PERANCANGAN APLIKASI ALGORITMA AES RIJNDAEL PADA ENKRIPSI CITRA DIGITAL FILE JPEG 128 BIT

Dewi Cita Anggarini[1], Citra Kurniawan[2]
Sekolah Tinggi Teknik Malang[12]
dewicitaanggarini@gmail.com[1]
airakurniawan@gmail.com[2]

ABSTRACT

Human Problems Abuse Digital Image Data, Sender To Communicate That Sender Send Data To Recipient And want the data sent safe but in fact the data is susceptible to tapping on process of sending data so that it not up to recipient of data and fall into the hands of unauthorized people so can be misused. The way to maintain data security and confidentiality is by encryption and decryption techniques. This study aims to explain the implementation of jpeg rgb and grayscale file format in Aes Rijndael 128 bit Algorithm Application for encryption and decryption of digital image files. This research type is research & development (R & D). In this research, testing is done, that is the application feasibility test which includes media expert has 98% feasibility percentage and material expert has a feasibility percentage of 86%, concluded this application is very feasible. Conclusion if the Key used numbers with different pixel size and image capacity and resulted in different running times. The larger the pixel value of the image the time required is also the time and duration between encryption and decryption can be longer or even faster. If the length of the key pixel size and the same size of the image, does not affect the long running time, while if the pixel size is the same but the bigger the image is smaller then the running time is faster.

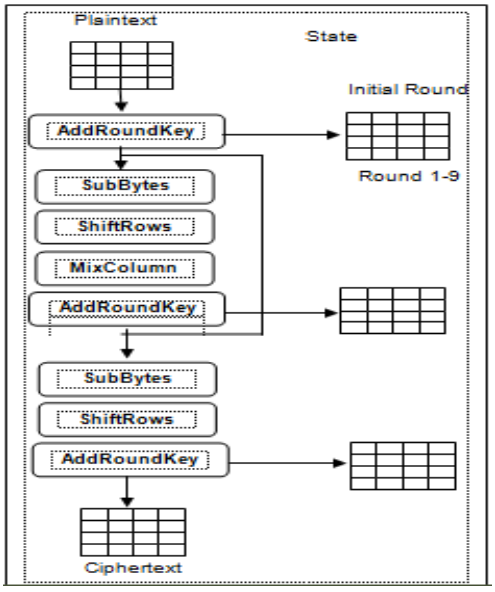
Keywords: Digital Image, Security, Algorithm Aes Rijndael

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi juga memudahkan manusia untuk mengakses data dan informasi dengan mudah. Manusia banyak melakukan penyalahgunaan data citra digital yang dilakukan sengaja atau tidak sengaja sehingga menyebabkan kerugian pada pihak lain. Salah satu penyalahgunaan yang sangat umum seperti pengirim melakukan proses komunikasi yaitu pengirim mengirim data kepada penerima dan menginginkan data terkirim aman namun faktanya pada perkembangan dan kemajuan teknologi data tersebut rentan terjadi penyadapan pada proses pengiriman data sehingga tidak sampai oleh penerima data dan jatuh ketangan orang yang tidak berhak sehingga dapat disalahgunakan. Kemanan yang digunakan untuk melindungi data menggunakan teknik enkripsi terhadap *file* citra digital.

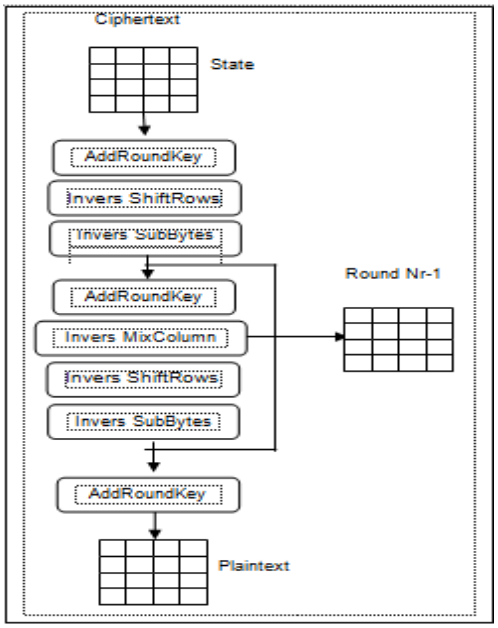
TINJAUAN PUSTAKA

Algoritma AES merupakan aturan, proses atau fungsi matematika yang digunakan dalam pengamanan data dan informasi yang disebut enkripsi dan dekripsi. Menurut Didi (2006), Proses enkripsi yaitu mengubah pesan asli *(plaintext)* menjadi pesan dalam bentuk kode *(ciphertext)* dan hanya dapat dibuka atau dibaca oleh pihak penerima yang berhak sedangkan proses dekripsi adalah mengembalikan data dalam bentuk kode menjadi bentuk data asli. Algoritma AES Rinjdael memiliki ukuran blok dengan panjang kunci 128 bit, 192 bit dan 256 bit yang dipilih secara independen. Pemilihan blok dan kunci akan menentukan jumlah putaran *(round)* yang akan dilalui untuk proses enkripsi dan dekripsi.



Gambar 1 Proses Enkripsi

(Sumber: Kristoforus, dkk ,2012)



Gambar 2 Proses Dekripsi

(Sumber: Kristoforus, dkk ,2012)

Algoritma AES Rijndael memiliki 4 tahap utama dalam satu kali putaran *(round)* yang terdiri dari SubBytes, ShiftRows, MixColumns dan AddRoundKey untuk enkripsi dan *diinvers* untuk dekripsi, namun sebelum tahap *round* diatas diproses akan ada tahap utama pada Algoritma Aes Rijndael terdiri dari *key schedule* atau menentukan *subkey* yang selanjutnya akan diproses untuk enkripsi dan dekripsi. Tahap subkey terdiri dari 4 tahap yaitu tahap RotWord, tahap SubWord, tahap XOR nilai dari SubWord dengan tabel R-Con dan tahap terakhir XOR nilai tahap sebelumnya dengan Wi-4. Hasil dari proses *key schedule* disebut *cipher key*. Tahap Enkripsi dan Dekripsi Algoritma AES Rijndael 128bit terdiri dari 10 round.

METODE PENELITIAN

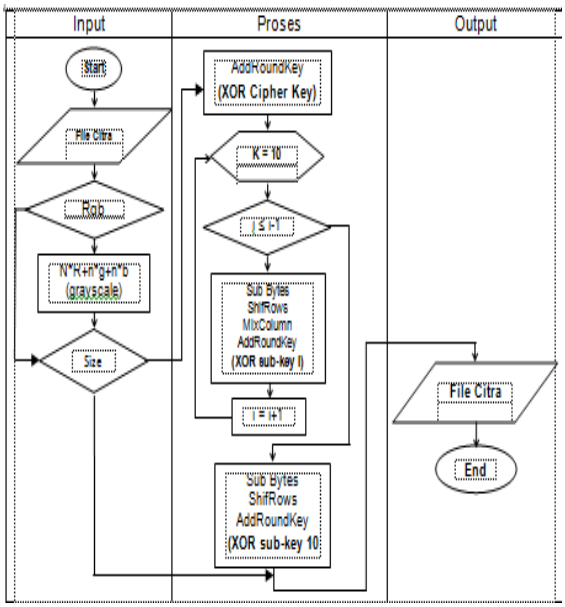
Dalam penelitian dengan judul "Perancangan Aplikasi Algoritma Aes Rijndael Pada Enkripsi File Citra Digital Jpeg 128 Bit" menggunakan metode penelitian R & D *(Research and Development)*. Menurut Maya dalam Sugiono (2012:407), Penelitian R & D *(Research and Development)* adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk tertentu. Pada metode penelitian dijelaskan jenis data yang digunakan pada penelitian ini adalah data primer dan data sekunder. Data primer adalah data yang diperoleh dari penelitian langsung seperti ukuran dari *file* citra digital yang akan digunakan sedangkan data sekunder adalah data yang diperoleh dari penelitian terdahulu atau penelitian yang sudah ada, dari jurnal dan buku. Sumber data pada penelitian ini diperoleh dari penelitian terdahulu atau penelitian yang sudah ada, dari jurnal dan buku. Sifat dari penelitan ini adalah perancangan dari latar belakang permasalahan yang ada.

HASIL PEMBAHASAN

Penelitian ini dilakukan menggunakan ukuran maksimal, jenis dan format *file* citra digital yang dibatasi. Kunci yang digunakan sebagai pengaman adalah angka dengan panjang maksimal 15 angka. Algoritma dalam penelitian ini adalah Algoritma AES Rijndael 128 bit. Software implementasi yang digunakan adalah Matlab R2011a. Dalam penelitian ini variabel bebas yang digunakan adalah ukuran *file* maksimal 750 x 750 piksel, jenis *file* citra yang digunakan *Rgb* dan *grayscale* dengan format *file* yaitu jpeg yang diimplementasikan pada Algoritma Aes Rijndael 128 bit, merupakan karakteristik dari *file* citra digital untuk enkripsi dan dekripsi, variabel terikat dari penelitian ini adalah hasil implementasikan *file* citra digital jpeg *grayscale* pada Algoritma Aes Rijndael 128. Dari penelitian ini diperoleh prediksi waktu selama *running time* dari enkripsi dan dekripsi *file* citra digital yang dipengaruhi oleh karakteristik dari *file* citra digital tersebut.

ALUR APLIKASI ENKRIPSI DAN DEKRIPSI

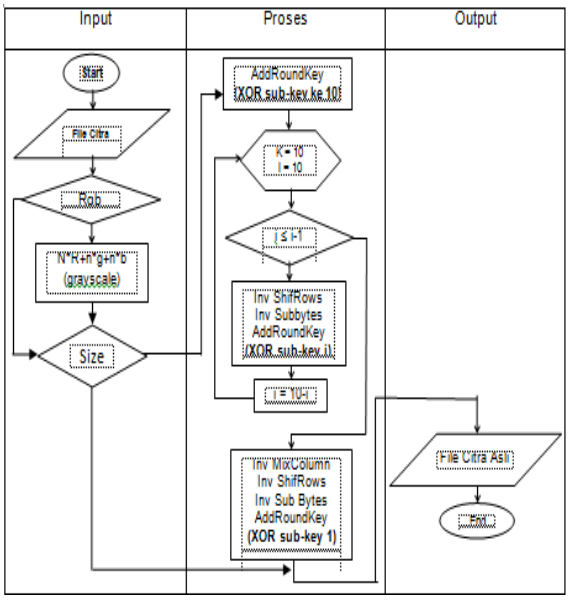
Pada gambar dibawah akan dijelaskan mengenai alur aplikasi dalam proses enkripsi dan dekripsi *file* citra digital *rgb* maupun *grayscale*.



Gambar 3 Flowchart Enkripsi

(Sumber : Peneliti)

Pada tabel *input* adalah *file* citra akan *diinputkan rgb* atau *grayscale* sebelum diproses akan mencari tahu *size* nya sesuai batasan atau melebihi maksimal 750 x 750 piksel, jika melebihi batasan maka tidak dapat diproses namun jika sesuai dengan batasan yang ditentukan maka akan diproses sesuai alur pada tabel proses dan menghasilkan *output* file citra yang sudah dienkripsi.



Gambar 4 Flowchart Dekripsi

(Sumber : Peneliti)

Pada tabel *input* adalah *file* citra hasil enkripsi akan *diinputkan rgb* atau *grayscale* sebelum diproses akan mencari tahu *size*nya sesuai batasan atau melebihi maksimal 750 x 750 piksel, jika melebihi batasan maka tidak dapat diproses namun jika sesuai dengan batasan yang ditentukan maka akan diproses sesuai alur pada tabel proses dan menghasilkan *output file* citra asli yang sudah didekripsi.

LAY OUT APLIKASI

1. Menu Utama

Menu utama pada aplikasi Perancangan Aplikasi Algoritma Aes Rijndael Pada Enkripsi Citra Digital File Jpeg 128 Bit ini adalah menu yang akan mengarahkan user pada menu enkripsi, menu dekripsi, menu help dan button *exit*.

Gambar 5 Tampilan Menu utama

(Sumber : Peneliti)

Menu Utama pada aplikasi ini berisi *button* enkripsi untuk masuk menu enkripsi, *button* dekripsi untuk masuk menu dekripsi, *button help* untuk masuk menu *help* dan *exit* untuk keluar aplikasi.

2. Menu Enkripsi

Menu enkripsi adalah menu yang berisi tentang proses mengubah *file* citra digital jpeg menjadi *file* citra yang tidak dapat dilihat aslinya. Pada menu enkripsi terdapat 6 *button*

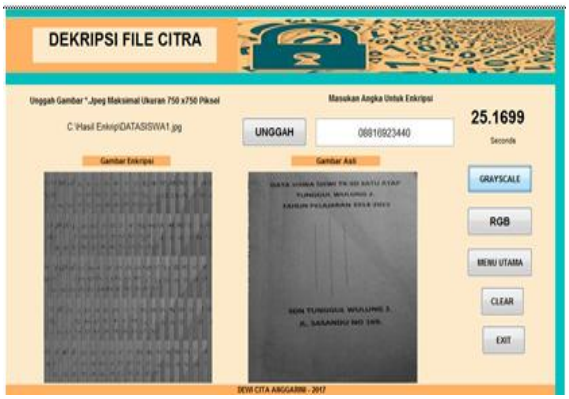
yaitu *button* unggah yang berfungsi untuk mengunggah *file* citra jpeg asli, *button* enkripsi rgb dan *grayscale* yang berfungsi untuk melakukan proses enkripsi *file* citra, *button* menu utama yang berfungsi untuk masuk pada menu utama, *button clear* berfungsi untuk membersihkan tampilan dari aplikasi dan *button exit* untuk keluar dari aplikasi. Pada menu enkripsi terdapat 1 *edit text* untuk memasukan kunci dan 2 *axes* untuk menampilkan *file* citra asli dan *file* citra hasil enkripsi.

Gambar 6 Tampilan Menu Enkripsi
(Sumber : Peneliti)

Pada menu enkripsi terdapat *text* untuk menampilkan lokasi *file* dan *running time* untuk mengetahui lama waktu yang dibutuhkan dalam proses enkripsi dengan satuan *second* dan terdapat *edit text* untuk memasukan angka sebagai pengaman dari *file* citra hasil enkripsi. Hasil enkripsi akan tersimpan secara otomatis pada folder hasil enkrip di *drive* C.

3. Menu Dekripsi

Menu dekripsi adalah menu yang berisi tentang proses mengembalikan *file* citra enkripsi menjadi *file* citra digital jpeg asli. Pada menu dekripsi terdapat 6 *button* yaitu *button* unggah yang berfungsi untuk mengunggah *file* citra jpeg asli, *button* dekripsi rgb dan *grayscale* yang berfungsi untuk melakukan proses dekripsi *file* citra, *button* menu utama yang berfungsi untuk masuk pada menu utama, *button clear* berfungsi untuk membersihkan tampilan dari aplikasi dan *button exit* untuk keluar dari aplikasi. Pada menu dekripsi terdapat 1 *edit text* untuk memasukan kunci dan 2 *axes* untuk menampilkan *file* citra hasil enkripsi dan *file* citra asli.



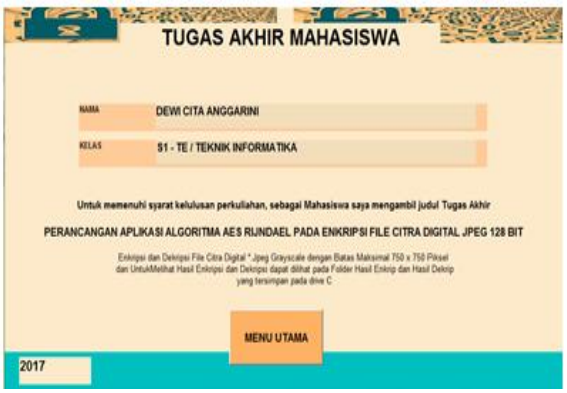
Gambar 7 Tampilan Menu Dekripsi
(Sumber : Peneliti)

Pada menu dekripsi terdapat *text* untuk menampilkan lokasi file dan *running time* untuk mengetahui lama waktu yang dibutuhkan dalam proses dekripsi dengan satuan *second* dan terdapat *edit text* untuk memasukan angka sebagai pengaman dari *file* citra dekripsi. Hasil

dekripsi akan tersimpan secara otomatis pada folder hasil dekrip di *drive* C.

4. Menu *Help*

Menu *help* aplikasi adalah menu yang berisi informasi tentang aplikasi, judul penelitian dan karakteristik *file* citra yang dapat digunakan pada aplikasi.



Gambar 8 Tampilan Menu Help

(Sumber : Peneliti)

Menu *help* menggunakan satu *button* untuk menuju ke menu utama.

KESIMPULAN

Berdasarkan hasil penelitian **Perancangan Aplikasi Algoritma Aes Rijndael Pada Enkripsi Citra Digital File Jpeg 128 Bit** yang telah dilakukan, kesimpulan yang diperoleh adalah Ukuran piksel dari *file* citra digital mempengaruhi lamanya *running time* dari proses enkripsi dan dekripsi, Penggunaan kunci pada proses enkripsi dan dekripsi harus sama, jika penggunaan kunci berbeda dari proses enkripsi dan dekripsi tidak dapat dikembalikan ke *file* citra asli, Semakin besar ukuran *file* citra digital maka semakin lama waktu *running time* yang dibutuhkan, *File* Citra Digital *grayscale* format Jpeg dapat diimplementasikan pada algoritma Aes Rijndael 128 bit.

DAFTAR RUJUKAN

Adhi Kusnadi. 2011. *Identifikasi Objek Berdasarkan Citra Warna Menggunakan Matlab. Laporan Hasil Penelitian*. Program Studi Teknik Informatika Fakultas Teknik, Matematika dan Ilmu Pengetahuan Alam Universitas Indraprasta PGRI

Agustinna Yosanny. 2010. *Perancangan Enkripsi Pada Citra Bitmap Dengan Algoritma Des, Triple Des dan Idea. Laporan Hasil Penelitian.* Comtech Vol.1 No.2, Desember 2010, 853-866. Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Bina Nusantara University

Anisah Muharini. 2012. Aplikasi Algoritma Rivest Code 6 Dalam Pengamanan Citra Digital. *Laporan Hasil Penelitian*. Fakultas Matematika Dan Ilmu Pengetahuan Alam Program Study Sarjana Matematika Universitas Indonesia. Depok

Bertalya. 2005. *Representasi Citra*

Dedi Alyanto. 2016. Penerapan Algoritma Aes : Rijndael Dalam Pengenkripsian Data

Rahasia Sekolah Tinggi Manajemen Informatika Dan Komputer. *Laporan Hasil Penelitian.* Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika Dan Komputer Stmik Time. Medan

Dessy Purwandani. Implementasi Metode Gaussian Smoothing Untuk Penghalusan Citra (Image Smoothing). *Pelita Informatika Budi Darma*, Volume. Ix No. 2, Maret 2015, Issn 2301-9425

Didi Suriana. 2006. Algoritma Kriptografi Aes Rijndae. *Jurnal Teknik Elektro.* Vol. 8 No.2, Oktober 2010, Hal 97-101

Fadhilah Hanifah. 2012. Aplikasi Algoritma Aes Rijndael Dalam Pengamanan Citra Digital. *Laporan Hasil Penelitian*. Fakultas Matematika Dan Ilmu Pengetahuan Alam Program Study Sarjana Matematika. Universitas Indonesia. Depok

Henry, Awang Harsa Kridalaksana, Zainal Arifin. 2016. Kriptografi Aes Mode Cbc Pada Citra Digital Berbasis Android . *Prosiding Seminar Ilmu Komputer dan Teknologi Informasi,* Vol.1, No.1, September 2016, 45-52 ISSN 2540 – 7902

Jb, R.Kristoforus, Stefanus Aditya Bp. 2012. Implementasi Algoritma Rijndael Untuk Enkripsi Dan Dekripsi Pada Citra Digital. Makalah disajikan dalam Seminar Nasional Aplikasi Teknologi Informasi *2012 (SNATI 2012).* Yogyakarta, 15-16 Juni 2012

Kusumanto, R. D, Alan Novi Tompunu Dan Wahyu Setyo Pambudi. Klasifikasi Warna Menggunakan Pengolahan Model Warna Hsv. *Jurnal Ilmiah Elite Elektro*, Vol. 2. No.2, September 2011, Hal 83-87

Maya Marselia. 2012. Pembuatan Media pembelajaran Berbasis Film Animasi Kartun Pada Pengenalan Perangkat Keras Komputer Dalam Pembelajaran TIK di Kelas VII. *Laporan Hasil Penelitian*. Universitas pendidikan Indonesia

Nur Nafi'iyah. Algoritma Kohonen Dalam Mengubah Citra Graylevel Menjadi Citra Biner. *Jurnal Ilmiah Teknologi Dan Informasi ASIA (JITIKA),*Vol. 9 No. 2, Agustus 2015, ISSN: 0852-730X, Prodi Teknik Informatika Universitas Islam Lamongan

Rifkie Primartha. 2013. Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Advanced Encryption Standard (Aes). *Laporan Hasil Penelitian*. Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Rizki Muriliasari , Murinto. Analisis Perbandingan Metode Li Dan Chan-Vese Pada Proses Segmentasi Citra Digital . *Jurnal Sarjana Teknik Informatika*, Vol. 1 No. 2, Oktober 2013, E-Issn: 2338-5197 Program Studi Teknik Informatika

Universitas Ahmad Dahlan Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo. Yogyakarta

Rohmat Nur Ibrahim. 2012. Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (Dwt). *Jurnal Computech & Bisnis*. Vol. 6, No. 2, Desember 2012, 82-95 ISSN 2442-4943

Sri Wahyuningsih1, Theodora V.D Pandex, Vanessa Stefanny. 2016. Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital. *Jurnal Telematika Mkom*. Vol.8 No.2, September 2016, Program Studi Magister Ilmu Komputer, Program Pascasarjana Universitas Budi Luhur, Jakarta Selatan