IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA TEKS TERENKRIPSI MENGGUNAKAN BLOCK CIPHER RIVEST CODE-6 KE DALAM GAMBAR

SKRIPSI

Oleh :

ANDREW CHANDRA
22094659

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

IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA TEKS TERENKRIPSI MENGGUNAKAN BLOCK CIPHER RIVEST CODE-6 KE DALAM GAMBAR

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 :

ANDREW CHANDRA
22094659

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

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA TEKS TERENKRIPSI MENGGUNAKAN BLOCK CIPHER RIVEST CODE-6 KE DALAM GAMBAR

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, Mei 2014

ANDREW CHANDRA
22094659

HALAMAN PERSETUJUAN

Judul	: IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA TEKS TERENKRIPSI MENGGUNAKAN BLOCK CIPHER RIVEST CODE-6 KE DALAM GAMBAR
Nama	: ANDREW CHANDRA
NIM	: 22094659
Mata Kuliah	: Skripsi (Tugas Akhir)
Kode	: TIW276
Semester	: Genap
Tahun akademik	: 2013/2014

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal Mei 2014

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom., M.Cs.	Junius Karel , S.Si., MT.

HALAMAN PENGESAHAN

IMPLEMENTASI STEGANOGRAFI DENGAN METODE END OF FILE PADA TEKS TERENKRIPSI MENGGUNAKAN BLOCK CIPHER RIVEST CODE-6 KE DALAM GAMBAR

Oleh: ANDREW CHANDRA / 22094659

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 ....

Yogyakarta, Mei 2014
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom, M.Cs. _____
2. Junius Karel , S.Si., MT. _____
3. _____
4. _____

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 "Implementasi Steganografi dengan Metode End of File pada Teks yang Terenkripsi Menggunakan Cipher Block Rivest Code-6 ke dalam Gambar" dengan baik.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Bapak Willy Sudiarto Raharjo, S.Kom, 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 Tampubolon, S.Si., MT. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
3. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
4. 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 sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian, sehingga suatu saat nanti penulis dapat memberikan karya yang lebih baik lagi.

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, Mei 2014

Penulis

INTISARI

Implementasi Steganografi dengan Metode End of File pada Teks yang Terenkripsi Menggunakan Cipher Block Rivest Code-6 ke dalam Gambar

Informasi adalah sesuatu yang sangar berharga saat ini. Keamanan dan kerahasiaan informasi menjadi salah satu faktor penting dalam melakukan komunikasi oleh manusia. Banyak terdapat media untuk melakukan komunikasi ini, namun banyak juga terdapat pihak-pihak yang tidak menghargai *privacy* ataupun nilai kerahasiaan informasi yang dimiliki pihak tertentu. Untuk menjaga informasi tersebut tidak jatuh ke pihak yang tidak bertanggungjawab, maka informasi tersebut bisa disamarkan menjadi sebuah media lain. Selain disamarkan informasi tersebut juga bisa diubah menjadi sebuah informasi yang hanya bisa dibaca dan dimengerti oleh pihak yang diijinkan.

Pada penelitian ini akan dibangun sebuah sistem untuk menjaga keamanan dan kerahasiaan sebuah informasi, khususnya adalah bentuk teks. Pada sistem ini akan diimplementasikan kombinasi antara kriptografi dan steganografi, yaitu kriptogradi dengan metode *Rivest Code-6* dan steganografi dengan metode *End of File*. Hasil dari sistem yang akan dibangun ini adalah pengkodean sebuah teks agar tidak bisa dipahami orang yang tidak berhak dan juga menyisipkannya ke sebuah citra agar tidak diketahui orang yang tidak berhak.

Sebagai hasil dari penelitian ini, informasi yang dikodekan dengan algoritma *Rivest Code-6* dan mengalami penyisipan dengan algoritma *End of File* mengalami perubahan ukuran dari ukuran awalnya. Perubahan ukuran ini tergantung dari besarnya citra dan besarnya pesan yang ingin disisipkan.

Kata Kunci : Algoritma, Kriptografi, Rivest Code 6, *Block Cipher,* Steganografi, *End of File.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Cepatnya pertumbuhan teknologi informasi saat ini membuat sangat banyak orang bergantung padanya. Hal ini membuat banyak orang melakukan komunikasi dengan media elektronik, tentunya ada juga informasi yang bersifat rahasia atau hanya ditujukan pada orang tertentu saja. Namun zaman sekarang sudah terdapat banyak ancaman di dunia maya, misalnya saja seorang *hacker* yang mampu mengambil data atau informasi orang lain tanpa diketahui. Hal ini menimbulkan kekhawatiran bagi pemilik informasi rahasia tersebut.

Untuk mengatasi hal tersebut, informasi ini biasanya di-enkripsi atau disamarkan menjadi informasi yang berbeda, namun informasi yang sudah dienkripsi tidak jarang menimbulkan rasa curiga bagi sekelompok orang sehingga mudah dipecahkan. Untuk itu selain informasi tersebut di-enkripsim sebaiknya informasi itu juga disembunyikan keberadaannya, salah satu teknik untuk menyembunyikan informasi ini adalah steganografi. Steganografi merupakan teknik menyembunyikan informasi di dalam informasi lainnya yang tidak bersifat rahasia. Salah satu metode untuk melakukan steganografi ini adalah *End of File (EOF).*

Diharapkan dengan melakukan enkripsi dengan metode *Rivest Code 6* informasi rahasia akan menjadi sebuah informasi lain dan informasi ini dapat disembunyikan ke dalam sebuah *image* dengan metode *End of File*.

1.2 Perumusan Masalah

1. Apakah dapat menyembunyikan informasi dengan baik di *image* berformat BMP menggunakan metode *Rivest Code 6* lalu melakukan steganografi dengan metode *End of File* ?
2. Apa pengaruh panjang kunci terhadap citra yang disisipi pesan?
3. Apa pengaruh panjang pesan terhadap citra yang disisipi pesan?

1.3 Batasan Masalah

Dalam penelitian ini, penulis memberikan batasan masalah untuk sistem yang akan dibuat. Adapun batasan masalah dalam penelitian ini, yaitu adalah format *image* yang digunakan adalah .BMP,

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk memahami cara kerja algoritma steganografi *End of File* serta menerapkannya pada teks yang terenkripsi algoritma *Rivest Code 6* ke dalam *image.*

1.5 Metode Penelitian

Dalam penulisan Skripsi ini, digunakan beberapa metode sebagai acuan dalam perancangan, implementasi dan penelitian terhadap sistem yang dibuat. Metode tersebut sebagai berikut:

1. Studi Pustaka

   Studi Pustaka dilakukan dengan mempelajari teori-teori melalui buku, artikel, jurnal dan bahan lain yang mendukung yang berhubungan dengan *steganografi* yang menggunakan metode *End of File* serta kriptografi metode *Rivest Code 6*, dan metode-metode pendukung lainnya yang dibutuhkan.

2. Perancangan Sistem

   Pada tahap ini sistem yang akan dirancang didasarkan pada penginputan gambar berformat BMP yang kemudian diberikan pesan rahasia berupa teks.

3. Pembangunan Sistem

   Tahap ini progam akan dibuat disesuaikan dengan rancangan sistem.

4. Implementasi dan Testing

   Pengujian terhadap progam dengan memasukkan beberapa inputan gambar berformat BMP, dan diberikan *input* berupa teks yang terenkripsi menggunakan metode *Rivest Code 6* yang akan dimasukkan kedalam citra awal. Dan *output* yang diharapkan adalah pesan rahasia dapat dimasukkan atau disamarkan ke dalam citra awalnya.

5. Analisis Hasil Percobaan dan Evaluasi

   Pada tahap ini kesimpulan dapat ditarik setelah melakukan uji coba pada progam.

1.6 Sistematika Penulisan

Skripsi ini disusun dalam sebuah laporan dengan sistematika atau spesifikasi terdiri dari 5 bab:

Bab 1 PENDAHULUAN yang berisi latar belakang masalah, perumusan masalah, batasan masalah, hipotesis, tujuan penelitian, metodologi, dan sistematika penulisan skripsi.

Bab 2 TINJAUAN PUSTAKA yang berisi gagasan-gagasan yang muncul dengan memberikan landasan teori yang akurat dari berbagai sumber dan konsep-konsep yang dibutuhkan dalam penyembunyian teks kedalam citra.

Bab 3 ANALISIS DAN PERANCANGAN SISTEM yang berisi perancangan sistem yang akan memberikan gambaran sistem yang akan dibuat serta prosedur–prosedur yang digunakan dalam sistem.

Bab 4 IMPLEMENTASI DAN ANALISIS SISTEM yang berisi implementasi dari hasil perancangan sistem dan pengujian terhadap sistem yang telah dibuat.

Bab 5 KESIMPULAN DAN SARAN yang berisi kesimpulan atas sistem yang telah dibuat serta saran-saran dalam pengembangan dari Skripsi ini agar dapat dikembangkan kembali.

BAB 5
KESIMPULAN DAN SARAN

1.1 Kesimpulan

Dalam pengerjaan Tugas Akhir ini ada beberapa hal yang dapat disimpulkan :

1. Proses enkripsi RC6 dan steganografi *End of File* dapat melakukan penyisipan pesan dengan baik, dimana ukuran citra penampung dapat bertambah sesuai dengan pesan yang ingin disisipkan.
2. Dengan menggunakan metode *End of File* maka pesan yang ingin disisipkan tidak dibatasi.
3. Perubahan ukuran *file* citra ini tergantung dari besarnya citra yang digunakan dan juga besarnya pesan yang disisipkan.
4. Panjang kunci yang ingin disisipkan pasti sebesar 16 byte dikarenakan melalui proses enkripsi dengan algoritma MD5.

1.2 Saran

Untuk pengembangan lebih lanjut, saran yang dapat diberikan adalah sebagai berikut :

1. Melakukan pengujian dengan menggunakan teknik-teknik tertentu terhadap citra yang telah disisipi pesan. Pengujian ini bertujuan untuk mengetahui ketahanan enkripsi dan penyisipan terhadap teknik-teknik yang digunakan.
2. Melakukan proses penyisipan dengan lebih efisien, misalnya tidak hanya mengisi nilai-nilai di nilai RGB, melainkan setiap Red, Green, dan Blue value menampung 1 byte pesan. Hal ini akan membuat *space* untuk penyisipan digunakan lebih efisien.
3. Untuk penelitian selanjutnya, menerapkan algoritma RC6 dan *End of File* dapat dilakukan lebih lanjut terhadap media yang disisipkan dan media yang menjadi penampung. Media yang disisipkan untuk penelitian lebih lanjut bisa berupa *file* citra dengan format selain BMP, audio, atau video.

DAFTAR PUSTAKA

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

Yudi Triyanto, Fransiskus. (2010). Analisis Perbandingan Algoritma Enkripsi AES-128 dengan Algoritma RC6. Yogyakarta : Universitas Kristen Duta Wacana

Rivest, R.L., Robshaw, M.J.B., Sidney, R., dan Yin, Y.L, (2001). The RC6 Block Cipher. USA. MIT Laboratory for Computer Science, Cambridge.

Prayudi, Yudi, Idham, Malik, (2005). Studi dan Analisis Algoritma RIVEST CODE 6(RC6) Dalam Enkripsi/Dekripsi Data**.** Yogyakarta : Universitas Islam Indonesia

Krisnawati, (2008), Metode Least Significant Bit(LSB) dan End of File (EOF) untuk Menyisipkan Teks ke dalam Citra Grayscale, Medan : Universitas Sumatera Utara

Wandani, Henny, (2012), Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem, Medan : Universitas Sumatera Utara

Aditya, Yogie, (2010), Studi Pustaka untuk Steganografi dengan Beberapa Metode, Yogyakarta : Universitas Islam Indonesia

Wasino, (2012), Implementasi Steganografi Teknik End of File dengan Enkripsi Rijndael, Tangerang : STMIK Dharma Putra

Rachmawanto, Eko Hari, (2010), Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vernam Cipher dan Steganografi dengan Metode End of File(EOF), Semarang : Universitas Dian Nuswantoro

Edisuryana, Mukharrom, (2013), Aplikasi Steganografi pada Citra Berformat Bitmap dengan Menggunakan Metode End of File, Semarang : Universitas Diponegoro

Sejati, Adiputra, (2010), Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading), Bandung : Institut Teknologi Bandung

Muharini, Anisah, (2012), Aplikasi Algoritma Rivest Code 6 dalam Pengamanan Citra Digital, Jakarta : Universitas Indonesia

Cormen, Thomas H., Leiserson, Charles E, Rivest, Ronald L., Stein, Clifford, (2009), Introduction to Algorithm Third Edition, London

Permana, Rangga Wisnu Adi, (2008), Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler, Bandung : Institut Teknik Bandung

https://www.facebook.com/notes/ickha-za/contoh-studi-kasus-metode-rivest-code-6-rc6/481402271918779

https://www.facebook.com/notes/ickha-za/contoh-studi-kasus-metode-rivest-code-6-rc6-part-ii/492953590763647

http://www.codeproject.com/Articles/2545/RC6-encryption-and-decryption

http://n3vrax.wordpress.com/2011/08/14/aesrijndael-java-implementation/

http://hari-cio-8a.blog.ugm.ac.id/2013/03/22/fungsi-hash-teknik-kriptografi/