Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma *Least Significant Bit (Lsb)*

[1]Jhoni Verlando Purba, [1]Marihat Situmorang, [1]Dedy Arisandi

[1]Program Studi S1 Teknologi Informasi
Fakultas Ilmu Komputer dan Teknologi Informasi
Universitas Sumatera Utara
E-mail: poerba@students.usu.ac.id

Abstrak-Kemajuan teknologi komputer yang sangat bermanfaat pada kehidupan manusia sekarang adalah kecepatan dalam menyampaikan informasi dari tempat yang jauh yaitu melalui Internet. Dalam pengiriman informasi tersebut terdapat masalah yang mengganggu keamanan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab yaitu dengan mengubah bahkan mengganti informasi data dalam sebuah media data wav yang disampaikan. Penulis menggunakan steganografi dengan metode modifikasi *Least Significant Bit* sebagai media yang akan menyembunyikan informasi berupa setiap nilai–nilai bit data ke dalam nilai–nilai bit media audio. Bit-bit data yang akan disembunyikan atau diamankan dengan LSB ke dalam media audio. Setelah di analisis dan diimplementasikan maka di peroleh bahwa nilai–nilai bit yang disisipkan ke dalam media audio masih tampak seperti normal sehingga tidak menimbulkan kecurigaan bagi orang yang mendengar. Kemudian jika diekstraksi maka akan didapat kembali nilai–nilai bit yang telah disisipkan tersebut secara utuh. Dengan demikian, kriteria–kriteria steganografi yang baik yaitu *imperceptibility*, *fidelity* dan *recovery* dapat terpenuhi.

Kata kunci :Modifikasi LSB (Least Significant Bits), Steganografi, Data wav.

I. PENDAHULUAN

Teknologi komunikasi dan informasi sangat berkembang dengan pesat dan memberikan pengaruh besar bagi seluruh kehidupan manusia. Sebagai contoh perkembangan jaringan internet yang memungkinkan setiap orang untuk saling bertukar data atau informasi melalui jaringan internet tersebut. Seiring dengan perkembangan jaringan internet, maka kejahatan atas teknologi komunikasi dan informasi juga turut berkembang dan maju, seperti yang sering kita dengar adalah *hacker*, *cracker*, *carder*, *phreaker* dan sebagainya [1].

Steganografi merupakan seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak dapat menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung" [2].

Teknik ini meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia. Yaitu Oleh bangsa Yunani. Herodatus, penguasa Yunani, mengirim pesan rahasia dengan menggunakan kepala budak sebagai media. Dalam hal ini, rambut budak dipotong, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, maka disruh untuk menyampaikan pesan rahasia di balik rambutnya kepada Aristagoras.

II. INDENTIFIKASI MASALAH

Sistem yang akan dibangun untuk menyisipkan Pesan *text* ke dalam media format WAV yang dilakukan dengan menerapkan metode Modifikasi *Least Significant Bit* (LSB). Metode Modifikasi *least Significant Bit* dengan mengubah nilai–nilai bit terakhir dalam satu byte ke dalam satu byte data audio. Dimana nilai–nilai byte data audio tersebut akan disusun dengan cara random agar tidak kelihatan oleh orang yang tidak berhak mengaksesnya. Maka dapat dibuat rumusan masalah yaitu : Bagaimana menyisipkan pesan *text* pada media format WAV dengan metode Modifikasi *Least Significant Bit* (LSB), Bagaimana kualitas *file* audio digital yang telah disisipkan pesan *text*, Bagaimana pengaruh ukuran data yang telah disisipkan pesan *text* atau informasi pada media format WAV.

Mencakup batasan masalah yang akan diteliti adalah Karakter yang akan disisipkan adalah semua karakter, Bahasa Pemrograman yang digunakan adalah Microsof Visual Basic 6.0, Cover object adalah Media WAV, Ukuran panjang pesan text disesuaikan dengan ukuran file .wav, Metode steganografi yang digunakan adalah Metode Modifikasi *Least Significant Bit* (LSB).

Dari permasalahan diatas, maka tujuan yang harus dicapai dan dilakukan dalam penelitian ini adalah sebagai berikut Bagamana Membagun sebuah Software aplikasi yang dapat menyisipkan pesan *text* atau informasi ke dalam media formar WAV, Menyembunyikan pesan rahasia agar tidak jatuh ke tangan orang yang tidak berhak mengaksesnya, Memberitahukan informasi bagaimana penerapan steganografi di dalam audio digital.

Manfaat yang diharapkan dari penelitian ini adalah dapat memperkaya literature mengenai pola pengenalan karakter dan menerapkan ilmu pengetahuan yang didapatkan penulis di masa kuliah serta menambah wawasan ilmu dan pemahaman kepada penulis dan pembaca tentang penggunaan metode Metode Modifikasi Least *Significant Bit* (LSB) dalam menyelesaikan penyisipan pesan *text* atau informasi ke dalam format WAV.

III. PENELITIAN TERDAHULU

Beberapa penelitian yang telah dilakukan untuk menyelesaikan penyisipan pesan text dengan menggunakan Metode Steganografi Berbasis Least Significant Bit dengan Penyisipan Variable-Size dan Penambahan Redundant Gaussian Noise. Pada bagian ini digunakan suatu metode steganografi berbasis *Least Significant Bit* untuk menjamin keamanan komunikasi. Ada dua kontribusi utama dari metode yang digunakan pertama *stego-image* diciptakan dengan metode yang digunakan untuk dapat menyelamatkan, tidak hanya pada sistem visualisasi manusia tetapi juga *common-cover carrier attack*. Ini dicapai oleh dua cara yaitu dengan penyisipan *variable-size* dan menambahkan *redundant Gaussian Noise*. Penyisipan *variable-size* melekatkan data rahasia sebagian *pixel cover-image* dengan sejumlah variable *Least Significant Bit.* Cara ini menyediakan suatu basis penempelan seperti *Gaussian noise* Penambahan *Gaussian noise* pada sisa *pixel cover-image* digunakan untuk meningkatkan distribusi *Gaussian* dalam menempelkan *noise.* Dengan cara ini perbedaan image mempunyai suatu distribusi Gaussian dan dapat bertahan dari *common cover carrier attack* [3].

Hasil yang dicapai pada penelitian Studi dan Implementasi *Steganography* metode LSB dengan Preprocessing Kompresi Data dan Ekspansi Wadah yaitu dengan melakukan *preorocessing* terlebih dahulu terhadap berkas data maupun berkas wadah yang akan digunakan, teknik steganografi ini mampu menyimpan data yang lebih besar dari kapasitas maksimum dari wadah sebenarnya [4].

Hasil yang dicapai pada penelitian Metode Least Significant Bit (LSB) dan END of FILE (EOF) untuk menyisipkan text ke dalam citra grayscale yaitu dengan metode *Least Significant Bit* akan menggantikan *bit* terakhir kode biner dari masing-masing piksel. Kelebihan metode ini tidak mengalami perubahan ukuran atau tampak seperti file normal yang dilihat oleh indra manusia, sehingga tidak mengakibatkan kecurigaan akan adanya pesan rahasia dalam citra. Sedangkan metode END of FILE akan meletakkan pesan di akhir citra sehingga ukuran file akan bertambah besar, oleh karena itu pesan teks yang disisipkan tidak terbatas jumlahnya [5].

IV. METODE PENELITIAN

A. Steganografi

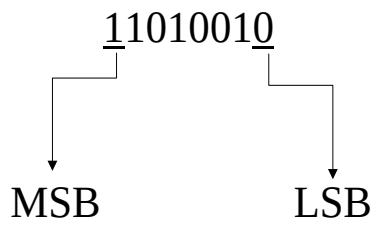
Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal [6].

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis [7].

Perbedaannya adalah hasil keluarannya yang dihasilkan. Hasil dari Kriptografi biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan dan dapat dikembalikan ke bentuk semula. Sedangkan Steganografi ini memiliki bentuk persepsi yang sama dengan bentukv aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya [8].

B. Metode Least Significant Bit

Metode *Steganografi* yang paling umum pada format suara adalah Modifikasi *Least Significant Bit*. Metode ini banyak digunakan karena komputasinya tidak terlalu kompleks dan pesan yang disembunyikan cukup aman. Strategi penyembunyian data pesan yang digunakan untuk menyisipkan kedalam media audio adalah dengan metode *Least Significant Bit* (LSB). Dimana bit data pesan akan digantikan dengan bit paling rendah dalam media audio.



Gambar 1 MSB dan LSB

MSB : *Most Significant Bit*
LSB : *Least Significant Bit*

Pada gambar 1, menandakan bahwa bit 1 dari depan menyatakan bit MSB dan bit 0 dari bilangan biner terakhir adalah bit LSB. Dapat dilihat contoh dibawah ini.

1. Jika pesan = 10 bit, maka jumlah byte yang digunakan = 10 byte

00110011 10100010 10100011 00100110
01011001 01101110 10110101 00010101
11100110 11011010

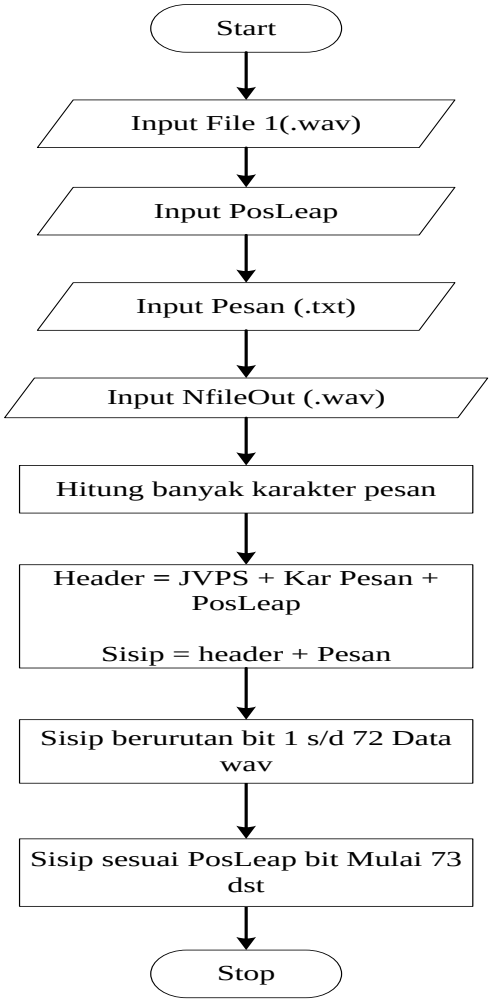
Misalkan binary dari *embedded message*: 1110101011
Hasil penyisipan pada bit LSB:

00110011 10100011 10100011 00100110
01011001 01101110 10110101 00010100
11100111 11011011

Pada contoh diatas, hanya sebagian yang berubah dari *Least Significant Bit*. Berdasarkan teori maka didapatkan bahwa ukuran file asli tidak mengalami perubahan yang begitu besar sehingga sulit terdeteksi oleh indra manusia.

C. Perancangan Flowchart Sistem

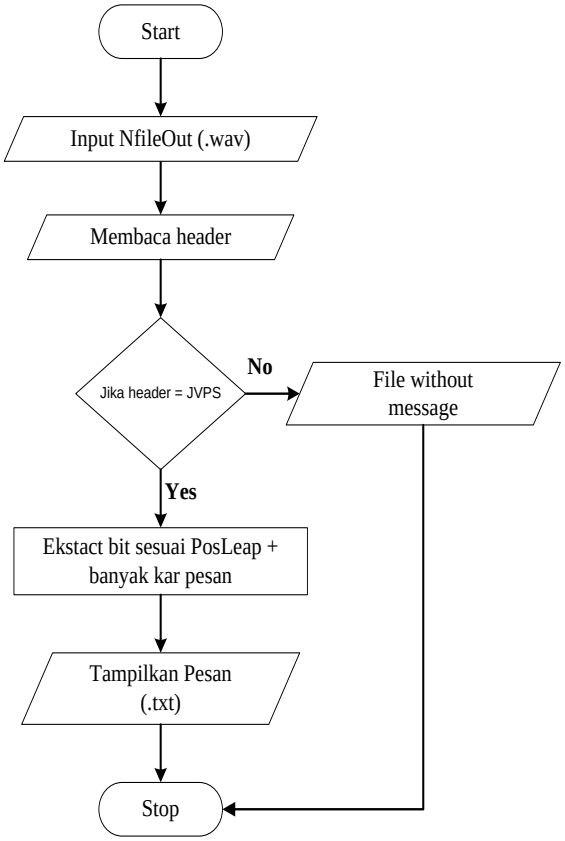
Untuk mempermudah suatu proses *embedding* maka diperlukan langkah-langkah pada gambar 2.



Gambar 2 Diagram Alur Pada Proses *Embedding*

Setelah Proses *embedding* berhasil di lakukan maka akan di dapatkan *file Stego* yang telah di sisipkan pesan tersebut. Sedangkan untuk mempermudah suatu proses *extracting* maka diperlukan langkah-langkah pada gambar 3.

pada extracting untuk mengambil pesan *text* atau informasi yang telah disisipkan ke dalam *file stego* maka dibutuhkan suatu proses pengekstraan agar pesan *text* atau informasi tersebut dapat di kembalikan tanpa mengubah bit-bit dari file audio yang digunakan.



Gambar 3 Diagram Alur Pada Proses *Extracting*

V. HASIL DAN PEMBAHASAN

A. Pengujian Data

Nama file penyisipan pesan : Bird.wav
Ukuran file 20.480 byte
Sebagian Data binary dari file ini diperlihatkan pada gambar berikut.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	52	49	46	46	24	4C	00	00	57	41	56	45	66	6D	74	20
00000010	10	00	00	00	01	00	01	00	22	56	00	00	22	56	00	00
00000020	01	00	08	00	64	61	74	61	00	4C	00	00	80	80	80	80
00000030	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000040	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000050	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000060	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000070	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000080	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80

Gambar 4 Data binery file Bird.wav

a. Analisis Untuk Posisi Leap 3

Misal pesan yang disisipkan adalah : FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI USU. Banyak karakter pesan yang disisipkan adalah 50 karakter Dengan Posisi leap 3 maka header menjadi JVPS + chr (50) + chr (0) + chr (0) + chr (0) + chr (3).

Karakter header digabungkan dengan karakter pesan sehingga diperoleh susunan kode ASCII sebagai berikut.

4a	56	50	53	32	00	00	00	03	46	41	4b	55	4c	54	41
53	20	49	4c	4d	55	20	4b	4f	4d	50	55	54	45	52	20
44	41	4e	20	54	45	4b	4e	4f	4c	4f	47	49	20	49	4e
46	4f	52	4d	41	53	49	20	55	53						

Gambar 5 Karakter Header dan karakter Pesan

Susunan kode ASCII diatas di konversikan menjadi kode binary, sehingga diperoleh seperti gambar 6.

010010100101011001010000010100110011001000000
000000000000000000000000001101000110010000010100101101010101001100010101000100000101010011001000000100100000100100101001100010011010101010100100000010010110100111101001101010100000101010101010001000101010100100010000001000100010000010100111000100000010101000100010101001011010011110010011111010011000100111101000111010010010010000001001001010011100100011001001111010100100010011010100000101010011010010010010000001010101010001101010101

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	52	49	46	46	24	4C	00	00	57	41	56	45	66	6D	74	20
00000010	10	00	00	00	01	00	01	00	22	56	00	00	22	56	00	00
00000020	01	00	08	00	64	61	74	61	00	4C	00	00	80	81	80	80
00000030	81	80	81	80	80	81	80	81	80	81	81	80	80	81	80	81
00000040	80	80	80	80	80	81	80	81	80	80	81	81	80	80	81	81
00000050	80	80	81	80	80	80	80	80	80	80	80	80	80	80	80	80
00000060	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000070	80	80	81	81	80	80	80	80	80	81	80	80	80	80	80	80
00000080	80	80	80	80	80	81	80	80	81	80	80	80	80	80	80	80
00000090	80	81	80	80	80	80	80	80	80	80	80	80	80	80	80	80
000000A0	80	80	80	81	80	80	80	80	80	81	80	80	80	80	80	80

Gambar 7 Tampilan Penyisipan dengan Leap 3

b. Analisis Penyisipan Dengan Posisi Leap 5

Misal pesan yang disisipkan adalah : FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI USU, Banyak karakter pesan yang disisipkan adalah 50 karakter Dengan Posisi leap 5 maka header menjadi JVPS + chr (50) + chr (0) + chr (0) + chr (0) + chr (5).

Karakter header digabungkan dengan karakter pesan sehingga diperoleh susunan kode ASCII sebagai berikut.

4a	56	50	53	32	00	00	00	05	46	41	4b	55	4c	54	41
53	20	49	4c	4d	55	20	4b	4f	4d	50	55	54	45	52	20
44	41	4e	20	54	45	4b	4e	4f	4c	4f	47	49	20	49	4e
46	4f	52	4d	41	53	49	20	55	53						

Gambar 8 Karakter Header dan karakter Pesan

Susunan kode ASCII diatas di konversikan menjadi kode binary, sehingga diperoleh seperti gambar 9.

01001010010101100101000001010011001100100000
00000000000000000000000001010100011001000001 01
00101101010101010011000101010001000001010100 1
10010000001001001010011000100110101010101001 0
00000100101101001111010011010101000001010101 0
10101000100010101010010001000000100010001000 0
01010011100010000001010100010001010100101101 0
01110010011110100110001001111010001110100100 1
00100000010010010100111001000110010011110101 0
01001001101010000010101001101001001001000000 1
01010101010011010101

Gambar 9 kode ASCII ke binary dengan Leap 5

Mulai bit ke 1 sampai bit ke 72 merupakan bit header. Bit-bit ini akan disisipkan secara berurut ke bit LSB file bird.wav mulai posisi ke 44 (posisi data wav). Posisi penyisipan header ini adalah byte ke 44,45,46,47,…, 116.

Bit ke 73 dan seterusnya akan disisipkan ke bit LSB file bird.wav dengan pertambahan posisi 5 dari posisi terakhir setiap penyisipan bit (posisi penyisipan byte ke 121, 126, 131, 136, dan seterusnya). Sehingga setelah penyisipan diperoleh file wav dengan data binary sebagai gambar 10.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	52	49	46	46	24	4C	00	00	57	41	56	45	66	6D	74	20
00000010	10	00	00	00	01	00	01	00	22	56	00	00	22	56	00	00
00000020	01	00	08	00	64	61	74	61	00	4C	00	00	80	81	80	80
00000030	81	80	81	80	80	81	80	81	80	81	81	80	80	81	80	81
00000040	80	80	80	80	80	81	80	81	80	80	81	81	80	80	81	81
00000050	80	80	81	80	80	80	80	80	80	80	80	80	80	80	80	80
00000060	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000070	80	81	80	81	80	80	80	80	80	80	80	80	80	81	80	80
00000080	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000090	80	81	80	80	80	80	81	80	80	80	80	80	80	80	80	80
000000A0	80	80	80	80	80	81	80	80	80	80	80	80	80	80	80	80

Gambar 10 Tampilan Penyisipan dengan Leap 5

c. Analisis Penyisipan Dengan Posisi Leap 7

Misal pesan yang disisipkan adalah : FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI USU, Banyak karakter pesan yang disisipkan adalah 50 karakter Dengan Posisi leap 5 maka header menjadi JVPS + chr (50) + chr (0) + chr (0) + chr (0) + chr (7).

Karakter header digabungkan dengan karakter pesan sehingga diperoleh susunan kode ASCII sebagai berikut.

4a	56	50	53	32	00	00	00	07	46	41	4b	55	4c	54	41
53	20	49	4c	4d	55	20	4b	4f	4d	50	55	54	45	52	20
44	41	4e	20	54	45	4b	4e	4f	4c	4f	47	49	20	49	4e
46	4f	52	4d	41	53	49	20	55	53						

Gambar 11 Karakter Header dan karakter Pesan

Susunan kode ASCII diatas di konversikan menjadi kode binary, sehingga diperoleh seperti gambar 12.

010010100101011001010000010100110011001000000
000000000000000000000000011101000110010000010
001011010101010100110001010100010000010101001
100100000010010010100110001001101010101010010
000001001011010011110100110101010000010101010
101010001000101010100100010000001000100010000
010100111000100000010101000100010101001011010
011100100111101001100010011110100011101001001
001000000100100101001110010001100100111101010
010010011010100000101010011010010010010000001
010101010100110101010101

Gambar 12 kode ASCII ke binary dengan Leap 7

Mulai bit ke 1 sampai bit ke 72 merupakan bit header. Bit-bit ini akan disisipkan secara berurut ke bit LSB file bird.wav mulai posisi ke 44 (posisi data wav). Posisi penyisipan header ini adalah byte ke 44,45,46,47,…, 116.

Bit ke 73 dan seterusnya akan disisipkan ke bit LSB file bird.wav dengan pertambahan posisi 5 dari posisi terakhir setiap penyisipan bit (posisi penyisipan byte ke 123, 130, 137, 144, dan seterusnya). Sehingga setelah penyisipan diperoleh file wav dengan data binary sebagai gambar 13.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	52	49	46	46	24	4C	00	00	57	41	56	45	66	6D	74	20
00000010	10	00	00	00	01	00	01	00	22	56	00	00	22	56	00	00
00000020	01	00	08	00	64	61	74	61	00	4C	00	00	80	81	80	80
00000030	81	80	81	80	80	81	80	81	80	81	81	80	80	81	80	81
00000040	80	80	80	80	80	81	80	81	80	80	81	81	80	80	81	81
00000050	80	80	81	80	80	80	80	80	80	80	80	80	80	80	80	80
00000060	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000070	80	81	81	81	80	80	80	80	80	80	80	80	80	80	80	80
00000080	80	81	80	80	80	80	80	80	80	80	80	80	80	80	80	80
00000090	80	80	80	80	80	80	80	80	80	80	80	80	80	81	80	80
000000A0	80	80	80	80	81	80	80	80	80	80	80	80	80	80	80	80

Gambar 13 Tampilan Penyisipan dengan Leap 7

VI. KESIMPULAN

Setelah melakukan studi literatur, perancangan, analisis, implementasi dan pengujian aplikasi untuk steganografi pesan text ke dalam media audio dengan metode Modifikasi *Least Significant Bit* maka dapat disimpulkan bahwa Steganografi data berupa pesan text atau informasi data ke dalam media audio dapat diimplementasikan menggunakan metode modifikasi *Least Significant Bit* yaitu dengan mengkonversikan setiap nilai–nilai bit data kedalam nilai–nilai bit media audio, Ukuran dari daya tampung media audio tidak mempengaruhi seberapa besar jumlah data yang dapat disembunyikan. Ukuran media audio harus lebih besar dari jumlah data yang akan disembunyikan atau diamankan, Perubahan yang terjadi pada *steganografi* tidak signifikan dan masih tampak seperti audio normal karena bit yang mempengaruhi pada media audio adalah byte yang terendah dan saran Agar keamanan dan kualitas audio *steganografi* lebih baik lagi dapat dilakukan penyembunyian secara random yaitu posisi peletakan nilai bit data ke bit audio tidak lagi berurutan mengikuti titik awal, Untuk penelitian berikutnya perlu dikembangan lagi system yang modifikasinya dapat meyembunyikan beberapa file.

DAFTAR PUSTAKA

[1]Sukrisno, 2007, "*Implementasi Steganografi Teknik Eof Dengan Gabungan Enkripsi Rijndael,Shift Cipher Dan Fungsi Hash Md5",* Jurusan Sistem Informasi, Stmik Amikom, Yogyakarta.

[2]Sellers, 1996, "*An Introduction to Steganography",* University of Cape Town, South Africa

[3]Krisnandi, Dikdik, 2004, "Metode *Steganography* Berbasis *least significant bit* dengan penyisipan Variable-Size dan Penambahan Redundant Gaussian Noise", program Magister Teknik Elektro, Institut Teknologi bandung.

[4]Hakim, Muhammad, 2007, "Studi dan Implementasi *Steganography* Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah", Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.

[5] Krisnawati, 2008, Metode Least Significant Bit (LSB) dan END of FILE (EOF) untuk menyisipkan text ke dalam citra grayscale, Jurusan Manajemen Informatika, Stmik Amikom, Yogyakarta.

[6] Kipper, Greg, 2004.*Investigator's Guide to Steganography.*Washington:Auerbach.

[7]Cox, Ingemar J,(2008), *"Digital Watermarking and Steganography Second Edition*", Poytechnic University, Fox, Virginia.

[8] Bender, W, (1996), *"Techniques For Data Hiding"*, IBM system journal vol 35, Nos 3&4, Germany.