

**APLIKASI STEGANOGRAFI PESAN TEKS PADA MEDIA AUDIO
MP3 MENGGUNAKAN METODE PENYISIPAN *LEAST
SIGNIFICANT BIT* DAN *ADVANCED ENCRYPTION STANDARD***



SKRIPSI

**Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
pada Jurusan Ilmu Komputer / Informatika**

Disusun Oleh :

ILHAM FIRMAN ASHARI

24010311130032

**JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO**

2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini,

Nama : Ilham Firman Ashari

NIM : 24010311130032

Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Dengan ini saya menyatakan bahwa dalam tugas akhir atau skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 31 Agustus 2015



Ilham Firman Ashari
24010311130032

HALAMAN PENGESAHAN

Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Nama : Ilham Firman Ashari

NIM : 24010311130032

Telah diujikan pada sidang tugas akhir pada tanggal 20 Agustus 2015 dan dinyatakan lulus pada tanggal **31 Agustus 2015**.

Semarang, 1 September 2015

Mengetahui,
Ketua Jurusan Ilmu Komputer / Informatika
FSM UNDIP



Panitia Penguji Tugas Akhir
Ketua,

Sukmawati Nur Endah, S.Si, M.Kom
NIP. 19780502 200501 2 002

The image shows a black ink signature of Sukmawati Nur Endah. Below the signature, the name "Sukmawati Nur Endah, S.Si, M.Kom" and the NIP number "NIP. 19780502 200501 2 002" are printed.

HALAMAN PENGESAHAN

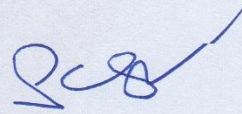
Judul : Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* Dan *Advanced Encryption Standard*

Nama : Ilham Firman Ashari

NIM : 24010311130032

Telah diujikan pada sidang tugas akhir pada tanggal 20 Agustus 2015

Semarang, 1 September 2015
Dosen Pembimbing,



Aris Sugiharto, S.Si, M.Kom
NIP. 19710811 199702 1 004

ABSTRAK

Perkembangan teknologi informasi telah berkembang sangat pesat, sehingga memberikan kemudahan dalam mengakses dan mendapatkan data informasi. Dampak negatifnya adalah masalah keamanan dan munculnya berbagai macam teknik yang digunakan oleh berbagai pihak untuk mendapatkan informasi yang bersifat rahasia. Oleh karena itu, keamanan informasi merupakan aspek penting untuk menjaga kerahasiaan suatu informasi. Salah satu metode keamanan yang dapat digunakan untuk mengamankan pesan rahasia tanpa dapat dipersepsi adalah dengan menggabungkan metode kriptografi dan steganografi. Dalam penelitian ini, metode kriptografi yang digunakan adalah *Advanced Encryption Standard* (AES) dan metode Steganografi yang digunakan adalah *Least Significant Bit* (LSB) dengan media audio MP3. Pada awalnya pesan teks akan dilakukan enkripsi menggunakan AES, kemudian hasil *ciphertext*nya akan disisipkan ke dalam audio MP3 dengan menggunakan metode LSB untuk mendapatkan file MP3Stego. Tahapan terakhir untuk mendapatkan file pesan adalah melakukan ekstraksi pada MP3Stego dan melakukan dekripsi dengan menggunakan AES untuk mendapatkan pesan asli. Hasil akhir dari aplikasi ini berupa audio MP3 stego yang telah memuat pesan yang disisipkan. Audio MP3 stego mempunyai ukuran dan bentuk yang sama persis seperti audio MP3 aslinya. Meskipun bit-bit audio MP3 sudah mengalami perubahan akibat penyisipan, namun perubahan itu tidak begitu signifikan, sehingga audio MP3Stego tidak menimbulkan kecurigaan. Berdasarkan pengujian terhadap *Signal Noise to Ratio* (SNR) maka didapatkan nilai SNR berbanding terbalik dengan ukuran pesan yang disisipkan, semakin besar ukuran pesan yang disisipkan maka nilai SNR semakin kecil.

Kata Kunci : Steganografi, Kriptografi, AES, LSB

ABSTRACT

The development of information technology has been growing very rapidly, so as to provide easy access and obtain information data. The negative impact of security problems and the emergence of a wide range of techniques used by the various parties to obtain secret information. Therefore, information security is an important aspect for maintaining the confidentiality of the information. One of the security methods that can be used to secure the secret message without perceptible is to combine methods of cryptography and steganography. In this study, the method used is AES cryptography and steganography method used is LSB with MP3 audio containers. At first text message will be carried out using the AES encryption, then the results will inserted into MP3 audio by using LSB method to obtain Stego.MP3 file. The last stage to get the message file is doing extracting the MP3Stego and perform decryption using the AES to get the original message. The end result of this application in the form of audio MP3stego contains messages that have been inserted. MP3 audio stego have the same size and shape exactly as the original MP3 audio. Although the MP3 audio bits have changed as a result of the insertion, but the change was not so significant, so the MP3 audio Stego not to arouse suspicion. Based on the testing of the SNR then obtained SNR value is inversely proportional to the size of the message is inserted.

Keywords : Steganography, Cryptography, AES, LSB

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah Subhanahu wa Ta'ala yang telah melimpahkan segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini yang mempunyai judul “Aplikasi Steganografi Pesan Teks Pada Media Audio MP3 Menggunakan Metode Penyisipan *Least Significant Bit* dan *Advanced Encryption Standard*”.

Skripsi ini dibuat dengan tujuan sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada Jurusan Ilmu Komputer/Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.

Dalam pelaksanaan tugas akhir serta penyusunan dokumen skripsi ini, penulis menyadari banyak pihak yang membantu sehingga akhirnya dokumen ini dapat diselesaikan. Oleh karena itu, melalui kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Prof. Dr. Widowati, S.Si, M.Si, selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
3. Indra Waspada, S.T, M.TI, selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro, Semarang.
4. Aris Sugiharto, S.Si, M.Kom, selaku dosen pembimbing yang telah membantu dalam membimbing dan mengarahkan penulis hingga selesainya skripsi ini.

Penulis menyadari bahwa dokumen skripsi ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang membangun sangat penulis harapkan. Akhir kata, semoga skripsi ini dapat bermanfaat bagi semua pihak.

Semarang, 20 Agustus 2015

Penulis

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI	ii
HALAMAN PENGESAHAN	iii
HALAMAN PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xv
DAFTAR KODE	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan dan Manfaat	3
1.4. Ruang Lingkup	4
1.5. Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA	6
2.1. Steganografi.....	6
2.2. Kriptografi	8
2.3. <i>Moving Picture Expert Group-1 Layer 3 (MP3)</i>	9
2.4. Struktur File MP3	10
2.4.1. <i>Header</i>	14
2.4.2. CRC	17
2.4.3. Side Information.....	17

2.4.4.	<i>Main Data</i>	17
2.4.5.	<i>Ancillary Data</i>	18
2.5.	<i>Least Significant Bit (LSB)</i>	18
2.6.	<i>Advanced Encryption Standard (AES)</i>	19
2.6.1.	Struktur Enkripsi AES	22
2.6.2.	Struktur Dekripsi AES	26
2.6.3.	Ekpansi Kunci	28
2.7.	Penilaian Kualitas Audio.....	29
2.7.1.	SNR (<i>Signal to Noise Ratio</i>)	30
2.7.2.	CER (<i>Character Error Rate</i>).....	30
2.8.	Model Pengembangan Perangkat Lunak <i>Unified Process</i>	30
2.9.	<i>Unified Modelling Language</i>	33
2.9.1.	<i>Things</i>	33
2.9.2.	<i>Relationship</i>	34
2.9.3.	Diagram.....	37
BAB III	FASE <i>INCEPTION</i> DAN FASE <i>ELABORATION</i>	39
3.1.	<i>Iteration Plan</i>	39
3.2.	Fase <i>Inception</i>	39
3.2.1.	Gambaran Umum Perangkat Lunak.....	40
3.2.2.	<i>Business Rules</i>	41
3.2.3.	Kebutuhan Non-Fungsional	42
3.2.4.	Model <i>Use Case</i>	42
3.3.	Fase <i>Elaboration</i>	44
3.3.1.	<i>Elaboration</i> Iterasi Pertama	44
3.3.2.	<i>Elaboration</i> Iterasi Kedua	53
BAB IV	FASE <i>CONSTRUCTION</i> DAN FASE <i>TRANSITION</i>	88
4.1.	Fase <i>Construction</i>	88

4.1.1. Implementasi Sistem.....	88
4.1.2. Implementasi Algoritma	88
4.1.3. Implementasi Antarmuka	100
4.2. Fase <i>Transition</i>	106
4.2.1. Lingkungan Pengujian	106
4.2.2. Pelaksanaan Pengujian.....	106
BAB V PENUTUP	115
5.1 Kesimpulan.....	115
5.2 Saran	116
DAFTAR PUSTAKA	117
LAMPIRAN-LAMPIRAN	119

DAFTAR GAMBAR

Gambar 2.1. Diagram Penyisipan dan Ekstraksi Pesan (Munir, 2006).....	7
Gambar 2.2. Tulisan <i>Hieroglyph</i> (Fisher, 1999).....	8
Gambar 2.3. Model <i>Simmetric Encryption</i> (Stallings, 2011)	8
Gambar 2.4. Struktur File MP3 (Raharjo, et al., 2009).....	11
Gambar 2.5. Struktur Main Data MP3 (Raharjo, et al., 2009)	11
Gambar 2.6. Struktur <i>Frame</i> ID3v2 (Newell, 2005).....	12
Gambar 2.7. Struktur Lengkap File MP3 (Raissi, 2002).....	13
Gambar 2.8. Struktur <i>Header</i> MP3 (Raissi, 2002)	14
Gambar 2.9. Struktur Main Data MP3 (Raissi, 2002).....	18
Gambar 2.10. LSB tiap 8 bit diganti dengan 1 bit Hidden Data (Djebbar, 2010)	19
Gambar 2.11. Struktur Data AES (Stallings, 2011).....	20
Gambar 2.12. Proses Enkripsi dan Dekripsi AES 128 bit (Stallings, 2011)	21
Gambar 2.13. Transformati Substitusi S-Box (Stallings, 2011)	23
Gambar 2.14. S-Box Rijndael (Stallings, 2011).....	23
Gambar 2.15. Transformasi Pegerseran Baris (ShiftRows)	24
Gambar 2.16. Matriks MixColumns Multiplication (Stallings, 2011).....	25
Gambar 2.17. Ilustrasi operasi transformasi MixColumns (Stallings, 2011)	25
Gambar 2.18. Transformasi Penambahan Kunci dengan Operasi XOR (Stallings, 2011)	26
Gambar 2.19. Invers S-Box Rijndael (Stallings, 2011).....	27
Gambar 2.20. Transformasi Invers Pegerseran Baris (InvShiftRows).....	27
Gambar 2.21. Matriks InvMixColumns Multiplication (Stallings, 2011).....	28
Gambar 2.22. Ekspansi Kunci AES (Stallings, 2011)	28

Gambar 2.23. Alur Kerja <i>Unified Process</i> (Arlow & Neustadt, 2002).....	31
Gambar 2.24. Siklus Hidup <i>Unified Process Process</i> (Arlow & Neustadt, 2002)	31
Gambar 2.25. Hubungan Fase dan Alur Kerja dalam <i>Unified Process</i> (Arlow & Neustadt, 2002).....	32
Gambar 2.26. <i>Dependency</i> antara Class ‘Filmclip’ dan ‘Channel’	34
Gambar 2.27. Contoh penggunaan <i>Name</i> Asosiasi Antara Class ‘Person’ dan ‘Company’	35
Gambar 2.28. Contoh penggunaan <i>role</i> dari Asosiasi antara class ‘Person’ dan ‘Company’	35
Gambar 2.29. Contoh penggunaan <i>Multiplicity</i> dari Asosiasi Antara Class ‘Person’ dan ‘Company’	36
Gambar 2.30. Contoh penggunaan <i>Aggregation</i> antara Class ‘Company’ dan ‘Department’	36
Gambar 2.31. <i>Generalization</i> : Class ‘Rectangle’, ‘Circle’, ‘Polygon’ Spesialisasi dari Class ‘Shape’	36
Gambar 2.32. Contoh <i>Class Diagram</i> Pemesanan Barang.....	37
Gambar 2.33. Contoh <i>Sequence Diagram</i> untuk proses Pemesanan Barang.	38
Gambar 3.1. Gambaran Umum Sistem	40
Gambar 3.2. <i>Use Case Diagram</i> Sistem	43
Gambar 3.3. <i>Class diagram</i> Aplikasi.....	45
Gambar 3.4. <i>Sequence diagram</i> Pemilihan Pesan <i>Plaintext</i>	46
Gambar 3.5. <i>Sequence diagram</i> Pemilihan Pesan <i>Ciphertext</i> Embed.....	47
Gambar 3.6. <i>Sequence diagram</i> Pemilihan Pesan <i>Ciphertext</i> Embed.....	47
Gambar 3.7. <i>Sequence diagram</i> Pemilihan MP3 File.....	48
Gambar 3.8. <i>Sequence diagram</i> Pemilihan MP3 Stego File	48
Gambar 3.9. <i>Sequence diagram</i> Save Pesan <i>Ciphertext</i>	49
Gambar 3.10. <i>Sequence diagram</i> Save Pesan <i>Ciphertext</i> <i>Extract</i>	49
Gambar 3.11. <i>Sequence diagram</i> Save <i>Plaintext</i> <i>Decrypt</i>	50

Gambar 3.12. <i>Sequence diagram</i> Embedding	50
Gambar 3.13. <i>Sequence diagram</i> Extracting	51
Gambar 3.14. <i>Sequence diagram</i> Enkripsi	52
Gambar 3.15. <i>Sequence diagram</i> Dekripsi	52
Gambar 3.16. <i>Flowchart</i> Encrypt Plaintext	54
Gambar 3.17. <i>Flowchart</i> Ekspansi Kunci	55
Gambar 3.18. Ekspansi Kunci AES	57
Gambar 3.19. Hasil konversi kunci dan struktur <i>word</i> kunci	57
Gambar 3.20. Rot <i>Word</i> w_3	58
Gambar 3.21. Hasil ekspansi kunci w_0 sampai w_{43}	69
Gambar 3.22. AddRoundKey <i>state</i> dengan <i>roundkey</i>	70
Gambar 3.23. Transformasi SubBytes, ShiftRows, dan Perkalian MixColumn	70
Gambar 3.24. AddRoundKey <i>state</i> dan <i>round key</i>	72
Gambar 3.25. <i>Flowchart</i> Decrypt Ciphertext	73
Gambar 3.26. <i>Flowchart</i> Penyisipan LSB	74
Gambar 3.27. Pesan Ke Biner	75
Gambar 3.28. <i>Flowchart</i> Ekstraksi LSB	77
Gambar 3.29. Perancangan Antarmuka Splash	80
Gambar 3.30. Perancangan Antarmuka Home	80
Gambar 3.31. Perancangan Antarmuka <i>Encryption & Embedding Detail Option Key</i>	81
Gambar 3.32. Perancangan Antarmuka <i>Encryption & Embedding Detail Input Key</i>	81
Gambar 3.33. Perancangan Antarmuka <i>Extracting & Decryption Detail Option Key</i>	82
Gambar 3.34. Perancangan Antarmuka <i>Extracting & Decryption Detail Input Key</i>	82
Gambar 3.35. Perancangan Antarmuka <i>Warning Failed To Save File</i>	83
Gambar 3.36. Perancangan Antarmuka <i>Warning Check Your Input MP3 File</i>	83

Gambar 3.37. Perancangan Antarmuka <i>Warning Check Confirmation Key</i>	83
Gambar 3.38. Perancangan Antarmuka <i>Message The Key ust In Accordance With Term 128 bit</i>	84
Gambar 3.39. Perancangan Antarmuka <i>Warning Reset</i>	84
Gambar 3.40. Perancangan Antarmuka <i>Embedding Finish</i>	84
Gambar 3.41. Perancangan Antarmuka <i>Message There's Hidden Message</i>	85
Gambar 3.42. Perancangan Antarmuka <i>Message No Hidden Message</i>	85
Gambar 4.1. Implementasi Antarmuka <i>Splash</i>	100
Gambar 4.2. Implementasi Antarmuka <i>Main</i>	100
Gambar 4.3. Implementasi Antarmuka <i>Encryption & Embedding Detail Option Key</i>	101
Gambar 4.4. Implementasi Antarmuka <i>Encryption & Embedding Detail Input Key</i> ..	101
Gambar 4.5. Implementasi Antarmuka <i>Extraction & Decryption Detail Option Key</i> .	102
Gambar 4.6. Implementasi Antarmuka <i>Extraction & Decryption Detail Option Key</i> .	102
Gambar 4.7. Implementasi Antarmuka <i>Warning Check Your Input Message</i>	103
Gambar 4.8. Implementasi Antarmuka <i>Check Your Input MP3 File</i>	103
Gambar 4.9. Implementasi Antarmuka <i>Warning Check Confirmation Key</i>	103
Gambar 4.10. Implementasi Antarmuka <i>Message The Key Must In Accordance With Term 128 bit</i>	104
Gambar 4.11. Implementasi Antarmuka <i>Warning Reset</i>	104
Gambar 4.12. Implementasi Antarmuka <i>Message Embedding Finish</i>	105
Gambar 4.13. Implementasi Antarmuka <i>Message There's Hidden Message</i>	105
Gambar 4.14. Implementasi Antarmuka <i>Message No Hidden Message</i>	105

DAFTAR TABEL

Tabel 2.1 Detail Struktur ID3v2 (Nilsson, 2000)	11
Tabel 2.2 Struktur ID3v1 (Raissi, 2002)	12
Tabel 2.3. Nilai bit ketika menggunakan 2 <i>id</i> bit (Raissi, 2002)	15
Tabel 2.4. Nilai layer (Raissi, 2002)	15
Tabel 2.5. Definisi Nilai Bitrate (Raissi, 2002)	15
Tabel 2.6. <i>Frequency</i> Audio MP3 (Raissi, 2002)	16
Tabel 2.7. <i>Channel Mode</i> (Raissi, 2002)	16
Tabel 2.8. <i>Bit Mode Extension</i> (Raissi, 2002)	16
Tabel 2.9. Parameter AES (Stallings, 2011)	21
Tabel 2.10. (Stallings, 2011)	29
Tabel 2.11. Jenis <i>Relationship</i> pada <i>Use Case Diagram</i>	38
Tabel 3.1 Daftar Aktor Sistem	42
Tabel 3.2 Daftar <i>Use Case</i> Sistem	43
Tabel 3.3. Rencana Pengujian Fungsi Aplikasi	86
Tabel 3.4 Rencana Pengujian Parameter	87
Tabel 4.1 Hasil dan Evaluasi Pengujian Fungsi Aplikasi	107
Tabel 4.2. Tabel Uji Perhitungan Waktu Eksekusi Enkripsi	109
Tabel 4.3. Tabel Uji Perhitungan Waktu Eksekusi Dekripsi	110
Tabel 4.4. Hasil Pengujian Nilai SNR dengan Ukuran Pesan Berubah	111
Tabel 4.5. Tabel Pengujian Terhadap Aspek <i>Recovery</i>	112
Tabel 4.6. Hasil Pengujian Manipulasi MP3 <i>Cover</i> Terhadap <i>Bit Rate</i>	113
Tabel 4.7. Hasil Pengujian Manipulasi MP3 <i>Cover Modus Channel</i>	113
Tabel 4.8. Hasil Pengujian Manipulasi MP3 <i>Cover</i> Terhadap <i>Sample Frequency</i>	113

DAFTAR KODE

Kode 4.1. Kode untuk <i>KeyExpansion</i>	89
Kode 4.2. Kode untuk mengisi nilai array $w[0]$, $w[1]$, $w[2]$, dan $w[3]$	89
Kode 4.3. Kode untuk melakukan ekspansi dengan $i=4$	90
Kode 4.4. Kode untuk fungsi g , jika $i \bmod 4,6,8 = 0$	91
Kode 4.5. Skema fungsi g pada ekspansi kunci.....	91
Kode 4.6. Kode untuk operasi <i>rotWord</i>	91
Kode 4.7. Kode untuk operasi <i>subWord</i>	91
Kode 4.8. Kode untuk transformasi <i>subBytes</i>	92
Kode 4.9. Kode untuk transformasi <i>shiftRows</i>	93
Kode 4.10. Kode untuk transformasi <i>MixColumns</i>	94
Kode 4.11. Kode untuk transformasi <i>AddRoundKey</i>	94
Kode 4.12. Kode untuk transformasi <i>invSubBytes</i>	94
Kode 4.13. Kode untuk transformasi <i>invShiftRows</i>	95
Kode 4.14. Kode untuk transformasi <i>invMixColumns</i>	96
Kode 4.15. Kode penyisipan <i>LSB</i>	96
Kode 4.16. Kode untuk fungsi utama penyisipan	97
Kode 4.17. Kode untuk pergeseran bit.....	97
Kode 4.18. Kode untuk menandai akhir penyisipan	97
Kode 4.19. Kode untuk membentuk file <i>MP3Stego</i>	97
Kode 4.20. Kode untuk <i>looping</i>	97
Kode 4.21. Kode untuk menulis sisa <i>byte</i>	98
Kode 4.22. Kode untuk ekstraksi <i>LSB</i>	98
Kode 4.23. Kode inti fungsi utama ekstraksi	99
Kode 4.24. Kode untuk konversi ke string jika telah satu <i>byte</i>	99

Kode 4.25. Kode untuk mengambil pesan sampai <i>mark</i>	99
Kode 4.26. Kode untuk mengakhiri ekstraksi	99

BAB I

PENDAHULUAN

Bab pendahuluan ini menjelaskan tentang latar belakang dari pemilihan tema dan judul tugas akhir ini, rumusan masalah dalam pelaksanaan tugas akhir, tujuan dan manfaat yang dapat diperoleh, ruang lingkup yang menjadi batasan-batasan dari tugas akhir, dan sistematika penulisan dokumen tugas akhir ini.

1.1. Latar Belakang

Perkembangan teknologi sekarang ini yang tumbuh semakin pesat terutama di bidang internet dan multimedia telah memberikan kemudahan kepada masyarakat. Perkembangan ini tentu memberikan dampak positif dan dampak negatif. Dampak positif dari perkembangan teknologi internet antara lain adalah memberikan kemudahan dalam mendapatkan pesan atau data informasi. Sayangnya dengan berkembangnya teknologi ini tentu memberikan dampak negatif. Berbagai teknik yang *modern* banyak digunakan oleh orang yang tidak bertanggung jawab untuk dapat memperoleh data atau informasi yang bukan haknya, maka dari itu dengan semakin berkembangnya teknologi informasi ini juga harus berbanding lurus dengan perkembangan pengamanan data informasi.

File audio yang telah dikenal masyarakat umumnya antara lain MIDI, WAV, FLAC, dan MP3. Saat ini dokumen audio yang sering digunakan ialah audio MP3. Menurut (Arubusman, 2007), format kompresi audio MP3 saat ini menjadi yang terpopuler dan merupakan kompresi audio yang jauh lebih baik dari segi kapasitas dan kualitas, ditunjukkan dengan meluasnya penggunaan MP3 oleh banyak orang. Akan tetapi bukan hal yang mustahil, bahwa MP3 dapat digunakan untuk aplikasi keamanan informasi. MP3 memiliki ukuran yang relatif lebih besar daripada dokumen citra, sehingga memungkinkan lebih banyak data yang bisa disembunyikan dalam media ini. Dengan begitu, dalam beberapa waktu ke depan MP3 tidak hanya berfungsi sebagai media audio saja tetapi dapat berfungsi lebih banyak, salah satunya sebagai alternatif media penyimpanan pesan rahasia.

Steganografi merupakan sebuah seni dalam menyamarkan atau menyembunyikan pesan dimana tidak ada yang menyadari adanya pesan tersembunyi kecuali pengirim pesan dan penerima pesan yang dituju (Ariyus,

2008). Steganografi bersifat *nonrepudiation* sehingga dapat mencegah suatu pihak untuk menyangkal bahwa pesan tersebut berasal dari dirinya (Munir, 2006). Jika terdapat seseorang yang mencoba untuk membajak sebuah lagu dan mengklaim bahwa dirinyalah sebagai pemilik lagu tersebut dapat dibuktikan dengan penggunaan teknik steganografi.

Metode steganografi yang digunakan adalah metode *Low Bit Encoding* atau biasa dikenal dengan nama *Least Significant Bit (LSB)*. LSB adalah sebuah teknik steganografi dengan mengganti bagian tertentu dari bit-bit yang kurang berpengaruh dengan bit-bit informasi yang disisipkan. Penggunaan metode ini populer dikarenakan implementasinya yang sederhana dan dapat menyisipkan informasi lebih banyak dibandingkan dengan metode audio steganografi yang lain seperti *spread spectrum*, *echo hiding* ataupun *phase coding*. Namun pada perkembangannya diketahui bahwa penggunaan metode LSB pada audio steganografi rentan terhadap serangan analisis statistik dan proses steganalisis (Djebbar, 2010).

Untuk menjaga keamanan data lebih lanjut maka sebelum digunakan metode LSB untuk penyisipan pesan maka data dienkripsi terlebih dahulu. Enkripsi adalah proses pengubahan suatu pesan teks ke dalam bentuk kode atau sandi untuk mengamankan data dari pencurian (Ariyus, 2008), sehingga meskipun data yang disisipkan dapat diekstraksi, data yang diekstraksi masih aman karena masih dalam kondisi terenkripsi. Metode enkripsi yang digunakan adalah metode AES karena metode ini lebih fleksibel dan memiliki faktor keamanan yang lebih baik dari segi kunci maupun ukuran blok dibandingkan metode lain seperti Blowfish, Twofish, RC4, DES ataupun Triple DES dan untuk memecahkan kunci AES-128 bit maka terdapat $2^{128} = 3,4 \times 10^{38}$ kemungkinan kunci.

Riset terdahulu terkait dengan steganografi audio dengan LSB telah dilakukan oleh Aminah Rizki Lubis(2012). Aminah Rizki membuktikan suatu teknik penyembunyian pesan rahasia di dalam media audio MP3 dengan menggunakan metode penyisipan LSB. Hasil file keluaran yang dihasilkan mengalami perubahan rendah, hal ini dapat terlihat dari rata-rata nilai *Peak Signal To Noise Ratio* sebesar 99.5 % yang artinya bahwa hanya terjadi kerusakan audio 0.5 % dalam setiap file hasil keluaran yang dibandingkan dengan file asli yang menjadi masukannya.

Pada penelitian ini diterapkan sebuah aplikasi perangkat lunak yang dapat menyisipkan teks dengan konsep steganografi menggunakan metode LSB dan enkripsi pesan menggunakan algoritma AES ke dalam *file audio* MP3. Diharapkan dengan adanya aplikasi ini merupakan salah satu solusi dalam menjaga keamanan data agar dapat lebih terjamin, karena yang dapat mengambil dokumen yang tersembunyi hanya orang yang memiliki kata kunci untuk mengaksesnya.

1.2. Rumusan Masalah

Melihat latar belakang yang ada, dapat dirumuskan permasalahannya yaitu bagaimana menghasilkan suatu aplikasi steganografi menggunakan metode LSB dan algoritma AES yang memiliki output berupa stego file audio MP3 yang dapat menyimpan data informasi berupa pesan text dan dapat menampilkan kembali pesan informasi.

1.3. Tujuan dan Manfaat

Tujuan tugas akhir mengenai pembangunan aplikasi steganografi dan enkripsi dengan AES ini adalah :

1. Penelitian ini bertujuan untuk membangun sebuah sistem yang dapat menyisipkan pesan teks dengan menggunakan enkripsi AES ke dalam media audio MP3 dan memunculkan kembali pesan teks yang telah disisipi.
2. Penelitian ini bertujuan untuk mengetahui perubahan yang terjadi pada berkas audio MP3 setelah terjadinya proses penyisipan pesan dilihat dari :
 - a. Aspek *fidelity*, pengukuran menggunakan parameter SNR.
 - b. Aspek *recovery*, pengukuran menggunakan parameter nilai CER.
 - c. Aspek *robustness*, pengujian dilakukan dengan melakukan manipulasi terhadap sinyal MP3(*Bitrate, Mode Channel, Frequency Sampling*)
 - d. Aspek *security*, pengujian dilakukan dengan mencoba menggunakan kunci yang sesuai dan tidak sesuai (*AES*).

Manfaat dari penelitian tugas akhir ini adalah aplikasi steganografi audio MP3 ini diharapkan dapat dapat dimanfaatkan sebagai salah satu solusi dalam mengamankan pesan rahasia.

1.4. Ruang Lingkup

Pada tugas akhir ini terdapat beberapa pembatasan ruang lingkup agar nantinya pengerjaan tugas akhir ini tidak keluar dari target yang diharapkan, diantaranya adalah sebagai berikut.

1. Media penampung yang digunakan adalah file audio MP3.
2. File yang disisipkan berupa pesan teks dengan ukuran lebih kecil dibandingkan file pembawanya.
3. Key yang digunakan terbatas sebanyak 16 karakter untuk AES 128 bit, 24 karakter untuk AES 192 bit, dan 32 karakter untuk AES 256 bit .
4. Bahasa pemrograman yang digunakan adalah Java dengan bantuan IDE Netbeans.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dokumen tugas akhir ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan tentang hal-hal yang melatar belakangi dari pembuatan tugas akhir ini, rumusan permasalahan yang dikerjakan, tujuan dan manfaat yang diharapkan, ruang lingkup yang membatasi, dan sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang keseluruhan dari teori-teori yang digunakan dalam pengerjaan tugas akhir ini.

BAB III FASE *INCEPTION* DAN FASE *ELABORATION*

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan *Unified Process*. Pada Bab ini disajikan dua fase awal yaitu *Inception* dan *Elaboration*.

BAB IV FASE *CONSTRUCTION* DAN FASE *TRANSITION*

Bab ini membahas mengenai tahapan akhir dari pembangunan perangkat lunak untuk model pengembangan *Unified Process*. Pada Bab ini disajikan fase *Construction* yaitu fase untuk melakukan implementasi dan fase *Transition* untuk melakukan pengujian sistem.

BAB III PENUTUP

Bab ini berisi tentang kesimpulan dari pengerjaan tugas akhir ini, beserta dengan saran yang dapat diajukan guna pengembangan sistem ini ke depannya.