sample.wav (00:00:20)	stego_lalala_8_xx.mp3(00:00:20)	
sample.wav (00:00:20)	stego_raisa_lala_xx.mp3 (00:00:20)	
sample.wav (00:00:20)	stego_decrypt_png_xx.mp3 (00:00:20)	
sample.wav (00:00:20)	stego_tangan_bmp_xx.mp3 (00:00:20)	

Tabel 2. Pengujian Perubahan *Cover-audio*

Cover-audio	*Stego-audio*
 sample.wav (00:00:20)	 stego_lalala_8_xx.mp3 (00:00:20)
 sample.wav (00:00:20)	 stego_raisa_lala_xx.mp3 (00:00:20)
 sample.wav (00:00:20)	 stego_decrypt_png_xx.mp3 (00:00:20)
 sample.wav (00:00:20)	 stego_tangan_bmp_xx.mp3 (00:00:20)

6. Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkan pembahasan pada bab 1 hingga 6 dapat ditarik beberapa kesimpulan, yaitu:

a) Hasil pengujian menunjukkan bahwa dari pengujian kesesuaian data yang telah dilakukan, dapat di tarik kesimpulan bahwa data/pesan rahasia yang disisipkan ke dalam cover-audio¬ dapat diambil kembali tanpa terjadi kerusakan pada data.

b) Hasil pengujian menunjukkan bahwa perubahan cover-audio¬ sebelum dan sesudah di lakukan penyisipan sulit di deteksi dari bentuk gelombang frekuensinya.

c) Hasil pengujian menunjukkan bahwa perubahan cover-audio¬ sebelum dan sesudah di lakukan penyisipan dapat terdeteksi dengan cara membandingakan bentuk hexadecimal dari cover-audio sebelum dan sesudah di lakukan penyisipan.

d) Aplikasi ini telah berhasil menerapkan metode kriptografi menggunakan algoritma Blowfish untuk memberi keamanan lebih kepada data/pesan rahasia sebelum disisipkan.

6.2 Saran

Berdasarkan penelitian ini, ada beberapa hal yang disarankan, yaitu:

a) Aplikasi ini dapat dikembangkan lagi dengan menambahkan format data/ekstensi dari file yang akan disisipkan ke dalam cover-audio. Sebagai contoh dengan menambahkan file formated text seperti *.Docx, *.Doc, *.XML, dan sebagainya.

b) Pada penelitian ini, embedding data disisipkan dengan cara berurutan. Untuk menambah keamanan data dari serangan, pada penelitian selanjutnya diharapkan penyisipan dilakukan secara acak.

Daftar Pustaka:

Basuki Rakhmat, 2010, Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4, Universitas PGRI Yogyakarta.

Suriski Sitinjak, Yuli Fauziah, Juwairiah, 2010, Aplikasi Kriptografi File Menggunakan Algoritma Blowfish, UPN "Veteran" Yogyakarta

Jhoni Verlando Purba, Marihat Situmorang, Dedy Arisandi, 2012, Implementasi Steganografi Pesan Text Ke Dalam File Sound(.WAV) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb), Universitas Sumatera Utara

David Ireland, 2002, Blowfish : a visual basic version, di management service, Sidney-

Australia. http://www.di-mgt.com.au/crypto.html , [24 juli 2002]
Gregory Kipper , 2004, Investigator's Guide to Steganography, CRC Press.
Christof Paar, Jan Pelzl, 2009, Understanding Cryptography : a textbook for student and practitioners, Springer Science & Business Media.