Implementasi Enkripsi AES Cipher dan Discrete Wavelet Transform Dalam Metode Steganografi

David Christ Antono, Henry Novianus Palit, Rudy Adipranata
Program Studi Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jln. Siwalankerto 121-131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) - 8417658
dchristantono@gmail.com, hnpalit@petra.ac.id, rudya@petra.ac.id

ABSTRAK

Ilmu steganografi mengarah pada cabang ilmu komputer yang tentang penyembunyian informasi data dalam media yang tidak bisa dengan mudah dapat dideteksi. Terdapat berbagai macam jenis media steganografi, tetapi yang paling populer adalah steganografi gambar. Seiring berkembangnya ilmu steganalysis, semakin diperlukan juga cara untuk mengamankan data yang terkandung. Dengan steganalysis kita dapat dengan mudah mendeteksi adanya data yang tersembunyi dalam sebuah media. Oleh karena itu, penelitian ini berusaha untuk menjawab kebutuhan terhadap pengamanan data tersebut.

Program berupa aplikasi yang berguna untuk mengamankan data yang disembunyikan. Fungsi dari program ini adalah untuk mengenkripsi data yang akan disembunyikan menggunakan metode AES cipher. Dengan mengubah data yang tersembunyi menjadi ciphertext, meskipun data yang tersembunyi dapat diambil bentuknya masih berupa teks yang tidak dapat dibaca tanpa menggunakan kunci yang digunakan untuk mengenkripsi. Proses ini melibatkan data yang akan disembunyikan diubah terlebih dahulu menjadi ciphertext dan akhirnya di steganografi menggunakan least significant bit. Tidak hanya itu, program juga akan melakukan kompresi terhadap stego image.

Dari hasil uji coba enkripsi, steganografi dan kompresi yang dilakukan, data gambar yang disembunyikan dapat diambil kembali dengan menggunakan kunci yang digunakan saat enkripsi. Data yang disembunyikan tidak mengalami kehilangan informasi karena proses yang dilakukan lossless. Data yang disembunyikan telah dibandingkan dengan data hasil ekstraksi dan menghasilkan nilai PSNR tak terbatas.

Kata Kunci: *AES Cipher*, Cipherteks, Steganografi, *Jpeg2000, Discrete Wavelet Transform*

ABSTRACT

The science of steganography leads to a branch of computer science that is about hiding data information in media that cannot be easily detected. There are many types of media for steganography. The most popular ones are digital images. Along with the development of the science of steganalysis, there is needs of a way to add security to the hidden data. With steganalysis, one can easily reveal existence of hidden data in media files. Therefore, this study seeks to answer the need for securing the data.

The program is an application that is useful for securing hidden data. The function of this program is to encrypt data that will be hidden using the AES cipher method. By converting hidden data into ciphertext, even though hidden data can be taken its form is still in the form of text that cannot be read without using the key used to encrypt. This process involves data that will be hidden to be converted into ciphertext first and finally steganography will be performed using least significant bits. Not only that, the program will also compress stego image.

From the results of the encryption, steganography and compression trials, the hidden image data can be retrieved using the key used during encryption. The hidden data does not experience loss of information because the process is carried out lossless. The hidden data has been compared with extracted data and produces unlimited PSNR values.

Keywords: *AES Cipher, Ciphertext, Steganography, Jpeg2000, Discrete Wavelet Transform.*

1. PENDAHULUAN

Penggunaan komputer dalam berbagai macam bidang kehidupan membawa perkembangan pesat pada perkembangan perangkat lunak komputer. Teknologi internet juga sudah berkembang pesat di seluruh dunia. Kemudahan penggunaan dan fasilitas yang lengkap adalah keunggulan internet. Hal ini menjadikan internet sebagai salah satu media komunikasi data yang sangat populer. Seiring dengan berkembangnya aplikasi yang berbasis internet, semakin banyak orang yang mengakses informasi yang bukan haknya. Oleh karena itu, sejalan dengan perkembangan internet yang sangat cepat, harus diikuti perkembangan pengamanan dalam sistem informasi yang berbasis internet tersebut..

Steganografi mengacu pada cabang ilmu komputer yang mana berurusan dengan menyembunyikan informasi data dalam media yang tidak bisa dengan mudah dapat dideteksi. Citra digital adalah salah satu data yang bisa dikirimkan melalui internet. Semakin pentingnya informasi dari citra digital tersebut, semakin berkembang pula metode-metode yang digunakan untuk merahasiakan citra digital yang didukung pula dengan perkembangan media elektronik. Pada saat tertentu informasi yang dikirimkan tidak ditujukan kepada semua orang, namun ditujukan hanya kepada orang atau badan usaha tertentu [3].

Saat ini telah ada aplikasi yang dapat melakukan serangan terhadap teknik steganografi yang digunakan, sehingga orang yang tidak berwenang dapat memperoleh informasi yang di sembunyikan tersebut. Seiring dengan adanya serangan, maka keamanan data juga perlu untuk ditingkatkan [3].

2. LANDASAN TEORI

2.1 Steganografi

Steganografi adalah seni untuk menyembunyikan informasi yang sensitif dengan suatu cara pada sebuah media sehingga selain pengirim dan penerima informasi tidak ada yang mengetahui bahwa ada informasi yang tersembunyi pada media pembawa informasi tersebut. Steganografi dapat diterapkan pada berbagai

macam file format. Tujuan steganografi adalah merahasiakan atau menyembunyikan informasi [7].

Dalam praktiknya, informasi disembunyikan dengan membuat perubahan terhadap data digital lain sehingga sulit untuk diketahui jika ada informasi yang disembunyikan. Perubahan dibuat sesedikit mungkin sehingga tidak akan menarik perhatian dari penyerang potensial. Perubahan ini bergantung pada algoritma yang dipakai dan pesan untuk disembunyikan. Penerima kemudian dapat mengambil informasi terselubung dengan cara membalik algoritma yang digunakan.

LSB adalah salah satu algoritma steganografi yang menyisipkan informasi di bagian bit dari pixel yang berpengaruh paling minimal dari gambar yang digunakan. Semakin banyak bit yang digunakan untuk menyisipkan informasi, semakin berpengaruh pula kepada media yang disisipi. Setelah informasi disisipkan, setiap pixel dibangun kembali menjadi gambar yang utuh menyerupai dengan media gambar semula [1].

2.2 *Discrete Wavelet Transform*

Discrete Wavelet Transform(DWT) adalah sebuah metode kompresi gambar yang memiliki tingkat kompresi yang tinggi. DWT sendiri memiliki frekuensi ruang sendiri yang sangat baik. DWT membagi sinyal menjadi bagian frekuensi tinggi dan rendah. Bagian frekuensi tinggi berisi informasi tentang komponen yang mencolok, sementara bagian frekuensi rendah dibagi lagi menjadi bagian frekuensi tinggi dan rendah. Komponen frekuensi tinggi biasanya digunakan untuk steganografi karena mata manusia kurang sensitif terhadap perubahan di frekuensi yang tinggi [4].

Langkah yang dilakukan oleh DWT adalah membagi *image* menjadi 2 bagian yang dipisah berdasarkan frekuensi secara vertikal. Lakukan hal yang sama secara horizontal sehingga sub-*image* berukuran ¼ kali dari citra asli. Sub-*image* pada posisi atas kanan, bawah kiri, dan bawah kanan terlihat seperti versi kasar dari gambar asli karena berisi komponen frekuensi tinggi dari gambar asli. 1 sub-image atas kiri terlihat seperti gambar asli yang lebih halus karena berisi komponen frekuensi rendah dari gambar asli. Sedangkan nilai piksel (koefisien) 3 sub-image yang lainnya cenderung bernilai rendah dan terkadang bernilai nol sehingga mudah dikompresi.

Dalam keadaan kompresi *lossless*, gambar yang telah direkonstruksi setelah kompresi, secara numerik identik dengan gambar asli. Namun kompresi *lossless* hanya bisa mencapai jumlah kompresi yang sederhana. Sebuah gambar yang dikompresi menggunakan *lossy compression* mengandung degradasi relatif terhadap yang asli. Hal ini terjadi karena kompresi yang *lossy* membuang informasi yang bernilai tinggi. Namun kompresi *lossy* mampu mencapai rasio kompresi yang lebih tinggi. Dalam kondisi normal tidak terlihat berbeda [2].

2.3 Jpeg2000

Saat ini gambar dan video digital digunakan di banyak bidang kehidupan kita. Dari kamera digital yang lebih sederhana ke jaringan server di Internet. Karena gambar disimpan dalam perangkat ini, kita perlu mengurangi ukuran gambar untuk mengumpulkan sebanyak mungkin gambar di ruang penyimpanan minimum tanpa kehilangan kualitas. Kebutuhan ini telah diturunkan dalam penampilan beberapa algoritma yang didedikasikan untuk kompres gambar dengan atau tanpa kehilangan data. Gambar adalah matriks titik (piksel) yang masing-masing menunjukkan tingkat nada atau warna pada posisi spasialnya. Oleh karena itu, suatu gambar dapat direpresentasikan secara matematis sebagai matriks dengan angka yang menunjukkan nilai piksel pada setiap posisi.

Tujuan dari pengembangan sistem JPEG2000 tidak hanya untuk memberikan efisiensi kompresi yang lebih tinggi dibandingkan dengan JPEG. Tujuan dari pengembangan JPEG 2000 juga untuk memberikan representasi gambar baru dengan serangkaian fitur yang kaya, semuanya didukung dalam hal yang sama bit-stream terkompresi, yang dapat mengatasi suatu variasi aplikasi kompresi yang ada [5].

Pengembangan JPEG 2000 dimulai pada tahun 1996, setelah munculnya beberapa algoritma kompresi awal tahun 1990 dengan kinerja kompresi yang lebih baik dan fitur-fitur baru yang. Setelah beberapa kontribusi teknis dan pembuatan beberapa model verifikasi, JPEG 2000 menjadi standar internasional pada Desember 2000. Untuk menghindari artefak yang terjadi pada gambar, JPEG 2000 menggunakan transformasi wavelet dengan lifting implementation, yang memiliki sifat pelokalan yang baik, untuk memproses blok yang lebih besar daripada JPEG. Wavelet juga menyediakan properti skalabilitas resolusi. Karakteristik lain adalah bahwa blok yang diproses dalam JPEG 2000 berasal dari domain wavelet dan bukannya domain ruang dan run length encoding yang digunakan dalam JPEG diganti dengan bit-plane encoding, yang memastikan rekonstruksi gambar dengan degradasi yang anggun dari setiap titik terpotong. dari bit stream terbentuk setelah bit-plane encoding [5].

2.4 *Lossy* dan *Lossless Compression*

Ada dua jenis skema kompresi gambar yaitu: Kompresi lossless dan kompresi lossy. Dalam skema kompresi lossless, gambar yang direkonstruksi adalah replika yang tepat dari gambar aslinya. Dalam kompresi gambar lossy, gambar yang direkonstruksi mengandung degradasi relatif terhadap aslinya. Dalam kompresi lossy, kompresi yang lebih tinggi dapat dicapai jika dibandingkan dengan skema kompresi lossless [6].

Dalam hal lossless metode pengkodean umum terdiri dari teknik pengkodean entropi yang meliputi Huffman coding, arithmetic coding, run length coding, dan dictionary based coding. Metode domain spasial beroperasi langsung pada piksel gambar, menggabungkan algoritma domain spasial dan metode pengkodean. Metode transformasi domain mentransformasikan gambar dari representasi domain spasial ke tipe representasi berbeda menggunakan algoritma transformasi [6].

Secara umum, kompresi lossy diimplementasikan menggunakan pengkodean domain spasial dan mengubah metode pengkodean domain. Teknik domain spasial umumnya menggunakan fungsi prediksi, di mana nilai piksel saat ini ditentukan oleh pengetahuan tentang piksel yang sebelumnya dikodekan.

Dalam teknik mentransformasikan domain, transformasi gambar digunakan untuk menghias terkait piksel. Dengan demikian, informasi gambar dikemas ke dalam sejumlah kecil koefisien. Koefisien dalam domain transformasi kemudian dikuantisasi untuk mengurangi jumlah bit yang dialokasikan. Kesalahan atau kehilangan informasi disebabkan oleh langkah kuantisasi. Koefisien terkuantisasi yang dihasilkan memiliki probabilitas berbeda dan skema pengkodean entropi selanjutnya dapat mengurangi jumlah bit yang diperlukan. Transform coding umumnya digunakan untuk metode kompresi gambar lossy karena memberikan kompresi data yang lebih besar dibandingkan dengan metode lain [6].

2.5 *Advanced Encryption Standard*

Advanced Encryption Standard(AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok *ciphertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data menjadi data yang tidak dapat lagi dibaca yang disebut *ciphertext*; sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang dikenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkripsi dan dekripsi data pada blok 128 bits. .

2.6 *Peak Signal to Noise Ratio*

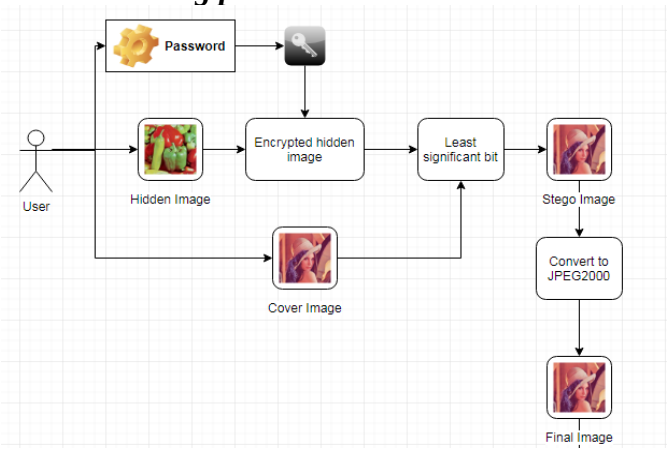
PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya *noise* yang berpengaruh pada sinyal tersebut. PSNR digunakan untuk mengukur kualitas citra digital sesudah disisipkan gambar. Untuk menentukan nilai PSNR, maka harus ditentukan terlebih dahulu nilai dari MSE(*Mean Square Error*). MSE adalah rata-rata dari nilai error kuadrat antara citra asli (*cover image*) dengan citra hasil penyisipan (*stego image*).

2.7 *Lossy* dan *Lossless Compression*

C#(dibaca C Sharp) adalah bahasa pemrograman yang didesain dan dikembangkan oleh Microsoft dan dirilis pada tahun 2000. C# memiliki fungsi seperti bahasa pemrograman pada umumnya, dengan menonjolkan OOP. Unity sebagai game engine, mendukung C# sebagai salah satu bahasa yang digunakan untuk melakukan scripting, selain Java. C# sebagai salah satu bahasa pemrograman yang simpel dan mudah digunakan mendukung Unity sebagai game engine agar mudah diakses oleh orang awam maupun berpengalaman karena membutuhkan waktu lebih singkat untuk dipelajari.

3. DESAIN SISTEM

3.1 *Embedding process*



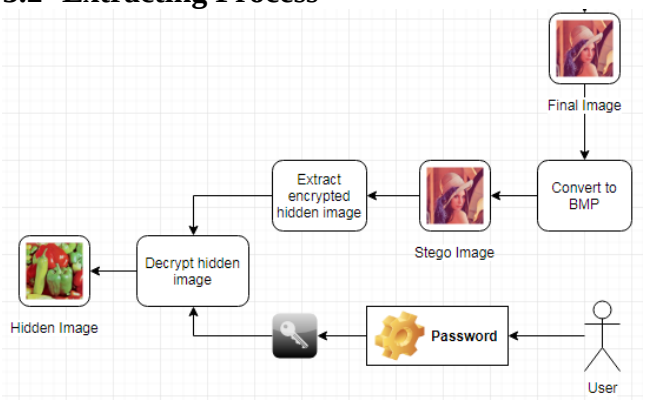
Gambar 1. Langkah - langkah menyembunyikan *hidden image*

Algoritma yang digunakan untuk menyembunyikan gambar adalah :

1) Membuat kunci dari sebuah *password* yang di inputkan oleh *user*.
2) Melakukan enkripsi terhadap *hidden image*.
3) Melakukan steganografi yaitu menyembunyikan *hidden image* menggunakan algoritma *least significant bit* pada *cover* image.
4) Melakukan konversi gambar menjadi jpeg2000.

Keseluruhan proses *embed* ditunjukkan pada Gambar 1.

3.2 Extracting Process



Gambar 2. Langkah - langkah mengekstrak *hidden image*

Algoritma yang digunakan untuk mengekstrak gambar adalah :
1) Membuat kunci dari sebuah *password* yang di inputkan oleh *user*.
2) Melakukan konversi gambar menjadi bmp.
3) Melakukan ekstraksi terhadap *stego image*.
4) Melakukan dekripsi pada *hidden image* dengan kunci yang sudah dibuat.

Keseluruhan proses ekstraksi ditunjukan pada Gambar 2

4. PENGUJIAN SISTEM

Tabel 1. Tabel Gambar Yang Digunakan

Image Role	Image Name	Width (pixel)	Height (pixel)	Size (bytes)	RGB
Cover Image	Downtown.bmp	1714	1162	5977382	Yes
Hidden Image	Tulip.bmp	512	384	589878	Yes
Final Image	Encoded.jp2	1714	1162	3378539	Yes

Pada Tabel 1 dilakukan pengujian PSNR dimana *cover image* adalah downtown.bmp dan *hidden image* adalah tulip.bmp. Hasil Pengukuran dilakukan dengan menggunakan PSNR, angka yang dicapai dengan membandingkan *final image* dan *cover image* adalah 52.1644.

Gambar 3. Perbandingan h*idden image* dengan gambar hasil ekstraksi

Gambar 3 menunjukkan perbandingan antara gambar asli yang disembunyikan dan gambar yang di ekstraksi. Jika diukur menggunakan PSNR, maka nilai PSNR adalah tidak terbatas. Hal ini terjadi karena hasil dari perbandingan antara 2 gambar memiliki *mean square error* bernilai nol. Hasil ekstraksi memiliki nilai citra yang sama dengan gambar asli.

5. KESIMPULAN

Dari hasil analisa saat implementasi dan pengujian program, ditarik beberapa kesimpulan sebagai berikut:

- Dengan mengenkripsi hidden image menggunakan algoritma AES dan steganografi least significant bit, informasi mengenai hidden image tetap terjaga karena hidden image berbentuk ciphertext. Tanpa adanya kunci yang tepat, data tetap berupa ciphertext.
- Kompresi yang digunakan adalah kompresi yang bersifat lossless. Meskipun melewati tahap kompresi menggunakan dan dekompresi discrete wavelet transform, gambar yang terenkripsi tidak hilang.

6. REFERENCES

[1] Badescu, I. , & Dumitrescu, C. 2014. *Steganography in image using discrete wavelet transformation*. URI= http://www.wseas.us/e-library/conferences/2014/Brasov/MATHPRO/MATHPRO-11.pdf.

[2] Das, J. 2017. *Lossless performance of image compression using 2D DWT*. URI= http://ficta.in/attachments/article/55/15%20Lossless%20performance%20of%20image%20compression%20using%202D%20DWT.pdf.

[3] Katre, B. & Bharti .2017. *Dynamic Key based LSB Technique for Steganography*. URI= http://www.ijcaonline.org/archives/volume167/number13/katre-2017-ijca-914332.pdf.

[4] Parul, Manju, & Rohil, H. 2015. *Optimized Image Steganography using Discrete Wavelet Transform*. URI= https://pdfs.semanticscholar.org/3207/296533f9e2180c8da1f9b7ceacd91c1cde43.pdf

[5] Ramis, J.J.B. 2015. *The JPEG 2000 Compression Standard.* URI= http://www.maia.ub.es/~soria/TFM_Juanjo-Bonet.pdf

[6] Vidhya, K., et al. 2016. *A Review of lossless and lossy image compression techniques.* URI= https://pdfs.semanticscholar.org/bb11/21d3873944b4d63fc3610b0abd89a15c3076.pdf.

[7] Wakure, M.A., & Holambe, A.N. (2015), *A Discrete Wavelet Transform: A Steganographic Method for Transmitting Images.* URI= http://www.ijcaonline.org/research/volume129/number5/wakure-2015-ijca-906915.pdf