

IMPLEMENTASI STEGANOGRAFI AUDIO MP3 DAN WAV UNTUK FILE PDF PADA SMARTPHONE ANDROID DENGAN MENGGUNAKAN METODE LSB (*LEAST SIGNIFICANT BIT*)

Rita Siburian¹, Lindawati², Aryanti³

^{1,2,3}Teknik Telekomunikasi Politeknik Negeri Sriwijaya

Jl. Sriwijaya Negara, Bukit Besar, Ilir Barat 1, Kota Palembang, Sumatera Selatan

e-mail: ritasimatupang333@gmail.com¹, lindawati9111@yahoo.com², aryanti@polsri.ac.id³

Abstrak – Steganografi merupakan teknik yang digunakan untuk menyisipkan informasi di dalam media lainnya dengan tujuan menjaga keamanan informasi. Steganografi membutuhkan dua media, yaitu media penampung dan data yang akan disisipkan. Berkembang pesatnya ilmu teknologi dalam dunia telekomunikasi dapat memunculkan cara-cara baru bagi beberapa pihak yang berniat menyalah gunakan untuk mengancam keamanan informasi seperti hacker, cracker, carder, phreaker dan sebagainya. Untuk menghindari penyalahgunaan tersebut maka penelitian ini. Salah satu metode yang dapat digunakan dalam steganografi adalah Least Significant Bit (LSB). Cara kerja metode ini adalah Pesan yang sudah dienkripsi terlebih dahulu akan disembunyikan secara merata pada setiap region pada MP3 atau Wav yang sudah dibagi, dengan memodifikasi/mengganti bit LSB dari media penampung dengan bit-bit dari informasi yang akan disembunyikan. Dalam pembuatan aplikasi steganografi ini, penulis menggunakan bahasa pemrograman Java eclipse, karena program tersebut cukup mudah dan dapat dijalankan dalam sistem operasi smartphone android. Dalam penelitian ini hasil yang didapat adalah waktu dalam proses enkripsi suatu file WAV lebih cepat dari pada MP3 begitu juga proses deskripsinya.

Kata kunci – Steganografi, audio mp3 dan wav, metode LSB, java eclipse

I. PENDAHULUAN

Berkembang pesatnya ilmu teknologi dalam dunia telekomunikasi dapat memunculkan cara-cara baru bagi beberapa pihak yang berniat menyalahgunakan untuk mengancam keamanan informasi seperti *hacker*, *cracker*, *carder*, *phreaker* dan sebagainya. Apabila informasi berada pada pihak yang salah akan menimbulkan kerugian. Informasi yang harus diperhatikan adalah keamanan bagi informasi yang rahasia [1].

Steganografi merupakan salah satu metode yang dapat digunakan untuk menyembunyikan pesan dengan menggunakan media digital. Steganografi digital menggunakan media digital sebagai wadah penampung misalnya gambar, suara, teks, maupun video. Data rahasia yang disembunyikan juga dapat berupa gambar, audio, teks, maupun video. Dalam penelitian ini steganografi audio yang diimplementasikan.

Berkas audio dipilih sebagai media penampung data karena memiliki kapasitas yang lebih besar dibandingkan

dengan berkas teks maupun gambar. Selain itu berkas audio memiliki ukuran yang lebih kecil dibandingkan dengan berkas video. Audio digital memiliki ukuran yang proporsional sehingga memungkinkan untuk menyisipkan lebih banyak pesan rahasia [2].

Salah satu metode steganografi adalah LSB (*least significant bit*). Metode ini merupakan metode yang sederhana dan menggunakan algoritma yang tidak terlalu rumit sehingga tidak memerlukan resource yang besar untuk menggunakannya. Metode ini cocok digunakan pada berbagai macam perangkat seperti komputer atau telepon genggam yang memiliki memori yang relatif kecil dan tidak dapat melakukan proses yang terlalu rumit dalam waktu cepat. Prinsip kerja dari metode least significant bit adalah mengubah nilai bit paling rendah dari suatu sampel audio dengan bit pesan yang akan disisipkan [2].

Smartphone android yang terus berkembang dan semakin canggih sehingga mempermudah seseorang untuk bermain game, bermedia sosial, tidak sedikit juga manusia memanfaatkan *Smartphone* Androidnya untuk pekerjaan, salah satunya mengirim dan menerima data. *Smartphone* android yang selalu dibawa, menjadikan pekerjaan tersebut lebih mudah dapat dilakukan dimanapun.

Banyak jurnal yang membahas aplikasi keamanan data dengan steganografi, tetapi kebanyakan aplikasi tersebut berbasis aplikasi dekstop, hanya beberapa berbasis aplikasi *smartphone*. Dan aplikasi tersebut hanya dapat menyembunyikan pesan dalam bentuk audio MP3 atau audio WAV saja.

II. DASAR TEORI

A Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphia* yang artinya menulis, sehingga arti steganografi adalah "menulis (tulisan) terselubung". Dengan menggunakan steganografi, kita dapat menyisipkan pesan rahasia ke dalam media lain dan mengirimkannya tanpa ada yang menyadari keberadaan pesan tersebut. Steganografi adalah ilmu yang digunakan untuk menyisipkan data di dalam media lainnya. Steganografi membutuhkan dua media, yaitu penampung dan data yang akan disisipkan [3].

B Audio Steganografi

Audio steganografi adalah teknik penyisipan pesan rahasia dalam media suara (audio). Proses penyisipan pesan rahasia dalam sistem steganografi pada dasarnya dilakukan dengan mengidentifikasi media audio pembawa pesan, yaitu *redundant bit* yang mana dapat dimodifikasi tanpa merusak integritas dari media audio itu sendiri. Pengaplikasian steganografi pada berkas audio dapat dilakukan dengan berbagai teknik.

C Gerbang Logika

Gerbang (*gate*) logika adalah suatu rangkaian digital yang mempunyai satu atau lebih *input* dan hanya mempunyai satu *output*. *Output* gerbang logika ini tergantung sinyal yang diberikan pada *input*-nya. Hal ini dapat kita lihat pada persamaan aljabar Boole dan tabel kebenaran yang dimiliki oleh setiap gerbang logika. Aljabar Boole juga memberikan persamaan untuk setiap gerbang serta memberi simbol untuk operasi gerbang tersebut. Suatu rangkaian digital dapat dibangun dari sejumlah gerbang logika. Untuk setiap gerbang dan tabel kebenaran tiap gerbang logika, maka dengan menggabungkan beberapa gerbang ini akan didapat operasi logika sesuai dengan keinginan dan tujuan yang diharapkan sehingga terbentuklah suatu rangkaian digital yang akan membangun sistem yang diinginkan. Gerbang logika dasar adalah NOT, AND dan OR. Sedangkan gerbang NAND, NOR, XOR, XNOR merupakan gerbang yang dibentuk dari gabungan beberapa gerbang dasar [5].

D Gerbang XOR (*Exclusive OR*)

Apabila input A dan B ada dalam keadaan logika yang sama, maka output Q akan menghasilkan logika 0, sedangkan bila input A dan B ada dalam keadaan logika yang berbeda, maka output akan menjadi logika 1. XOR sebetulnya merupakan variasi dari cara kerja logika OR. Untuk lebih jelas, coba perhatikan tabel kebenarannya:



Gambar 2. Simbol Gerbang XOR

Tabel 1. Kebenaran logika XOR

Masukan		Keluaran
A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

kebenaran XOR ini hanya berbeda satu langkah saja dengan tabel kebenaran OR, yaitu pada langkah terakhir saat input A dan B keduanya pada logika 1, outputnya menghasilkan 0, bukan 1 seperti pada logika OR.

Aplikasi dari proses logika XOR ini dapat dimanfaatkan

untuk membandingkan dua buah data, yaitu apabila data-data tersebut mengandung informasi yang persis sama, maka XOR akan memberikan output logika 0 [6].

E Audio MP3

MPEG-1 Audio Layer 3 atau lebih dikenal sebagai MP3 adalah salah satu format berkas pengodean suara yang memiliki kompresi yang baik (meskipun bersifat *lossy*) sehingga ukuran berkas bisa memungkinkan menjadi lebih kecil. Berkas ini dikembangkan oleh seorang insinyur Jerman Karlheinz Brandenburg. MP3 memakai pengodean *Pulse Code Modulation* (PCM). MP3 mengurangi jumlah bit yang diperlukan dengan menggunakan model *psychoacoustic* untuk menghilangkan komponen-komponen suara yang tidak terdengar oleh manusia.

F Audio WAV

WAV adalah singkatan dari istilah dalam bahasa Inggris *waveform audio format* merupakan standar format berkas audio yang dikembangkan oleh Microsoft dan IBM. WAV merupakan varian dari format *bitstream* RIFF dan mirip dengan format IFF dan AIFF yang digunakan komputer Amiga dan Macintosh. WAV maupun AIFF kompatibel dengan sistem operasi Windows dan Macintosh. Walaupun WAV dapat menampung audio dalam bentuk terkompresi, umumnya format WAV merupakan audio yang tidak terkompres [7].

G Android

Android yaitu sebuah sistem operasi telepon seluler berbasis Linux. Android juga memiliki *platform* terbuka bagi seseorang yang ingin menciptakan aplikasi untuk digunakan oleh bermacam-macam peranti bergerak. Android juga merupakan sebuah sistem operasi untuk telepon seluler seperti halnya Symbian pada Nokia, *Palm* dan *Windows Mobile* yang sebelumnya sudah dikenal selama ini. Seiring dengan perkembangannya, android berubah menjadi *platform* yang begitu cepat dalam melakukan pembaruan. Awalnya, android dikembangkan oleh Android inc, yang didukung finansial dari pihak google, yang kemudian membelinya pada tahun 2005. Tahun 2007, sistem operasi ini telah resmi yang bersamaan dengan didirikannya *Open handset Alliance*, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak serta telekomunikasi yang tidak lain bertujuan untuk memajukan standar terbuka perangkat seluler. Android, inc didirikan pada bulan Oktober tahun 2003 oleh Andy Rubin, Christ White, Rich Miner dan Nick Sears di Palo Alto California yang bertujuan untuk mengembangkan perangkat seluler pintar yang lebih tahu akan lokasi dan preferensi penggunaannya [8].



Gambar 3. Logo Android [18]

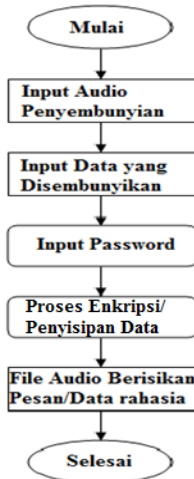
H Sejarah Eclipse

Eclipse awalnya dikembangkan oleh IBM untuk menggantikan perangkat lunak IBM Visual Age for Java 4.0. Sejak tahun 2006, Eclipse Foundation mengkoordinasikan peluncuran Eclipse secara rutin dan simultan yang dikenal dengan nama Simultaneous Release. Setiap versi peluncuran terdiri dari Eclipse Platform dan juga sejumlah proyek yang terlibat dalam proyek Eclipse. Tujuan dari sistem ini adalah untuk menyediakan distribusi Eclipse dengan fitur-fitur dan versi yang terstandarisasi.

III. METODELOGI PENELITIAN

A Proses Enkripsi (penyisipan) data

Proses ini dibutuhkan data masukan berupa audio, file pesan/data, dan kunci enkripsi/penyisipan yang akan digunakan. Sistem akan melakukan proses enkripsi pada audio dan data menggunakan metode LSB (*Least Significant Bit*).

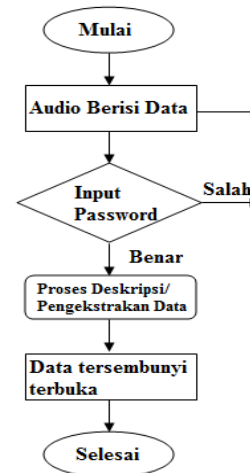


Gambar 4. Proses Enkripsi (penyisipan) data

B Proses Deskripsi (pengekstrakan) data

Proses ini dibutuhkan data masukan berupa audio yang mengandung pesan/file rahasia dan kunci untuk deskripsi data. Jika kata kunci benar maka sistem akan melakukan proses deskripsi pada audio, dengan mengambil bagian-bagian data dari bit-bit audio menggunakan metode LSB (*Least Significant Bit*). Sebaliknya jika kata kunci salah maka

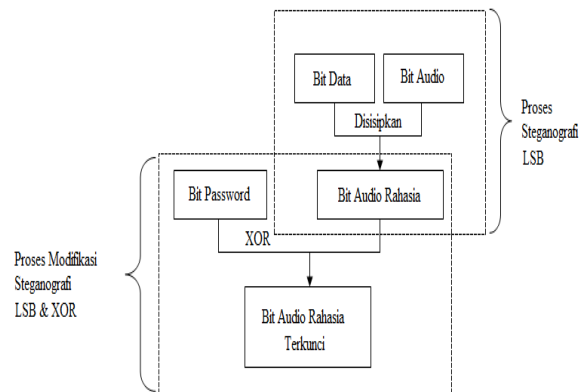
audio tidak akan melalui proses deskripsi, dan mendapatkan file audio pesan awal yang berisi pesan rahasia belum terbuka.



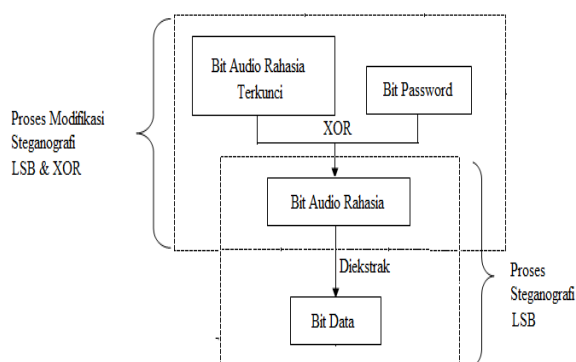
Gambar 5. Proses Deskripsi (pengekstrakan) data

C Pengembangan Metode

Metode yang akan dikembangkan dalam perancangan yaitu metode LSB (*Least Significant Bit*) dan memodifikasinya dengan gerbang logika XOR. Caranya mengganti bit-bit pada audio dan menyisipkan bit-bit data file yang akan disisipkan, serta memodifikasi lagi bit-bit tersebut dengan menggunakan logika XOR terhadap password yang dibuat.



Gambar 6. Modifikasi Metode Steganografi LSB dan Gerbang Logika XOR pada proses penyisipan



Gambar 7. Modifikasi Metode Steganografi LSB dan Gerbang Logika XOR pada proses pengestran

D Skenario Pengukuran Kualitas Audio

Pada hasil objek steganografi akan terdapat noise. Noise ini terjadi akibat perubahan bit yang dilakukan pada proses parity coding. Pengukuran noise pada objek steganografi dilakukan dengan menggunakan PSNR(Peak Signal to Noise Ratio). Noise ini dapat di dengar secara langsung ketika media objek steganografi di jalankan di pemutar musik. Secara matematis perhitungan noise akan memakai perhitungan nilai PSNR dengan nilai minimal 30 DB. Perhitungan PSNR ini dilakukan dengan memakai rumus persamaan :

$$PSNR = 10 \log_{10} \left(\frac{P_1^2}{P_1^2 + P_0^2 - 2P_1P_0} \right)$$

P1 adalah kekuatan sinyal berkas audio setelah proses penyembunyian pesan dan P0 adalah kekuatan sinyal awal. Jika nilai PSNR < 30 dB maka dapat dikatakan bahwa kualitas audio hasil steganografi buruk.

IV. HASIL DAN PEMBAHASAN

Hasil analisis, telah berhasil dikembangkan perangkat lunak yang memiliki fungsi untuk menyisipkan dan mengekstraksi pesan. Kemudian dilakukan pengujian untuk memeriksa kebenaran dari perangkat lunak tersebut, beserta kinerja perangkat lunak tersebut. Hasil penyembunyian audio MP3 ditunjukkan pada Tabel 1:

Tabel 1. Pengujian Enkripsi Audio MP3

File sisipan (MP3)		File yang disisipkan		Kunci	Waktu Penyisipan (S)	File setelah sisipan (Mp3)	
Judul Lagu	Size (KB)	Nama File	Size (KB)			Size (KB)	Nama File
Ibu_Kita_Kartini	1.122	BAB I – Copy.pdf	25	1234	56.696	_filesisipan6.mp3	1.122
Ibu_Pertiwi	10.348	Publikasi_09.11.3375.pdf	604	1234	14128.691	_filesisipan14.mp3	10.348

Dari Tabel 1 dapat dilihat semakin besar data yang disembunyikan maka semakin lama waktu yang dibutuhkan.

Hasil penyembunyian audio WAV ditunjukkan pada Tabel 2:

Tabel 2. Pengujian Enkripsi Audio WAV

File sisipan (Wav)		File yang disisipkan		Kunci	Waktu Penyisipan (S)	File setelah sisipan (Wav)	
Judul Lagu	Size (KB)	Nama File	Size (KB)			Size (KB)	Nama File
Ibu_Kita_Kartini	1.144	BAB I – Copy.pdf	25	1234	31.774	_filesisipan19.wav	1.144
Ibu_Pertiwi	11.398	Publikasi_09.11.3375.pdf	604	1234	1402.4972	_filesisipan15.wav	11.398

Dari Tabel 2 dapat dilihat semakin besar data yang disembunyikan maka semakin lama waktu yang dibutuhkan.

Hasil pengestrakan audio MP3 ditunjukkan pada Tabel 3:

Tabel 3. Pengujian Deskripsi Audio Mp3

File setelah sisipan (Mp3)		Kunci	Waktu (s)	Hasil	
Judul Lagu	Size (KB)			Judul Lagu	Size (KB)
_filesisipan6.mp3	1.122	1234	11.412	BAB I – Copy.pdf	25
_filesisipan14.mp3	10.341	1234	124.188	Publikasi_09.11.3375.pdf	604

Dari Tabel 3 dapat dilihat semakin besar data yang diekstrak maka semakin lama waktu yang dibutuhkan.

Hasil pengestrakan audio WAV ditunjukkan pada Tabel 4:

Tabel 4. Pengujian Deskripsi Audio Wav

File setelah sisipan (Wav)		Kunci	Waktu (s)	Hasil	
Judul Lagu	Size (KB)			Judul Lagu	Size (KB)
_filesisipan19.wav	1.144	1234	5.113	BAB I – Copy.pdf	25
_filesisipan15.wav	11.398	1234	121.119	Publikasi_09.11.3375.pdf	604

Dari Tabel 4 dapat dilihat semakin besar data yang diekstrak maka semakin lama waktu yang dibutuhkan.

Hasil pengujian PSNR audio asli dan audio hasil MP3 ditunjukkan pada Tabel 5:

Tabel 5. Pengujian PSNR Audio MP3

Audio Asli			Audio Hasil			Hasil Pengujian	
Judul Lagu	Size (KB)	P0	Judul Lagu	Size (KB)	P0	Judul Lagu	Size (KB)
Ibu_Kita_Kartini	1.122	-	_filesisipan6.mp3	1.122	-	Buku	11.2041
Ibu_Pertiwi	10.341	-	_filesisipan14.mp3	10.341	-	Buku	13.5278

Dari Tabel 5 dapat dilihat audio yang dihasilkan lebih kecil dari 30 dB jadi kualitas audio hasil MP3 buruk.

Hasil pengujian PSNR audio asli dan audio hasil WAV ditunjukkan pada Tabel 6:

Tabel 6. Pengujian PSNR Audio WAV

Audio Asli			Audio Hasil			Hasil Pengujian	
Judul Lagu	Size (KB)	P0	Judul Lagu	Size (KB)	P0	Judul Lagu	Size (KB)
Ibu_Kita_Kartini	1.144	-13.0294	_filesisipan 19.wav	1.144	-13.0288	Baik	87.5554
Ibu_Pertiwi	11.398	-16.8294	_filesisipan 15.wav	11.398	-16.8294	Baik	149.1931

Dari Tabel 6 dapat dilihat audio yang dihasilkan lebih besar dari 30 dB jadi kualitas audio hasil WAV baik.

Hasil pengujian diatas, didapatkan analisis bahwa dalam proses enkripsi. Semakin besar data yang ingin disisipkan maka semakin besar pula file audio yang dibutuhkan. Begitu juga dengan waktunya semakin besar data yang disisipkan maka semakin lama juga proses pengenkripsannya hal tersebut berlaku baik dalam pengenkripsian audio MP3 maupun WAV.

Sedangkan dalam proses deskripsi waktu yang dibutuhkan untuk mendeskripsikan audio kembali tidak terlalu lama. Dilihat dari pengujian deskripsi diatas juga berlaku semakin besar audio dan data yang di deskripsikan maka semakin besar atau lama pula proses pendeskripsian.

Pada kedua tabel enkripsi, waktu proses enkripsi pada audio MP3 lebih lama dari pada audio WAV, Begitu juga dengan proses deskripsinya.

Dari Tabel pengujian PSNR, Dapat dianalisis bahwa ada keterkaitan nilai objektif PSNR dengan nilai subjektif. Semakin besar nilai PSNR media maka semakin baik pula kualitas audio tersebut secara subjektif. Jika nilai PSNR yang didapat lebih kecil dari 30 dB maka akan terdengar *noise* yang sangat jelas terdengar oleh telinga manusia. Nilai PSNR ini sendiri dipengaruhi oleh dua hal yaitu besarnya pesan yang disembunyikan dan struktur media steganografi.

V. KESIMPULAN

Kesimpulan yang diperoleh setelah melewati tahap perancangan, pembuatan, serangkaian uji coba dan analisa pada penelitian ini, maka dapat dibuat suatu kesimpulan antara lain :

1. Steganografi audio dengan teknik LSB bias diterapkan pada berkas audio mp3 dan wav.
2. Kualitas besarnya berkas audio yang dihasilkan tergantung dari besarnya ukuran pesan. Semakin besar pesan yang dimasukkan maka semakin besar pula keluarannya.
3. Proses enkripsi waktu audio MP3 lebih besar dari pada audio WAV.
4. Proses deskripsi waktu audio MP3 lebih kecil dari pada audio WAV.
5. Hasil pengujian PSNR, Steganografi audio WAV lebih baik Hasil audionya dari pada WAV. Diterapkan Algoritma LSB pada proses enkripsi dan dekripsi, berjalan dengan baik sehingga isi audio tidak terbaca oleh pihak luar.

VI. SARAN

Beberapa saran yang perlu dipertimbangkan guna pengembangan aplikasi lebih lanjut, antara lain:

1. Pengembangan lebih lanjut dapat difokuskan pada penggunaan metode steganografi dengan kombinasi yang lain untuk meningkatkan keamanan data.
2. Dapat difokuskan pada kualitas hasil audio mp3 lebih baik.
3. Pengembangan lebih lanjut juga dapat dapat difokuskan pada penambahan kecepatan dalam mengenkripsi audio.

REFERENSI

- [1] Prima, Nikken and Bahtiar, Nurdin, "Kriptografi Hill Chiper dengan Menggunakan Operasi Matriks" in Seminar Nasional Ilmu Komputer Universitas Diponegoro ,2010 . ISSN 978-602-97737-0-5
- [2] Lovebbi, Dodick Z.S., " Rancang Bangun Aplikasi Steganografi dengan Metode Least Significant Bit di Audio pada Sistem Operasi Android", library.umh.ac.id, ISSN 2085-4552, Mei.2012.
- [3] (2010) UNIKOM Scholar Repository website.[online]. Available: <http://dir.unikom.ac.id/>
- [4] USU Repository website.[online]. Available: <http://repository.usu.ac.id/bitstream/123456789/20664/Chapter%20II.pdf>
- [5] Priadi, Prasetyo, "Gerbang Logika Digital", IlmuKomputer.Com, 2008.
- [6] (2016) Wikipedia website. [online]. Available: <https://id.wikipedia.org/wiki/Wav>
- [7] Guslita, Marsha., "Aplikasi Enkripsi dan Deskripsi sebagai Keamanan Data dan SMS menggunakan Metode Vigenere chiper berbasis Android", 2016.