

Pengamanan Pesan pada File Audio dengan Metode *LSB* dan
Blowfish

*Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika*



Oleh :

Ahmad Rizky Fauzan
NIM : 09021281722042

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN SKRIPSI

Pengamanan Pesan pada File Audio dengan Metode *LSB* dan *Blowfish*

Oleh :

Ahmad Rizky Fauzan
NIM : 09021281722042

Palembang, 22 Desember 2021

Pembimbing I



Alfarissi, M.Comp.Sc.
NIP. 198512152014041001

Pembimbing II



M. Naufal Rachmatullah, M.T.
NIP. 1671060112920006



Mengetahui,
Ketua Jurusan Teknik Informatika,
Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Rabu tanggal 5 Januari 2022 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Ahmad Rizky Pruzan
NIM : 09021281722042
Judul : Pengamanan Pesan pada File Audio dengan Metode RSA dan Blowfish

1. Ketua

Dr. Abdiansah, S.Kom, M.Cs.
NIP. 198410012009121005

2. Penguji I

Osyari Argalani, M.T.
NIP. 198806282018031001

3. Penguji II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

4. Pembimbing I

Alfarissi, M.Comp.Sc.
NIP. 198512152014041001

5. Pembimbing II

M. Naufal Rachmatullah, M.T.
NIP. 1671060112920006



HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Ahmad Rizky Fauzan
NIM : 09021281722042
Program Studi : Teknik Informatika Reguler
Judul Skripsi : Pengamanan Pesan pada File Audio dengan Metode
LSB dan Blowfish

Hasil Pengecekan Software *iThenticate / Turnitin* : 11%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, 24 Januari 2022



(Ahmad Rizky Fauzan)
NIM. 09021281722042

MOTTO DAN PERSEMPAHAN

Motto:

- “Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya.” – QS Al Baqarah 286
- “Jika Allah menolong kamu, maka tidak ada yang dapat mengalahkanmu, tetapi jika Allah membiarkan kamu (tidak memberi pertolongan), maka siapa yang dapat menolongmu setelah itu? Karena itu, hendaklah kepada Allah saja orang-orang mukmin bertawakal.” – QS Ali Imran 160
- “Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum, sebelum mereka mengubah keadaan diri mereka sendiri.” – QS Ar Rad 11.

Kupersembahkan karya tulis ini kepada:

- Kedua orang tua tercinta, Bapak Kgs. A. Rahman dan Ibu Maya Sopa yang selalu memberikan doa dan motivasi.
- Saudari saya, Sarah Fadhilah yang senantiasa membantu dalam menyelesaikan tugas akhir ini.
- Teman-teman seperjuangan IF Reg 2017

SECURE MESSAGE FILES ON AUDIO FILES USING LSB AND *BLOWFISH*

By:
Ahmad Rizky Fauzan
09021281722042

ABSTRACT

Along with the development of technology, communication can be done in various ways, one of which is digital messages. But often the messages sent do not reach their destination and are obtained by irresponsible parties. This happens because of the lack of security in the file. For this reason, security is needed so that messages cannot be stolen or seen by other parties. There are various ways to secure messages, including Steganography and Cryptography techniques. This study uses a combination of the Least Significant Bit method and the Blowfish algorithm to secure secret messages in audio files. This research will measure encryption and decryption time, analysis of message file size changes after encryption and decryption, and PSNR value of audio files. The result of encryption using blowfish is a change in the size of the message file caused by the size of the message file being less than the block cipher size, so additional bytes are given so that the message size matches the block cipher size. The speed of the encryption and decryption process using the blowfish algorithm results in an average time for encryption of 547.98ms while the average time for decryption is 538.19ms. The longest time for the encryption process is 557.30ms and the fastest is 534.50ms, while the longest time for the decryption process is 548.74ms and the fastest is 531.46ms. Hiding messages in audio files using LSB produces PSNR values above 30dB.

Keywords : Blowfish, Cryptography, Least Significant Bit, Steganography.

PENGAMANAN PESAN PADA FILE AUDIO DENGAN METODE *LSB* DAN *BLOWFISH*

Oleh:
Ahmad Rizky Fauzan
09021281722042

ABSTRAK

Seiring perkembangan teknologi, komunikasi dapat dilakukan dengan berbagai macam cara, salah satunya adalah pesan digital. Namun sering kali pesan yang dikirim tidak sampai ke tujuan dan didapatkan oleh pihak yang tidak bertanggung jawab. Hal ini terjadi karena kurangnya keamanan pada file tersebut. Untuk itu dibutuhkan keamanan agar pesan tidak dapat dicuri atau dilihat pihak lain. Terdapat beragam cara untuk mengamankan pesan, diantaranya teknik Steganografi dan Kriptografi. Penelitian ini menggunakan kombinasi metode Least Significant Bit dan algoritma Blowfish untuk mengamankan pesan rahasia pada file audio. Pada penelitian ini akan dilakukan pengukuran waktu enkripsi dan dekripsi, analisis perubahan ukuran file pesan setelah enkripsi dan dekripsi, dan nilai PSNR dari file audio. Hasil dari enkripsi menggunakan blowfish adalah perubahan pada ukuran file pesan yang disebabkan karena ukuran file pesan kurang dari ukuran *block cipher* sehingga diberikan tambahan byte agar ukuran pesan sesuai dengan ukuran *block cipher*. Kecepatan proses enkripsi dan dekripsi menggunakan algoritma blowfish menghasilkan waktu rata-rata lama waktu untuk enkripsi 547.98ms sedangkan untuk rata-rata waktu untuk dekripsi adalah 538.19ms. Waktu terlama untuk proses enkripsi adalah 557.30ms dan tercepat 534.50ms, sedangkan waktu terlama untuk proses dekripsi adalah 548.74ms dan yang tercepat adalah 531.46ms. Penyembunyian pesan pada file audio menggunakan LSB menghasilkan nilai PSNR diatas 30dB.

Kata Kunci : *Blowfish*, Kriptografi, *Least Significant Bit*, Steganografi.

KATA PENGANTAR

Puji syukur kepada Allah SWT atas segala rahmat dan karunia-Nya penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan pendidikan Strata-1 Program Studi Teknik Informatika pada Fakultas Ilmu Komputer, Universitas Sriwijaya.

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan bantuan baik dalam materil dan moril selama proses pembuatan Tugas Akhir ini, yaitu:

1. Bapak Prof. Dr. Ir. H. Anis Saggaff, MSCE, IPU selaku rektor dari Universitas Sriwijaya.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku dekan Fakultas Ilmu Komputer
3. Bapak Al Farrisi. M.Comp.Sc dan Bapak M. Naufal Rachmatullah, M.T. selaku dosen pembimbing yang telah dengan sabar memberikan bimbingan dan berbagai pengalaman kepada penulis.
4. Segenap Dosen Fakultas Ilmu Komputer Universitas Sriwijaya yang telah mendidik dan memberikan ilmu selama kuliah dan seluruh staf yang selalu sabar melayani segala administrasi selama proses penelitian ini.
5. Kedua orang tua saya, KGS. A. Rahman dan Maya Sopa yang selalu memberikan dukungan, doa, dan nasihat serta kesabarannya yang luar biasa.
6. Kakak saya, Sarah Fadhilah, terima kasih atas segala doa dan dukungan
7. Teman-teman Campur Sari (CS) dan YDN yang selalu mendukung dan memberikan semangat.
8. Teman-teman IF Reg B 2017.

9. Semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Semoga segala kebaikan dan pertolongan semuanya mendapat berkah dari Allah Swt. dan akhirnya saya menyadari bahwa skripsi ini masih jauh dari kata sempurna, karena keterbatasan ilmu yang saya miliki. Untuk itu saya dengan kerendahan hati mengharapkan saran dan kritik yang sifatnya membangun dari semua pihak demi membangun laporan penelitian ini.

Palembang, 24 Januari 2022

Penyusun,

Ahmad Rizky Fauzan
NIM. 09021281722042

DAFTAR ISI

Halaman

Pengamanan Pesan pada File Audio dengan Metode <i>LSB</i> dan <i>Blowfish</i>	i
LEMBAR PENGESAHAN SKRIPSI.....	ii
TANDA LULUS UJIAN SIDANG SKRIPSI.....	iii
HALAMAN PERNYATAAN	iv
MOTTO DAN PERSEMPAHAN	v
ABSTRACT	vi
ABSTRAK	vii
KATA PENGANTAR.....	viii
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	I-1
1.1 Pendahuluan.....	I-1
1.2 Latar Belakang Masalah	I-1
1.3 Rumusan Masalah.....	I-4
1.4 Tujuan Penelitian.....	I-5
1.5 Manfaat Penelitian.....	I-5
1.6 Batasan Masalah	I-5
1.7 Sistematika Penulisan	I-6
1.8 Kesimpulan.....	I-7
BAB II KAJIAN LITERATUR	II-1
2.1 Pendahuluan.....	II-1
2.2 Landasan Teori	II-1
2.2.1 File Audio (.WAV).....	II-1
2.2.2 Kriptografi	II-2
2.2.3 Steganografi.....	II-3
2.2.4 <i>Blowfish</i>	II-4
2.2.5 Least Significant Bit (<i>LSB</i>).....	II-7
2.2.6 Peak Signal-to-Noise Ratio (PSNR).....	II-7
2.2.7 Java	II-8
2.2.8 Rational Unified Process (RUP).....	II-9

2.3	<i>Library</i> yang digunakan.....	II-10
2.4	Penelitian Lain yang Relevan	II-11
2.5	Kesimpulan.....	II-14
BAB III METODOLOGI PENELITIAN		III-1
3.1	Pendahuluan.....	III-1
3.2	Pengumpulan Data.....	III-1
3.3	Tahapan Penelitian.....	III-2
3.3.1	Kerangka Kerja.....	III-2
3.3.2	Kriteria Pengujian.....	III-3
3.3.3	Format Data Pengujian dan Pengujian Penelitian	III-3
3.3.4	Alat Bantu Penelitian.....	III-5
3.3.5	Pengujian Penelitian	III-6
3.3.6	Analisis Hasil Pengujian dan Membuat Kesimpulan Penelitian	III-6
3.4	Metode Pengembangan Perangkat Lunak	III-7
3.4.1	Fase Insepsi.....	III-7
3.4.2	Fase Elaborasi.....	III-7
3.4.3	Fase Konstruksi	III-8
3.4.4	Fase Transisi	III-8
3.5	Manajemen Proyek Penelitian	III-8
BAB IV PENGEMBANGAN PERANGKAT LUNAK		IV-1
4.1	Pendahuluan.....	IV-1
4.2	Fase Insepsi.....	IV-1
4.3	Fase Elaborasi.....	IV-14
4.4	Fase Konstruksi	IV-35
4.5	Fase Transisi	IV-42
4.6	Kesimpulan.....	IV-51
BAB V ANALISIS PENELITIAN		V-1
5.1	Pendahuluan.....	V-1
5.2	Data Hasil Percobaan / Penelitian.....	V-1
5.2.1	Konfigurasi Percobaan.....	V-1
5.2.2	Hasil Pengujian <i>Blowfish</i>	V-1

5.2.3	Hasil Pengujian <i>LSB</i>	V-4
5.3	Analisis Hasil Penelitian.....	V-7
5.4	Kesimpulan.....	V-8
BAB VI KESIMPULAN DAN SARAN.....		VI-1
6.1	Pendahuluan.....	VI-1
6.2	Kesimpulan.....	VI-1
6.3	Saran	VI-2
DAFTAR PUSTAKA.....		iii
LAMPIRAN		vi

DAFTAR TABEL

Halaman

Tabel III-1. Hasil Uji Perubahan File Pesan Setelah Enkripsi dan Dekripsi	III-4
Tabel III-2. Hasil Uji Nilai PSNR.....	III-4
Tabel III-3. Hasil Uji Waktu Proses Enkripsi dan Dekripsi.....	III-4
Tabel III-4. Jadwal Penelitian	III-10
Tabel III-5. Gantt Chart.....	III-14
Tabel IV-1. Kebutuhan Fungsional.....	IV-2
Tabel IV-2. Kebutuhan Non-Fungsional.....	IV-3
Tabel IV-3. Definisi Aktor Use Case.....	IV-7
Tabel IV-4. Definisi Use Case	IV-7
Tabel IV-5. Skenario Use Case Enkripsi Pesan	IV-8
Tabel IV-6. Skenario Use Case Penyembunyian Pesan.....	IV-9
Tabel IV-7. Skenario Use Case Ekstrak Pesan	IV-11
Tabel IV-8. Skenario Use Case Dekripsi Pesan.....	IV-12
Tabel IV-9. Skenario Use Case Hitung PSNR.....	IV-13
Tabel IV-10. Daftar File Pesan yang akan dienkripsi	IV-43
Tabel IV-11. Daftar File audio yang akan dijadikan audio penampung	IV-44
Tabel IV-12. Pengujian Enkripsi Pesan	IV-46
Tabel IV-13. Pengujian Penyembunyian Pesan	IV-47
Tabel IV-14. Pengujian Ekstrak Pesan.....	IV-48
Tabel IV-15. Pengujian Dekripsi Pesan	IV-49
Tabel IV-16. Pengujian Menghitung Nilai PSNR.....	IV-50
Tabel V-1. Hasil Pengujian Enkripsi dan Dekripsi	V-2
Tabel V-2. Hasil Pengujian Rata-rata Waktu Enkripsi dan Dekripsi Pesan	V-3
Tabel V-3. Hasil Pengujian Penyembunyian Pesan	V-4

DAFTAR GAMBAR

Halaman

Gambar II-1. Format File WAV.....	II-2
Gambar II-2 Kriptografi.....	II-3
Gambar II-3 Proses Steganografi	II-4
Gambar II-4. Skema enkripsi Blowfish	II-6
Gambar II-5. Fungsi F.....	II-6
Gambar II-6 Fase RUP	II-9
Gambar III-1. Flowchart penelitian.....	III-5
Gambar IV-1. Diagram Use Case	IV-6
Gambar IV-2. Diagram Aktivitas Enkripsi Pesan.....	IV-16
Gambar IV-3. Diagram Aktivitas Penyembunyian Pesan.....	IV-16
Gambar IV-4. Diagram Aktivitas Ekstrak Pesan	IV-17
Gambar IV-5. Diagram Aktivitas Dekripsi Pesan.....	IV-18
Gambar IV-6. Diagram Aktivitas Menghitung PSNR	IV-18
Gambar IV-7. Diagram Alir Proses Enkripsi Pesan.....	IV-19
Gambar IV-8. Diagram Alir Proses Penyembunyian Pesan	IV-20
Gambar IV-9. Diagram Alir Proses Ekstrak Pesan	IV-21
Gambar IV-10. Diagram Alir Proses Dekripsi Pesan	IV-22
Gambar IV-11. Diagram Alir Proses Hitung PSNR	IV-22
Gambar IV-12. DFD Level 0	IV-23
Gambar IV-13. DFD Level 1	IV-24
Gambar IV-14. Diagram Sequence Enkripsi Pesan	IV-25
Gambar IV-15. Diagram Sequence Penyembunyian Pesan.....	IV-26
Gambar IV-16. Diagram Sequence Ekstrak Pesan	IV-27
Gambar IV-17. Diagram Sequence Dekripsi Pesan	IV-27
Gambar IV-18. Diagram Sequence Hitung Nilai PSNR	IV-28
Gambar IV-19. Rancangan Antarmuka Menu Awal.....	IV-29
Gambar IV-20. Rancangan Antarmuka Enkripsi Pesan.....	IV-30
Gambar IV-21. Rancangan Antarmuka Penyembunyian Pesan	IV-31
Gambar IV-22. Rancangan Antarmuka Pilih Data	IV-32
Gambar IV-23. Rancangan Antarmuka Ekstrak Pesan	IV-32
Gambar IV-24. Rancangan Antarmuka Dekripsi Pesan	IV-33
Gambar IV-25. Rancangan Antarmuka Hitung PSNR	IV-34
Gambar IV-26. Diagram Kelas Perangkat Lunak	IV-36
Gambar IV-27. Implementasi Antarmuka Menu Awal.....	IV-39
Gambar IV-28. Implementasi Antarmuka Enkripsi Pesan.....	IV-39
Gambar IV-29. Implementasi Antarmuka Penyembunyian Pesan	IV-40
Gambar IV-30. Implementasi Antarmuka Pilih Data	IV-40
Gambar IV-31. Implementasi Antarmuka Ekstrak Pesan	IV-41
Gambar IV-32. Implementasi Antarmuka Dekripsi Pesan	IV-41
Gambar IV-33. Implementasi Antarmuka Hitung PSNR	IV-42
Gambar V-1. Grafik Rata-rata Waktu Proses Enkripsi dan Dekripsi	V-4
Gambar V-2. Grafik Perubahan Nilai PSNR Terhadap Ukuran Pesan	V-7

DAFTAR LAMPIRAN

- Lampiran 1. Pengujian Enkripsi
- Lampiran 2. Pengujian Dekripsi
- Lampiran 3. Source Code MainUI.java
- Lampiran 4. Source Code EmbedUI.java
- Lampiran 5. Source Code class embed.java
- Lampiran 6. Source code class UiEkstraksi.java
- Lampiran 7. Source Code class Ekstraksi.java
- Lampiran 8. Source Code UiEnkripsi.java
- Lampiran 9. Source Code UiDekripsi.java
- Lampiran 10. Source code Blowfish.java
- Lampiran 11. Source Code UI_PSNR
- Lampiran 12. Source Code PSNR.java

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab pendahuluan ini akan membahas latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan serta kesimpulan dalam tugas akhir. Pada bab ini juga berisi penjelasan mengenai gambaran umum dari tugas akhir. Bab ini akan menjelaskan metode yang akan digunakan dalam penelitian dan penelitian terkait yang telah diteliti sebelumnya

1.2 Latar Belakang Masalah

Semakin maju nya teknologi sistem informasi saat ini membuat setiap orang dapat saling berinteraksi dan berkomunikasi melalui berbagai macam cara, salah satunya adalah pesan digital.

Menurut Jane dkk (2017) Seiring perkembangan kemajuan teknologi membuat pesan menjadi penting. Sering kali pesan yang ingin dikirim tidak sampai ke tujuan dan jatuh ke tangan orang yang tidak bertanggung jawab karena kurangnya keamanan pada penerimaan pesan tersebut. Untuk itu dibutuhkan keamanan yang dapat mengamankan pesan agar dapat sampai ke tujuan.

Untuk mengamankan pesan kedalam sebuah file dapat menggunakan gabungan dari metode steganografi dan kriptografi. Steganografi adalah seni untuk menyisipkan pesan rahasia kedalam suatu media, pesan rahasia tersebut akan disembunyikan tanpa merubah isi dari file tersebut, sehingga pihak yang tidak memiliki hak tidak dapat melihat pesan yang disembunyikan. Metode steganografi

yang dipakai adalah metode *Least Significant Bit* (LSB) (Jane dkk, 2017).

LSB adalah salah satu metode steganografi yang banyak digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain. Selain itu LSB mudah diimplementasikan dalam aplikasi (Nur Aini dkk, 2019). Metode LSB pada file audio bekerja dengan cara memodifikasi *bit-bit* terakhir dalam beberapa *byte file* audio untuk menyembunyikan urutan *byte* yang mengandung data rahasia.

Kriptografi berasal dari dua kata Yunani, yaitu “*cryptó*” yang berarti rahasia dan “*graphy*” yang berarti menulis. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Untuk menjaga keamanan data, kriptografi menenkripsi pesan (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dimengerti. (Budi dkk, 2017).

Pada kriptografi terdapat Algoritma Blowfish yang 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 archive seperti .zip dan .rar (Irtafa dkk, 2015).

Algoritma kriptografi blowfish dipilih dan digunakan dalam penelitian ini karena blowfish banyak kelebihan diantaranya cepat, sederhana, kompak dan memiliki tingkat keamanan yang fleksibel karena memiliki panjang kunci yang

beragam, sedangkan teknik steganografi LSB dipilih karena setelah pesan disisipkan ke dalam media penampung, hasil proses tidak akan berdampak pada perubahan ukuran dari media tersebut sehingga hal ini tidak akan menimbulkan kecurigaan.

Pengamanan data serta informasi menggunakan kombinasi teknik kriptografi dan steganografi ini menjadi hal yang lazim digunakan. Namun tidak jarang pula beberapa dari kombinasi teknik tersebut hanya salah satu teknik saja yang digunakan untuk menjaga kerahasiaan data. Kedua teknik tersebut semuanya dapat dipakai untuk menjaga keamanan informasi. Perbedaan kedua teknik tersebut adalah, jika pada Teknik kriptografi, data yang telah tersandi (ciphertext) tetap ditampilkan, sedangkan pada teknik steganografi pesan yang telah tersandi disembunyikan ke dalam media tertentu sehingga keberadaan pesan tersebut tidak terlihat oleh orang lain. Oleh karena itu, pemakaian kombinasi teknik pengamanan data menjadi pilihan agar kerahasiaan data benar-benar terjaga.

Pada penelitian ini file audio dengan format .wav yang digunakan sebagai media penampung karena file audio dengan format .wav tidak terkompresi dan memiliki kualitas suara yang baik, jadi ketika terjadi perubahan pada file audio tersebut tidak akan menimbulkan derau sehingga tidak mengundang kecurigaan (Peling, I. B. A., & Sastra, N. P).

Pada analisa hasil pengamanan pesan audio terdapat indikator untuk mengetahui kualitas setelah proses steganografi dengan menggunakan PSNR (Peak Signal to Noise Ratio) yang merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal

tersebut. PSNR biasanya diukur dalam satuan decibel (dB).

Dalam penelitian sebelumnya oleh Indriyono (2019) dibahas cara melakukan pengamanan informasi menggunakan kriptografi *blowfish* dan steganografi LSB dengan media MP3. Selain itu, dihasilkan pula perangkat lunak untuk implementasi kedua teknik pengamanan informasi tersebut. Dari hasil implementasi disimpulkan bahwa selain menggunakan media gambar, proses penyembunyian pesan dapat dilakukan dengan menggunakan media MP3 tanpa mengakibatkan perubahan yang signifikan pada file MP3 aslinya.

Pada Penelitian ini dilakukan untuk mengetahui cara pengamanan pesan dan menganalisa seberapa efektif penyembunyian pesan yang telah di enkripsi menggunakan metode LSB dan metode *blowfish*, sehingga pesan yang disembunyikan dalam file audio tersebut aman dan tidak terdeteksi oleh pihak luar. Dari hasil penelitian juga akan dilakukan analisa kualitas audio sebelum dan sesudah proses steganografi berdasarkan nilai PSNR (*Peak Signal to Noise Ratio*) serta lama proses enkripsi dan dekripsi dari algortima *Blowfish*.

1.3 Rumusan Masalah

Dari penjelasan dalam latar belakang didapat permasalahan dalam penelitian sebagai berikut:

1. Bagaimana cara mengamankan file pesan dan menyembunyikan file pesan kedalam file audio menggunakan kombinasi metode LSB dan algoritma *blowfish*?
2. Bagaimana perbedaan kualitas audio sebelum dan sesudah proses steganografi berdasarkan nilai PSNR?

3. Bagaimana perubahan ukuran dari file pesan setelah proses enkripsi dan dekripsi?
4. Berapa lama waktu proses enkripsi dan dekripsi terhadap file pesan menggunakan algoritma *Blowfish*?

1.4 Tujuan Penelitian

Adapun tujuan tugas akhir ini adalah:

1. Menerapkan algoritma *blowfish* untuk enkripsi dan dekripsi pesan dan menyembunyikan pesan yang telah terenkripsi kedalam file audio menggunakan metode *LSB*.
2. Menganalisis lama waktu proses enkripsi dan dekripsi file pesan menggunakan algoritma *Blowfish*.
3. Menganalisis perubahan pada file pesan setelah enkripsi dan dekripsi.
4. Melakukan perhitungan PSNR terhadap file audio setelah dilakukan penyembunyian pesan.
5. Melakukan penyembunyian pesan pada file audio dan ekstraksi pesan dari *Stego Audio*.

1.5 Manfaat Penelitian

Mengembangkan perangkat lunak audio steganografi menggunakan LSB dengan enkripsi pesan menggunakan algoritma *blowfish*.

1.6 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. File audio yang digunakan berformat .wav.
2. File pesan yang digunakan dalam format .txt dan .pdf

3. Ukuran dari file audio yang menjadi cover harus lebih besar minimal 8 kali dari ukuran pesan yang akan disembunyikan.
4. Perangkat lunak yang dibangun menggunakan bahasa pemrograman java yang berbasis desktop

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada bab ini diuraikan mengenai pokok-pokok pikiran yang melandasi pembuatan penelitian, seperti latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini membahas dasar-dasar teori yang digunakan dalam penelitian, seperti definisi algoritma LSB dan Blowfish, serta beberapa kajianliteratur mengenai penelitian lain yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Pada bab ini membahas mengenai tahapan yang akan dilaksanakan pada penelitian. Seperti pengumpulan data, analisis data, serta perancangan sistem yang akan dibangun. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci mengacu pada suatu kerangka kerja.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan dibahas mengenai analisis dan perancangan perangkat lunak yang akan digunakan untuk penelitian serta pengujian untuk memastikan semua kebutuhan pengembangan perangkat lunak

sesuai dengan kebutuhan.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini berisi tentang analisis perubahan terhadap file pesan setelah enkripsi dan dekripsi dan file audio setelah disisipkan file pesan. hasil pengujian berdasarkan langkah- langkah yang telah direncanakan disajikan. Analisis diberikan sebagai basis dari kesimpulan yang diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran terkait penelitian yang dilakukan.

1.8 Kesimpulan

Pada bab ini telah dijelaskan secara umum mengenai masalah yang menjadilatar belakang dilakukannya penelitian ini. Pada bab ini juga telah dijelaskan rumusan masalah, tujuan dari penelitian, manfaat dari penelitian, batasan masalah dalam penelitian serta sistematika penulisan.

DAFTAR PUSTAKA

- M.Baritha Begum ,Y.Venkataramani. 2012. *LSB Based Audio Steganography Based On Text Compression*, 2012.
- 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).
- Masruri, I., Mungki Astiningrum. 2015. Rancang Bangun Implementasi Steganografi Audio Menggunakan Metode *Least Significant Bit (LSB)* Dengan Kombinasi Algoritma *Blowfish*, 2015.
- K.P.Adhiya Swati A. Patil. 2012. *Hiding Text in Audio Using LSB Based Steganography*, 2012.
- Bhalshankar, S., & Gulve, A. K. (2015). Audio steganography: LSB technique using a pyramid structure and range of bytes. arXiv preprint arXiv:1509.02630.
- Sibarani, N. S., Munawar, G., & Wisnuadhi, B. (2018, October). Analisis Performa Aplikasi Android Pada Bahasa Pemrograman Java dan Kotlin. In Prosiding Industrial Research Workshop and National Seminar (Vol. 9, pp. 319-324).
- S. Sitinjak, Y. Fauziah, Juwairiah, “Aplikasi Kriptografi File Menggunakan Algoritma Blowfish”. Seminar Nasional Informatika 2010 (semnasIF 2010). UPN Veteran Yogyakarta, 22 Mei 2010. ISSN: 1979-2328, 2010.
- Kurniawan, H., Mardiani, E., & Rahmansyah, N. (2011). Aplikasi Penjualan Dengan Program Java Netbeans, Xammmp, dan iReport.
- J. Thakur, N. Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis”. International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, Volume 1, Issue 2, December 2011.
- A. R. Lubis, M. S. Lidya, A. Budiman, “Perancangan Perangkat Lunak Steganografi Audio MP3 Menggunakan Metode Least Significant Bit (LSB) dengan Visual Basic 6.0”. *Jurnal Dunia Teknologi Informasi*. Vol. 1. No. 1. Hal 63-68, 2012.
- S. Wardoyo, R. Fahrizal, Z. Imanullah, “Aplikasi Teknik Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android”. SETRUM Vol 3. No. 1. Juni 2014. ISSN: 2301-4652, 2014.

- D. Abdullah, D. N. Saputro, "Implementasi Algoritma Blowfish dan Metode Least Significant Bit Insertion Pada Video Mp3". Jurnal Pseudocode, Vol III. No 2. September 2016. ISSN 2355-5920, 2016.
- A. M. Ghorpade, H. Talwar, "The Blowfish Algorithm Simplified". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 5. Issue 4. April 2016. ISSN (Print) : 2320 – 3765. ISSN (Online): 2278 – 8875, 2016.
- R. Siburian, Lindawati, Aryanti. "Implementasi Steganografi Audio MP3 dan WAV untuk File Pdf pada SmartPhone Android dengan Menggunakan Metode LSB (Least Significant Bit)". Seminar Nasional Teknologi Informasi, Bisnis, dan Desain. STMIK – Politeknik PalComTech, 12 Juli 2017. ISBN: 978-602-74635-1-6, 2017.
- P. Patel, R. Patel, N. Patel, "Integrated ECC and Blowfish for Smartphone Security". International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015. Nagpur, INDIA, 2015.
- G. A. Dwi, Rumani, M. Nasrun, M. "Implementasi Kriptografi dan Steganografi pada Media Gambar Menggunakan Algoritma Blowfish dan Metode Least Significant Bit". e-Proceeding of Engineering. Vol.2, No.2 Agustus 2015. Page 3762. ISSN: 2355- 9365, 2015.
- B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Springer-Verlag, 1996.
- Indriyono, Bonifacius Vicky. 2019. Integrasi Algoritma Kriptografi Blowfish dengan Steganografi LSB untuk Pengamanan Data pada File MP3. Surabaya: Jurnal SISFO Vol.08 No.03.
- Peling, I. B. A., & Sastra, N. P. (2018). Enhanced Audio Steganografi dengan Algoritma Advanced Encryption Standard untuk Pengamanan Data pada File Audio. Majalah Ilmiah Teknologi Elektro, 17(1), 66-71.
- W.K..Chen, Linear Networks and Systems (Book Style). Belmont, CA: Wadsworth, pp. 123-135, 1993.
- Prasetyo, B., Muslim, M. A., & Susanto, H. (2017). Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks. Techno. Com, 16(4), 358-366.
- Ariyus, D. (2006). Kriptografi keamanan data dan komunikasi. Yogyakarta Graha Ilmu.
- R. Munir, Kriptografi. Bandung : Informatika, 2006.

Harjo, T. B., Kapriati, M., & Susanto, D. A. (2016). Aplikasi Steganografi Menggunakan LSB (Least Significant Bit) dan Enkripsi Triple Des Menggunakan Bahasa Pemrograman C#. vol, 6, 13-17.

Lovebbi, L., & Sudirman, D. Z. (2012). rancang bangun aplikasi steganografi dengan metode least significant bit di audio pada sistem operasi android. Ultimatics: Jurnal Teknik Informatika, 4(1), 7-16.

Styorini, W., & Harinitha, D. Analisis Performansi Algoritma AES dan Blowfish Pada Aplikasi Kriptografi. In Seminar Nasional (pp. 1-6).

Eric, C. (2003). Hiding in plain sight, Stegnography and the art of Covert Communication. Wiley, Indianapolis, Indiana, ISBN, 10, 0471444499.