

ABSTRAK

Saat ini kepopuleran dari MP3 sudah sangat meluas dan mendunia. Format kompresi audio MP3 saat ini menjadi yang terpopuler walaupun sudah terdapat jenis kompresi audio yang jauh lebih baik (dalam kapasitas) dan memiliki kualitas jauh lebih baik.

Kopopuleran dari MP3 ini tidaklah heran jika digunakan untuk aplikasi keamanan informasi. Teknik steganografi sudah dikenal sejak 2500 tahun yang lalu, dimana teknik ini sering digunakan pada jaman kerajaan Yunani.

Berbeda dengan teknik kriptografi yang dengan mudah dideteksi keberadaannya (walaupun sulit untuk dimengerti), steganografi menyamarkan keberadaan dari pesan yang ingin disampaikan. Beberapa teknik yang digunakan adalah menyamarkan pesan dalam bentuk file multimedia. Sekarang ini dikenal luas teknik untuk menyamarkan yaitu *digital watermarking*.

Salah satu teknik lainnya adalah menggunakan file dalam format audio yang dapat disisipi pesan yang ingin disampaikan. Teknik ini mungkin untuk dilakukan karena sifat dari file audio yang berlebihan (*redundant*) sehingga dengan teknik pengompresian menggunakan MP3 dapat menghilangkan informasi yang tidak signifikan bila dihilangkan. Sehingga dengan teknik ini pesan atau data dapat disisipkan pada file ini dengan mengganti informasi yang tidak dibutuhkan pada kompresi dengan data tersebut.

Karena kelemahan dari pendengaran manusia yang memiliki cakupan frekuensi dan atenuasi yang luas sehingga dapat dimanipulasi. Dengan menggunakan musik yang keras, seperti heavy metal, maka perubahan yang terjadi tidak akan mudah terdeteksi oleh pendengaran manusia.

Maka teknik audio steganografi dalam MP3 merupakan salah satu teknik yang sangat baik untuk menyamarkan data yang ingin dikirimkan untuk menghindari pihak-pihak yang tidak berhak.

ABSTRACT

Currently, the popularity of MP3 is very widespread and foremost. MP3 audio compression format now become the most popular, although there is the type of audio compression that is far better (in capacity) and have much better quality.

MP3 famous wonder if this is not used for the application of information security. Steganography techniques have been known since 2500 years ago, where this technique is often used at the time the Greek empire.

Contrasting with the cryptographic techniques that easily detect its existence (although difficult to understand), steganography disguise the existence of the message you want to be. Several techniques are used disguise the message in the form of multimedia files. Now this technique known to disguise the digital watermarking. One other technique is to use the audio file in a format that can disisipi want the message delivered. This technique perhaps to be done because of the nature of the audio file excessive (Redundant) so use compras techniques with MP3 can remove information that is not significant when removed. So with this technique messages or data can be pasted on this File change with the information that is not needed on the compression of data.

Because of the weakness of human hearing, which has a frequency coverage and a wide that can be manipulated. With the use of loud music, such as heavy metal, then the changes that occur will not be easily detected by human hearing. But techniques in the MP3 audio steganography one of the techniques that are very good to disguise the data you want to be sent to the parties who are not entitled.

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	iv
DAFTAR DIAGRAM	v
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan	2
1.4 Pembatasan Masalah	2
1.5 Sistematika Penulisan Laporan.....	2
BAB II DASAR TEORI	
2.1 Mp3	4
2.1.1 Pengertian Mp3	4
2.1.2 Sejarah Mp3.....	4
2.2. Steganografi	6
2.2.1 Sejarah Steganografi.....	6
2.2.2 Digital Watermaking.....	7
2.2.3 Steganalysis dan Penggunaan Steganografi	10
BAB III ANALISA DAN PEMODELAN	
3.1 Deskripsi Umum Perangkat Lunak.....	11
3.2 Arsitektur Aplikasi	11
3.2.1 Use Case Diagram	11
3.2.2 Activity Diagram	12
3.2.3 Class Diagram	14
3.3 Layout Aplikasi.....	16

BAB IV PERANCANGAN DAN IMPLEMENTASI	
4.1 Perancangan Sistem	20
4.2 Implementasi.....	26
BAB V PENGUJIAN	
5.1 Whitebox Testing	27
5.2 Blackbox Testing.....	30
BAB VI KESIMPULAN DAN SARAN	
1.1 Kesimpulan	32
1.2 Saran.....	32
DAFTAR PUSTAKA.....	33
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1. Teknik Penyusunan Gambar Yang Membentuk Gambar Lain	9
Gambar 3.1. Teknik Penyusunan Gambar Yang Membentuk Gambar Lain	11
Gambar 3.2. Activity Sisip Pesan	12
Gambar 3.3. Activity Tampil Pesan	13
Gambar 3.4. Activity Sisip File	13
Gambar 3.5. Activity Tampil File.....	14
Gambar 3.6. Layout Menu Utama	16
Gambar 3.7. Layout Sisip Pesan	17
Gambar 3.8. Layout Sisip File	18
Gambar 3.9. Layout Sisip File	19
Gambar 4.1. Antar Muka Menu Utama	21
Gambar 4.2. Antar Muka Olah Pesan	22
Gambar 4.3. Antar Muka Olah File	23
Gambar 4.4. Antar Muka Tentang	23

DAFTAR DIAGRAM

Diagram 3.1	Class Diagram Aplikasi	14
Diagram 3.2.	Class Diagram Stegano.....	15
Diagram 3.3.	Class Diagram Tampil.....	15
Diagram 3.4.	Class Diagram Sisip.....	16