TWOFISH AND LEAST SIGNIFICANT BIT (LSB) ALGORITHM IMPLEMENTATION FOR CONCEALMENT OF TEXT FILE ON THE DIGITAL IMAGE

Thesis

by
DEVRI RIZA SETYAWAN
22084567

STUDY ENGINEERING INFORMATICS FACULTY OF INFORMATION TECHNOLOGY
DUTA WACANA UNIVERSITY CHRISTIAN
2012

IMPLEMENTASI ALGORITMA TWOFISH DAN LEAST SIGNIFICANT BIT (LSB) UNTUK PENYEMBUNYIAN FILE TEXT PADA CITRA DIGITAL

Skripsi

oleh
DEVRI RIZA SETYAWAN
22084567

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2012

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI ALGORITMA TWOFISH DAN LEAST SIGNIFICANT BIT (LSB) UNTUK PENYEMBUNYIAN FILE TEXT PADA CITRA DIGITAL

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, 13 Desember 2012

DEVRI RIZA SETYAWAN
22084567

INTISARI

Implementasi Algoritma *Twofish* dan *Least Significant Bit* (LSB) untuk Penyembunyian File Text pada Citra Digital

Keamanan dan kerahasiaan informasi merupakan salah satu aspek penting dalam perkembangan dunia komunikasi. Komunikasi memegang peranan penting dalam hal pertukaran informasi yang dilakukan oleh manusia. Di dalam pertukaran informasi melalui media komunikasi banyak hal yang tidak dapat diprediksi kemungkinan apa yang terjadi saat penyampaian informasi tersebut. Faktanya banyak pihak-pihak yang tidak bertanggung jawab yang mengganggu jalannya pertukaran informasi seperti menyadap informasi yang menjadi rahasia diantara kedua belah pihak yang melakukan komunikasi. Maka dari itu, informasi yang dikirim setidaknya disamarkan dalam bentuk lain supaya informasi yang dikirim tidak bisa diketahui oleh pihaknya yang tidak berkepentingan.

Untuk mengatasi permasalahan tersebut, diperlukan suatu cara untuk menyamarkan informasi yang dikirim dengan menyandikan informasi tersebut lalu menyisipkan pada media lain. Pada penelitian ini, akan dibangun sebuah sistem yang mengimplementasikan perpaduan antara algoritma kriptografi *Twofish* dan steganografi *Least Significant Bit* (LSB) untuk menyandikan informasi dalam bentuk file teks lalu menyisipkannya pada media file citra.

Hasil dari penelitian ini, informasi yang disandikan dengan algoritma *Twofish* mengalami perubahan ukuran file yang sangat sedikit sehingga tidak terlalu mempengaruhi kapasitas yang ada pada file citra dijadikan wadah. Perubahan ukuran file teks yang terjadi disebabkan oleh *padding* yang dilakukan untuk memenuhi syarat algoritma *Twofish* yang berjalan pada 128 blok bit. Selain itu, kedua file citra output dari sistem yang dibangun sama-sama tidak tahan terhadap beberapa operasi manipulasi dan file citra BMP tidak mengalami perubahan ukuran file setelah disisipi pesan seperti yang dialami file citra PNG.

Kata Kunci : Algoritma, Kriptografi, *Twofish, Block Cipher,* Steganografi, *LSB.*

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI ALGORITMA TWOFISH DAN LEAST SIGNIFICANT BIT (LSB) UNTUK PENYEMBUNYIAN FILE TEXT PADA CITRA DIGITAL
Nama Mahasiswa	:	DEVRI RIZA SETYAWAN
N I M	:	22084567
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2012/2013

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 30 Oktober 2012

Dosen Pembimbing I	Dosen Pembimbing II
Drs. R. Gunawan Santosa, M.Si.	Willy Sudiarto Raharjo, SKom.,M.Cs

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA TWOFISH DAN LEAST SIGNIFICANT BIT (LSB) UNTUK PENYEMBUNYIAN FILE TEXT PADA CITRA DIGITAL

Oleh: DEVRI RIZA SETYAWAN / 22084567

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 30 November 2012

Yogyakarta, 13 Desember 2012
Mengesahkan,

Dewan Penguji:

1. Drs. R. Gunawan Santosa, M.Si.
2. Willy Sudiarto Raharjo, SKom.,M.Cs
3. Junius Karel, M.T.

Dekan	Ketua Program Studi
(Drs. Wimmie Handiwidjojo, MIT.)	(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 Algoritma *Twofish* dan *Least Significant Bit* (LSB) untuk Penyembunyian File Text pada Citra Digital" 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 Restyandito, S.Kom, MSIS. selaku dosen pembimbing I yang pertama yang selalu sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
2. Bapak Willy Sudiarto Raharjo, SKom.,M.Cs. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.\
3. Bapak Drs. R. Gunawan Santosa, M.Si. selaku dosen pembimbing I pengganti yang selalu sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
4. Keluarga Kirmadi – Yustina Sri Suyanti yang selalu memberikan doa dan dukungannya kepada penulis dalam menyelesaikan Tugas Akhir.

5. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
6. 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, 4 November 2012

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Implementasi Algoritma *Twofish* dan *Least Significant Bit* (LSB) untuk Penyembunyian File Text pada Citra Digital

Keamanan dan kerahasiaan informasi merupakan salah satu aspek penting dalam perkembangan dunia komunikasi. Komunikasi memegang peranan penting dalam hal pertukaran informasi yang dilakukan oleh manusia. Di dalam pertukaran informasi melalui media komunikasi banyak hal yang tidak dapat diprediksi kemungkinan apa yang terjadi saat penyampaian informasi tersebut. Faktanya banyak pihak-pihak yang tidak bertanggung jawab yang mengganggu jalannya pertukaran informasi seperti menyadap informasi yang menjadi rahasia diantara kedua belah pihak yang melakukan komunikasi. Maka dari itu, informasi yang dikirim setidaknya disamarkan dalam bentuk lain supaya informasi yang dikirim tidak bisa diketahui oleh pihaknya yang tidak berkepentingan.

Untuk mengatasi permasalahan tersebut, diperlukan suatu cara untuk menyamarkan informasi yang dikirim dengan menyandikan informasi tersebut lalu menyisipkan pada media lain. Pada penelitian ini, akan dibangun sebuah sistem yang mengimplementasikan perpaduan antara algoritma kriptografi *Twofish* dan steganografi *Least Significant Bit* (LSB) untuk menyandikan informasi dalam bentuk file teks lalu menyisipkannya pada media file citra.

Hasil dari penelitian ini, informasi yang disandikan dengan algoritma *Twofish* mengalami perubahan ukuran file yang sangat sedikit sehingga tidak terlalu mempengaruhi kapasitas yang ada pada file citra dijadikan wadah. Perubahan ukuran file teks yang terjadi disebabkan oleh *padding* yang dilakukan untuk memenuhi syarat algoritma *Twofish* yang berjalan pada 128 blok bit. Selain itu, kedua file citra output dari sistem yang dibangun sama-sama tidak tahan terhadap beberapa operasi manipulasi dan file citra BMP tidak mengalami perubahan ukuran file setelah disisipi pesan seperti yang dialami file citra PNG.

Kata Kunci : Algoritma, Kriptografi, *Twofish, Block Cipher,* Steganografi, *LSB.*

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. Internet membuat komunikasi antar manusia menjadi lebih mudah, cepat dan dapat dilakukan dimana saja. Disamping itu, Internet mempunyai kelemahan yang sulit untuk ditanggulangi, yaitu penyadapan data atau informasi yang dikirimkan melalui Internet. Aspek keamanan data atau informasi dalam komunikasi melalui Internet sangat penting untuk di perhatikan. Untuk hal tersebut dibutuhkan metode-metode untuk mengamankan informasi atau data yang di kirim melalui Internet.

Kriptografi dan Steganografi merupakan metode pengamanan data untuk menjaga kerahasiaan dan keaslian data serta dapat meningkatkan aspek keamanan suatu data atau informasi. Metode ini bertujuan agar informasi atau data yang dikirimkan melalui Internet tidak dapat diketahui dan dimanfaatkan oleh pihak-pihak yang tidak berkepentingan pada informasi atau data tersebut.

Dengan memadukan algoritma kriptografi *Twofish* dan steganografi *Least Significant Bit*, penulis mencoba mambangun sebuah sistem yang dapat menyembunyikan pesan ke dalam sebuah citra digital dengan menggunakan algoritma LSB. Akan tetapi, sebelum pesan tersebut di sisipkan, pesan tersebut dienkripsi terlebih dahulu dengan algoritma *Twofish*. Dengan cara tersebut, diharapkan informasi yang dikirim dapat terjaga kerahasiaannya dan mempunyai tingkat keamanan yang tinggi.

1.2 Rumusan Masalah

Rumusan masalah yang ada dalam penelitian ini antara lain :

1. Bagaimana dampak file yang dienkripsi dengan algoritma *Twofish* jika dilihat dari sisi ukuran file tersebut dan bagaimana pengaruhnya terhadap proses penyisipan file hasil enkripsi pada citra digital dengan algoritma *Least Significant Bit*?
2. Bagaimana dampak citra digital yang telah disisipkan file teks yang terenkripsi jika dilihat dari sisi kualitas serta ketahanan citra digital terhadap beberapa operasi manipulasi?

1.3 Batasan Masalah

Batasan-batasan pada penelitian ini antara lain :

- Panjang kunci maksimal untuk kriptografi adalah 32 karakter (256 bit).
- Format file teks yang digunakan dalam proses enkripsi dan nantinya akan disisipkan pada file citra digital adalah file yang mempunyai format .txt.
- Format file citra digital yang digunakan untuk menjadi media steganografi adalah file yang berformat BMP dan PNG.
- Ukuran minimal file citra digital adalah 200 kb.
- Tidak adanya fasilitas untuk mengingat kunci, sehingga pengguna harus mengingat kunci yang digunakan dalam proses enkripsi dan dekripsi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini antara lain :

- Membangun aplikasi dengan mengimplementasikan perpaduan algoritma *Twofish* dan algoritma *Least Significant Bit.*
- Meneliti dan menganalisa perpaduan algoritma *Twofish* dan LSB yang dipakai untuk menyembunyikan file teks ke dalam file citra digital.

1.5 Metode Penelitian

Metodologi atau pendekatan yang digunakan dalam penyusunan Tugas Akhir ini adalah :

- Melakukan studi pustaka dengan cara mencari informasi dan teori-teori dari berbagai literatur yang berkaitan dengan judul.
- Melakukan analisa dan perancangan aplikasi yang didapat dari literatur yang sudah dipelajari.
- Mengimplementasikan agloritma *Twofish* dan LSB dalam pembuatan sistem untuk menyembunyikan file teks pada file citra.
- Pengujian kinerja dari sistem yang dibangun dan menganalisa hasil.

1.6 Sistematika Penulisan

Sitematika penulisan tugas akhir ini akan terbagi dalam lima bab dengan urutan penulisan sebagai berikut

Bab 1 PENDAHULUAN pada bab ini yang berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Metode Penelitian, dan Sistematika Penulisan.

Bab 2 TINJAUAN PUSTAKA pada bab ini terdiri dari dua bagian utama, yaitu Tinjauan Pustaka dan Landasan Teori.

Bab 3 PERANCANGAN SISTEM pada bab ini mencakup analisis teori-teori yang digunakan, dan bagaimana menerapkannya ke dalam sistem yang akan dibuat.

Bab 4 IMPLEMENTASI DAN ANALISIS SISTEM pada bab ini memuat hasil riset / implementasi, dan pembahasan dari riset tersebut yang bersifat terpadu.

Bab 5 KESIMPULAN DAN SARAN pada bab ini terdiri dari kesimpulan dan saran-saran untuk pengembangan sistem.

Selain berisi bab-bab utama tersebut, skripsi ini juga dilengkapi dengan Intisari, Daftar Isi, Daftar Gambar, Daftar Tabel, Daftar Pustaka dan Lampiran.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Melalui pengerjaan Tugas Akhir ini, ada beberapa hal yang dapat disimpulkan yaitu sebagai berikut :

1. *Twofish* adalah sebuah algoritma kriptografi yang baik digunakan dalam penyandian pesan rahasia karena selain algoritma ini merupakan algoritma yang susah dipecahkan oleh para kriptanalisis, hasil dari penyandian pada algoritma ini hampir tidak mengubah ukuran file yang dilakukan penyandian tersebut. Ukuran file hanya berubah sedikit, hal itu terjadi dikarenakan *padding* yang dilakukan pada media yang disandikan supaya memenuhi syarat dari algoritma *twofish* yang mana berjalan pada 128 blok bit (*plainteks* 128 bit → *ciperteks* 128 bit).
2. File citra BMP tidak mengalami perubahan ukuran file setelah disisipi pesan terenkripsi, sedangkan file citra PNG mengalami perubahan ukuran file setelah disisipi pesan. Hal tersebut dapat terjadi karena input citra diproses dengan dalam bentuk bitmap.
3. Pengujian dari sistem yang dibangun menghasilkan file stego yang tidak tahan terhadap beberapa operasi manipulasi seperti penambahan ketajaman (*Sharpen*), kontras dan transformasi rotasi.

5.2 Saran

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

1. Dapat dilakukan penambahan fungsi untuk membandingkan apakah media penampung sebelum disisipi sama dengan media penampung setelah disisipi, seperti fungsi perangkat lunak VBinDiff yang digunakan pada penelitian ini.

2. Dapat juga dilakukan penambahan fungsi yang dapat membandingkan pesan rahasia asli dengan pesan rahasia hasil dari ekstrasi dan dekripsi apakah sama 100 % (nilai hashnya) atau tidak seperti fungsi perangkat lunak md5summer yang digunakan pada penelitian ini.
3. Untuk penelitian selanjutnya, dalam penerapan algoritma *twofish* dan LSB dapat dilakukan lebih lanjut terhadap media yang disisipkan dan media yang menjadi penampung. Media yang disisipkan bisa dilakukan penelitian lebih lanjut antara lain citra, audio, atau video. Sedangkan untuk media penampung bisa dilakukan penelitian lebih lanjut antara lain citra lain (JPG, JPEG, TIFF, GIF, dll), audio, atau video.

DAFTAR PUSTAKA

Aditya, Y., Pratama, A., & Nurlifa, A. (2010). Studi Pustaka untuk Steganografi dengan Beberapa Metode. Yogyakarta: Universitas Islam Indonesia.

Dani. (2006). Algoritma Twofish Sebagai Finalis AES dan Metode Kriptanalisnya. Bandung : Institut Teknologi Bandung.

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

Hyde, Randall. (1996). *The Art of Assembly Language Programming*. URL http://www.arl.wustl.edu/~lockwood/class/cs306/books/artofasm/toc.html. Akses : 4 Desember 2012

Johnson, N., & Jajodia, S. (1998). Exploring Steganography, Seeing the Unseen. IEEE Computer Magazine

Menezes, A., Oorschot, P., & Venstone, S. (1996). Handbook of Applied Cryptography. Cambridge : Massachusetts Institute of Technology.

Mukmin, I. (n.d.). Algoritma Twofish kinerja dan implementasinya sebagai salah satu kandidat algoritma AES (Advanced Encryption Standard). Bandung : Institut Teknologi Bandung.

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

Ratih. (2007). Studi dan Implementasi Enkripsi Pengiriman Pesan Suara Menggunakan Algoritma Twofish. Bandung : Institut Teknologi Bandung.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish : A 128-bit block cipher.

Setyawan, H., Muchallil, S., & Arnia, F. (2009). Implementasi Steganografi Dengan Metode Least Significant Bit (LSB). NAD : Universitas Syiah Kuala.

Waheed, Q. (2000). Steganography and Steganalysis. PhD thesis

Xue, Y. (2006). *Block cipher Principle*. URL https://tao.truststc.org/Members/yuanxue/cyptography_new/Public%20resources/lecture7.pdf. Akses : 10 Desember 2012.