IMPLEMENTASI ADVANCED ENCRYPTION STANDARD DALAM STEGANOGRAFI CITRA 24 BIT DENGAN DEKOMPOSISI WAVELET

Bagus Setyo Bawono[1], Setyorini[2], Fazmah Arif Yulianto[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Perkembangan teknologi digital berimbas pada semakin mudahnya proses reproduksi, penyimpanan dan pendistribusian data digital. Tetapi di sisi lain, hal ini memunculkan tindakan-tindakan kriminal seperti akuisisi dan penyalahgunaan ilegal terhadap data digital.
Steganografi melindungi data digital dengan jalan menyembunyikannya ke dalam medium penampung yang berfungi sebagai cover, sementara kriptografi menyandikan data sehingga tidak dapat dipahami oleh pihak ketiga. Kedua teknik ini dapat dikombinasikan untuk menghasilkan keamanan yang lebih baik dalam perlindungan terhadap data digital. Tugas akhir ini mencoba mengkombinasikan keamanan enkripsi AES dan keamanan steganografi wavelet.
Dari hasil implementasi terlihat bahwa citra stego yang dihasilkan dari sistem ini dinilai paling aman jika data di dalamnya disisipkan pada layer merah atau layer biru. Adanya error bit hasil ekstraksi mempengaruhi rusaknya blok data hasil dekripsi, yang kuantitas kerusakannya berkaitan langsung dengan ukuran blok cipher AES.

Kata Kunci : AES, Block Cipher, Kriptografi, Steganografi, Wavelet.

Abstract

The development of digital technology is resulting in totally easier way to reproduct, store and distribute digital data. But, in the other hand, it triggers some criminal actions, such as illegal data acquisition and the misuse of the data.
Steganography protects digital data by hiding it in the medium that acts as a cover, while cryptography encodes the data, so it can't be understood by the third party. Both techniques can be combined to produce a better security for digital data protection. This final assignment is combining the security of AES encryption and the security of wavelet steganography.
From the implementation, we can see that this system produce a stego-image with a better security, if the data embedded on the red or the blue layer. The existence of bit errors during extraction contributes to decryption error, in quantity that corresponds directly to the size of the AES block cipher.

Keywords : AES, Block Cipher, Criptography, Steganography, Wavelet.

1. Pendahuluan

1.1 Latar belakang

Perkembangan teknologi digital memungkinkan seseorang dengan mudah melakukan reproduksi, penyimpanan dan pendistribusian data digital dengan lebih mudah dan murah. Tetapi di sisi lain, kemudahan-kemudahan ini memunculkan tindakan-tindakan kriminal seperti akuisisi dan penyalahgunaan ilegal terhadap data digital.

Watermarking dan Steganografi memberikan solusi untuk melindungi data digital. Keduanya termasuk dalam teknik penyembunyian data *(data-hiding)*, tetapi memiliki perbedaan mendasar dalam hal spesifikasi dan tujuannya. Jika watermarking melindungi data digital dengan menyisipkan data kepemilikan, steganografi menyembunyikan data digital ke dalam medium penampung yang berfungi sebagai *cover*.

Kriptografi memiliki pendekatan berbeda dalam upaya perlindungan terhadap data. Jika *data-hiding* bersifat menyembunyikan, enkripsi cenderung menyandikan, sehingga pesan menjadi tidak bermakna.

Seiring dengan munculnya metode-metode cerdas untuk menyisipkan data rahasia pada media digital, muncul pula metode-metode cerdas untuk mendeteksi dan menyingkap keberadaannya (*steganalysis*). Pengiriman dan penyimpanan sebuah pesan yang telah terenkripsi akan sangat mengundang kecurigaan, sementara penyimpanan atau pengiriman pesan tak terlihat tidaklah demikian.

Kedua teknik ini (kriptografi dan steganografi) dapat dikombinasikan untuk menghasilkan perlindungan yang lebih baik terhadap pesan rahasia [14]. *Advanced Encryption Standard* (AES) adalah algoritma kriptografis berbasis algoritma Rijndael yang dapat dipakai untuk melindungi data elektronik. Enkripsi mengubah data menjadi bentuk yang tidak bermakna, yang disebut dengan *ciphertext*, dan dekripsi mengembalikan data dari bentuk yang tidak bermakna menjadi data asal yang disebut dengan *plaintext* [5]. AES dapat diimplentasikan sebagai enkripsi untuk menambah lapisan keamanan di dalam suatu sistem steganografi.

1.2 Perumusan masalah

Dalam tugas akhir ini, akan dirancang dan diimplementasikan sistem steganografi dengan medium penampung berupa citra 24 bit dengan enkripsi untuk menyandikan informasi rahasia sebelum disisipkan. Di dalam proses perancangan dan implementasinya, perlu diperhatikan beberapa point sebagai berikut:

1. Bagaimana menyisipkan *ciphertext* ke dalam citra digital, agar citra yang telah disisipi memiliki kualitas yang hampir sama dengan citra asli.
2. Bagaimana kualitas citra keluaran sistem steganografi (*stego image*) setelah disisipi informasi rahasia.

3. Bagaimana ketahanan informasi yang disembunyikan, apabila *stego image* diserang dengan gangguan-gangguan tertentu.
4. Bagaimana kualitas informasi rahasia yang telah diekstrak kemudian dilakukan dekripsi, apabila *stego image* mengalami gangguan.

1.3 Tujuan

Tujuan yang ingin dicapai dalam penulisan tugas akhir ini antara lain :

1. Membuat perangkat lunak yang mengimplementasikan steganografi dengan keamanan enkripsi dalam media yang berupa citra digital 24 bit.
2. Menganalisis citra *stego* dengan melakukan penilaian kualitas, yang dilakukan secara objektif dan subjektif.
3. Menganalisis informasi rahasia hasil ekstraksi dari *stego image* yang telah mengalami gangguan, yang dilakukan secara objektif.
4. Menganalisis hasil dekripsi atas informasi rahasia hasil ekstraksi dari *stego image* yang telah mengalami gangguan, yang dilakukan secara objektif.

Agar pembahasan masalah yang dibahas pada tugas akhir ini tidak menyimpang dari tujuan yang telah ditetapkan, maka batasan yang dipakai dalam penulisan tugas akhir ini antara lain :

1. Medium penyisipan data berupa citra bitmap 24 bit.
2. Data yang disisipkan berupa file teks (*.txt).
3. Metode dekomposisi sinyal digital yang digunakan adalah dekomposisi wavelet dengan *mother* wavelet Haar.
4. Citra digital yang dipakai berukuran 512x512 piksel.
5. Serangan yang dikenakan pada *stego image* berupa kompresi JPEG, *Gaussian Noise* dan *Gaussian Blur*.
6. Algoritma enkripsi yang dipakai adalah AES 128 bit.
7. *Hash function* tidak dibahas.

1.4 Metodologi penyelesaian masalah

Untuk menyelesaikan pembuatan tugas akhir ini, dilakukan beberapa langkah kerja sebagai berikut:

1. Mengumpulkan bahan-bahan referensi yang menunjang proses penelitian, seperti jurnal, artikel dan paper tentang steganografi, wavelet, pengolahan citra dan *AES*.
2. Studi literatur tentang pengolahan sinyal digital, wavelet, pengolahan citra, steganografi dan *AES* sebagai tahap pendalaman materi.
3. Membuat perangkat lunak untuk mengimplementasikan steganografi wavelet dengan enkripsi *AES* untuk menyandikan data rahasia.
4. Melakukan analisis hasil implementasi, baik dari sisi *stego image*, informasi rahasia hasil ekstraksi, dan informasi rahasia hasil dekripsi.
5. Membuat kesimpulan dari hasil penelitian.

Penyusunan laporan dalam bentuk tertulis sebagai laporan tugas akhir.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan analisis yang dilakukan selama tahap pengujian, maka dihasilkan beberapa kesimpulan sebagai berikut :

1. Dekomposisi wavelet memisahkan frekuensi sinyal dalam batasan yang jelas, sehingga modifikasi untuk penyisipan data dapat dilakukan dengan aman selama *sub-band* yang dipilih memiliki sifat *hidden* yang baik.
2. Keamanan sistem steganografi pada citra bitmap 24 bit ditentukan oleh pemilihan lokasi layer untuk menyisipkan data. Implementasi enkripsi AES dalam steganografi dapat memberikan nilai keamanan di level bawah pada sistem *data-hiding.*
3. *Bit error* yang terjadi selama ekstraksi pesan memberikan pengaruh pada hasil dekripsi atas pesan hasil ekstraksi, yang besarnya bersesuaian dengan ukuran blok *cipher* AES.

5.2 Saran

Setelah dilakukan analisis terhadap hasil implementasi dalam tugas akhir ini, dapat diperoleh beberapa saran guna meningkatkan kualitas dari steganografi, yaitu :

1. Penyisipan tidak dilakukan secara serial, tetapi disebar *(spread)* dengan metode tertentu.
2. Apabila implementasi enkripsi AES tetap ingin dipertahankan, sistem steganografi harus di-desain agar lebih *robust* terhadap gangguan sehingga error dekripsi pesan dapat dihindari.

Daftar Pustaka

[1] Breed, Gary. 2003. Bit Error Rate : Fundamental Concepts and Measurement Issues. Summit Technical Media, LLC.
http://www.highfrequencyelectronics.com/Archives/Jan03/HFE0103_Tutorial.pdf
diakses tanggal 6 Agustus 2007

[2] Davidson Jennifer. 2002. "Information Hiding : The New Digital Age". Electrical and Computer Engineering Department of Mathematics.

[3] Dharma, Eddy Muntina. 2004. Bahan kuliah Grafika dan Citra. Bandung: Sekolah Tinggi Teknologi Telkom.

[4] Dharma, Eddy Muntina. 2004. *Steganography* pada Citra Digital dengan Transformasi *Wavelet*. Bandung: Jurusan Teknik Informatika Sekolah Tinggi Teknologi Telkom.

[5] Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
diakses tanggal 5 Maret 2007

[6] Gaussian Blur
http://www.wikipedia.com/Gaussian_blur.html
diakses tanggal 24 November 2006

[7] Gaussian Noise
http://www.wikipedia.com/Gaussian_noise.html
diakses tanggal 24 November 2006

[8] Gonzalez, Rafael C dan Paul Wintz. 1987. Digital Image Processing. Addison-Wesley Publishing Company.

[9] Hanindito, Raden Abi. 2006. "Analisis dan Implementasi Image Denoising dengan Menggunakan Metode NormalShrink sebagai Wavelet Thresholding". Jurusan Teknik Informatika STT Telkom Bandung.

[10] Histograms Tutorial - Luminance and Color.
http://www.cambridgeincolour.com/tutorials/histograms2.htm
diakses tanggal 6 Agustus 2007

[11] Huong Ho. Steganography Information Hiding in Digital Images.
http://www.site.uottawa.ca/~jyzhao/courses/elg7173/huong_ho_ppt.ppt
diakses tanggal 15 April 2007

[12] Matlab. 2002. "Wavelet Toolbox". The Mathwork Inc.

[13] Niels, Provos, Peter Honeyman. 2003. Hide and Seek: An Introduction to Steganography. United States of America. University of Michigan.
http://www.niels.xtdnet.nl/papers/practical.pdf
diakses tanggal 19 Desember 2006

[14] Robert Krenn. Steganography and steganalysis.
http://www.krenn.nl/univ/cry/steg/article.pdf
diakses tanggal 1 Mei 2007

[15] Roger S. Pressman. *Software Engineering : A Practitioner's Approach*" fourth edition. McGraw-Hill.

[16] Ryan, Øyvind. 2004. Applications of the wavelet transform in image processing. Oslo.
http://heim.ifi.uio.no/~oyvindry
diakses tanggal 22 November 2006

[17] Wirabuwana, I DN. 2005. "Analisis Kerja Image Steganography Menggunakan Transformasi Wavelet". Jurusan Teknik Elektro STT Telkom Bandung.