STEGANOGRAFI PARITY CODING TERHADAP PESAN TEKS TERENKRIPSI AES PADA FILE AUDIO FORMAT MP3

Skripsi

oleh
I WAYAN WIASTA GUNA
22084516

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2014

STEGANOGRAFI PARITY CODING TERHADAP PESAN TEKS TERENKRIPSI AES PADA FILE AUDIO FORMAT MP3

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

I WAYAN WIASTA GUNA
22084516

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2014

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

STEGANOGRAFI PARITY CODING TERHADAP PESAN TEKS TERENKRIPSI AES PADA FILE AUDIO FORMAT MP3

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 20 Januari 2014

I WAYAN WIASTA GUNA
22084516

HALAMAN PERSETUJUAN

Judul Skripsi	:	STEGANOGRAFI PARITY CODING TERHADAP PESAN TEKS TERENKRIPSI AES PADA FILE AUDIO FORMAT MP3
Nama Mahasiswa	:	I WAYAN WIASTA GUNA
N I M	:	22084516
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2013/2014

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 20 Januari 2014

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Junius Karel, M.T.

HALAMAN PENGESAHAN

STEGANOGRAFI PARITY CODING TERHADAP PESAN TEKS TERENKRIPSI AES PADA FILE AUDIO FORMAT MP3

Oleh: I WAYAN WIASTA GUNA / 22084516

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 20 Januari 2014

Yogyakarta, 20 Januari 2014
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Junius Karel, M.T.
3. Erick Purwanto, S.Kom, M.Com.
4. Yuan Lukito, S.Kom., M.Cs.

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan karunianya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Steganografi Parity Coding terhadap pesan teks terenkripsi AES pada file audio format MP3".

Laporan ini disusun sebagai bentuk pertanggungjawaban penulis terhadap penelitian yang telah dilakukan selama satu semester. Sekaligus sebagai syarat untuk memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggung jawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Penulis menyadari bahwa laporan dan penelitian ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar – besarnya kepada:

1. Bapak Willy Sudiarto Raharjo, SKom.,M.Cs. selaku dosen pembimbing I yang pertama yang selalu sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
2. Bapak Junius Karel, S.Si., M.T. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas
3. Bapak Wija dan Ibu Astari selaku orang tua yang telah mendukung penulis baik berupa materil maupun spritual.
4. Dek Adi Wiasta dan keluarga besar di Tabanan-Ubud yang selalu memotivasi penulis.
5. Agustina yang selalu memberikan semangat dan banyak meluangkan waktu untuk membantu, mendengarkan dan menemani penulis selama proses pengerjaan penelitian ini.

6. Teman teman kontrakan Widnyana Raharja, dan Wawan Santika yang selalu memberikan kritikan dan saran kepada penulis.
7. Teman teman KMHD UKDW yang selalu memotivasi penulis.
8. Sahabat perguruan Pencak Silat yang selalu mendukung setiap keputusan yang diambil oleh penulis.
9. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
10. Pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis berharap adanya kritik dan saran sehingga penelitian yang akan dilakukan selanjutnya dapat lebih baik.

Akhir kata penulis meminta maaf bila ada kesalahan dalam penyusunan laporan maupun sewaktu penulis melakukan penelitian Tugas Akhir. Semoga penelitian dan laporan Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, Januari 2014

Penulis

INTISARI

Steganografi Parity Coding terhadap pesan teks terenkripsi AES pada file audio format MP3

Penggunaan teknologi semakin lama semakin berkembang, dimana internet digunakan sebagai sarana komunikasi maupun pertukaran informasi oleh banyak orang. Disamping itu internet mempunyai kelemahan yang susah untuk ditanggulangi, faktanya banyak kasus bocornya pesan maupun penyadapan yang sering disalah gunakan oleh para hacker. Maka dari itu aspek keamanan dan kerahasiaan informasi merupakan aspek yang sangat penting dalam perkembangan dunia informasi.

Untuk mengatasi permasalahan tersebut, diperlukan cara untuk mengamankan informasi yang akan dikirim agar tidak disalahgunakan oleh pihak pihak tertentu yang ingin mengambil keuntungan dari pertukaran informasi tersebut. Pada penelitian ini akan dibangun sebuah sistem keamanan yang memadukan metode *AES* dan *Parity Coding*. Sistem yang dibangun menyandikan pesan rahasia dengan metode *AES* serta menyisipkan dengan metode *Parity Coding* ke dalam media format MP3.

Hasil dari penelitian ini, proses enkripsi dengan *AES* file mengalami perubahan ukuran dikarenakan *padding* agar pesan memenuhi syarat perhitungan *AES* yang berjalan pada 128 bit. Selain itu media MP3 sebagai penampung tidak mengalami perubahan ukuran, setelah dilakukan proses penyisipan dengan metode *Parity Coding* akan tetapi suara *noise* akan semakin terdengar apabila karakter pesan yang akan disisipkan semakin panajang.

Kata Kunci : *Algoritma, Kriptografi*, *AES, Steganografi, Parity Coding.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Steganografi Parity Coding terhadap pesan teks terenkripsi AES pada file audio format MP3

Penggunaan teknologi semakin lama semakin berkembang, dimana internet digunakan sebagai sarana komunikasi maupun pertukaran informasi oleh banyak orang. Disamping itu internet mempunyai kelemahan yang susah untuk ditanggulangi, faktanya banyak kasus bocornya pesan maupun penyadapan yang sering disalah gunakan oleh para hacker. Maka dari itu aspek keamanan dan kerahasiaan informasi merupakan aspek yang sangat penting dalam perkembangan dunia informasi.

Untuk mengatasi permasalahan tersebut, diperlukan cara untuk mengamankan informasi yang akan dikirim agar tidak disalahgunakan oleh pihak pihak tertentu yang ingin mengambil keuntungan dari pertukaran informasi tersebut. Pada penelitian ini akan dibangun sebuah sistem keamanan yang memadukan metode *AES* dan *Parity Coding*. Sistem yang dibangun menyandikan pesan rahasia dengan metode *AES* serta menyisipkan dengan metode *Parity Coding* ke dalam media format MP3.

Hasil dari penelitian ini, proses enkripsi dengan *AES* file mengalami perubahan ukuran dikarenakan *padding* agar pesan memenuhi syarat perhitungan *AES* yang berjalan pada 128 bit. Selain itu media MP3 sebagai penampung tidak mengalami perubahan ukuran, setelah dilakukan proses penyisipan dengan metode *Parity Coding* akan tetapi suara *noise* akan semakin terdengar apabila karakter pesan yang akan disisipkan semakin panajang.

Kata Kunci : *Algoritma, Kriptografi*, *AES, Steganografi, Parity Coding.*

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Seiring berkembangnya teknologi komunikasi dewasa ini, cara manusia berkomunikasi ikut berubah. Cara berkomunikasi konvesional seperti mengirim surat melalui pos sudah ditinggalkan oleh kalangan manusia pada umumnya. Mereka sudah beralih menggunakan internet sebagai sarana komunikasi dengan sesamanya. Internet membuat komunikasi menjadi antar manusia lebih mudah, cepat dan bisa dilakukan dimanapun mereka berada. Disamping itu, internet mempunyai kelemahan yang susah untuk ditanggulangi, kelemahan tersebut yaitu penyadapan data atau informasi yang dikirimkan melalui internet. Saat ini para hacker sudah sangat pandai untuk melakukan penyadapan tersebut, mulai dengan menggunakan tools sampai membuat algoritma sendiri untuk menyadap informasi yang melalui internet. Aspek keamanan informasi dalam komunikasi melalui internet sangatlah penting untuk di perhatikan. Untuk hal tersebut dibutuhkan metode-metode untuk mengamankan informasi atau data yang di kirim melalui internet.

Kriptografi merupakan solusi dan salah satu metode untuk melindungi data, menjaga kerahasiaan, keaslian dan dapat meningkatkan aspek keamanan data atau informasi. Penggunaan kriptografi dirasakan masih kurang efisien, ini dibuktikan karena file yang sudah terenkripsi, sangatlah mencolok sehingga setiap orang sadar bahwa di dalamnya terdapat pesan yang sangat rahasia. Sehingga usaha untuk memecahkan kode enkripsi yang dikenal *Kriptaanalis* tidak dapat dihindarkan lagi.

Steganografi merupakan seni atau studi menyembunyikan informasi dengan cara menyisipkan pesan rahasia dalam suatu media. Medium ini disebut *cover object*.

Berbeda dengan Kriptografi, steganografi didesain untuk menyembunyikan pesan seolah-olah tidak ada sesuatu yang mencurigakan didalamnya. Salah satu metode dari steganografi adalah *Parity Coding*. Pada teknik Parity Coding sinyal dari berkas audio dipecah menjadi beberapa region berbeda dan setiap region tersebut akan disisipi setiap bit dari pesan rahasia..

Dengan memadukan metode kriptografi AES dan steganografi Pariti Coding, penulis mencoba membuat sistem yang mana akan menyembunyikan pesan ke dalam file audio. Namun sebelumnya pesan tersebut disandikan dengan Algoritma AES. Dengan cara tersebut diharpakan pesan yang ter*enkripsi* oleh AES tidak akan terlihat mencolok dikarenakan disisipkan dengan metode Parity Coding ke dalam audio.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka permasalahan yang akan diteliti oleh penulis adalah:

1. Bagaimana dampak file audio yang telah disisipi file *.aes* (file yang terenkripsi dengan algoritma AES) oleh metode Parity Coding, dilihat dari ukuran file serta kualitas suara?
2. Apakah terjadi perubahan dalam file *.aes* setelah disisipi dan diekstrak oleh metode Parity coding serta dampaknya terhadap pesan didalamnya?

1.3 Batasan Sistem

Dengan memadukan 2 metode yang berbeda maka batasan sistem perlu dibuat untuk memudahkan penulis dalam pembuatan sistem. Adapun batasan-batasan sebagai berikut:

1. File audio yang digunakan sebagai media steganografi adalah *Mp3*.
2. File yang dienkripsi dengan algoritma AES adalah file yang berformat *.txt*.
3. Panjang kunci yang dipakai adalah 128 bit.

4. Dalam penulisan pesan karakter yang didukung hanya ASCII.
5. Panjang maksimal pesan berjumlah 1000 karakter.

1.4 Tujuan Penelitian

1. Mengimplementasikan kriptografi algoritma AES 128 bit.
2. Mengimplementasikan steganografi Audio dengan metode Parity Coding.
3. Menguji kemampuan kemampuan system terpadu kriptografi dan steganografi dalam hal *recovery data*, waktu, dan *SNR*

1.5 Metode Penelitian

1. Studi Pustaka dengan mengumpulkan informasi yang berhubungan dengan metode Kriptografi AES dan Steganografi Parity Coding.
2. Analisis masalah dengan memahami cara kerja enkripsi dan deskripsi algoritma AES 128 bit, serta memahami cara kerja Setganografi Parity Coding untuk menyelesaikan masalah yang dijelaskan sebelumnya.
3. Melakukan perancangan sistem yang meliputi: arsitektur perancangan data, perancangan antarmuka, dan perancangan prosedural sistem.
4. Pengujian dilakukan dengan cara mencari seberapa besar efisiesn waktu yang dikerjakan oleh sistem, serta mencari kesalahan yang ada dalam sistem.
5. Membandingkan hasil output yang dihasilkan oleh sistem dengan input yang berbeda. Evaluasi kinerja program.

1.6 Sistematika Penulisan

Bab 1: Pendahuluan

Bab ini berisikan tentang Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Hipotesis, Tujuan Penelitian, Metode, dan Sistematika Penulisan.

Bab 2: Landasan Teori

Bab ini memberikan penjelasan tentang pengertian *Kriptografi* dan *Steganografi*, serta daftar pustaka dan teori pendukung yang berhubungan dengan perhitungan Algoritma AES dan Parity Coding.

Bab 3: Perancangan Sistem

Bab ini membahas tentang analisa dari algoritma yang digunakan untuk implementasi program beserta perancangan sistem, input, dan output program.

Bab 4: Implementasi dan Analisis Sistem

Berisi implementasi program berupa *interface*/tampilan program. Disertakan input dan output program, penjelasan, pengujian, dan analisa dari sistem kerja program.

Bab5: Kesimpulan dan Saran

Bab ini berisikan kesimpulan dari hasil perancangan program aplikasi secara keseluruhan dari dan saran saran yang memungkinkan untuk perkembangan dari program lebih lanjut.

BAB 5

KESIMPULAN & SARAN

5.1 Kesimpulan

Dari proses pengerjaan Tugas Akhir ini, ada beberapa hal yang dapat penulis simpulkan yaitu:

1. Penyisipan dengan metode *Parity Coding* tidak mengubah ukuran file MP3 sama sekali, hanya merubah bit ke delapan dari *bit parity* region bila ada perbedaan dengan *bit parity* pesan agar memiliki nilai yang sama, apabila bit parity region sama dengan bit parity pesan maka tidak ada perubahan sama sekali. Selain itu dalam perhitungan *parity coding* tidak ada penambahan karakter seperti *padding* pada AES karena tidak ada syarat khusus untuk ketentuan panjang *bit parity* region maupun *bit parity* pesan.
2. Hasil dekripsi dari *chipertext* yang sebelumnya mengalami proses penyisipan dan ekstrasi tidak mengalami perubahan baik dari sisi ukuran maupun isi pesan, hal ini dikarenakan pada *byte* ke lima MP3 disisipkan jumlah panjang dari blok *chipertext* agar program bisa menentukan jumlah panjang dari bit bit yang akan dilakukan proses ekstrasi, sehingga menghasilkan jumlah ukuran dari *chipertext* yang sama dengan sebelum mengalami proses penyisipan, tanpa kehilangan atau ketambahan jumlah bit.

5.2 Saran

1. Dapat menerapkan metode *AES* dengan menggunakan kunci 192 bit adan 256 bit, atau menggunakan metode penyandian yang lain seperti: *Twofish, Blowfish.*
2. Menggunakan media lain yang akan digunakan untuk menyembunyikan pesan rahasia seperti: video, gambar dan media lainnya. Dan tentu saja menggunakan algrotma Steganografi yang lain seperti: *LSB*, *Spread-Spectrum*.

DAFTAR PUSTAKA

Dony, Ariyus. (2005). "*Kriptografi Keamanan Data dan Komunikasi*". Yogyakarta: Penerbit Andi Offset.

Dony, Ariyus. (2009). "*Keamanan Multimedia*". Yogyakarta: Penerbit Andi Offset

Herianto. (2008). "*Pembangun Perangkat Lunak Steganografi Audio MP3 dengan Teknik Parity Coding pada Perankat Mobile Phone"*

Kurniawan, Yusuf. (2004). *"Kriptografi Keamanan Internet dan Jaringan Komunikasi*". Bandung: Penerbit Informatika

Munir, Rinaldi. (2006). "*Kriptografi*". Bandung : Penerbit Informatika.

Raissi, Rasol. (2002.). *"The Theory Behind MP3"*.http://www.mp3-tech.org/programmer/docs/mp3_theory.pdf. Diakses pada 1 maret 2013.

Rifki, Sadikin. (2012). "*Kriftografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java"*. Yogyakarta: Penerbit Andi Offset.

Riko, Saragih. (2006). "*Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganografi"*

Schneier, B., Oorschot, P., & Venstone, S. (1996). Handbook of Applied Cryptography.USA:Minneapolis

Stallings , Wiliam. (2003). "*Chryptography and Network Security Principles and Practice Third Edition"*. USA: Prentice Hall.

Schenier, Bruce . (1998). "*Performance Comparasion of the AES Submission*" Damen,John. Dan Rijmen, Vincent. AES Proposal: Rijndael. Brussel, Belgium.

Soehono, Stefanus. (2006). "*Audio Steganografi Menggunakan Mp3*". Mata Kuliah Keamanan Sistem Informasi ITB.

Voni, Yuniati. (2009)."*Enkripsi dan Dekripsi dengan Algoritma AES 256 Untuk Semua Jenis File*".

Wahyudi, & Parasian. (2008)*."Aplikasi Pertukaran Pesan Menggunakan Teknik Steganografi Dan Algoritma AES"*.

Wijaya, Ermadi Satriya. 2009. "*Konsep Hidden Message Menggunakan Teknik Steganografi*".