Paper

Optimasi Algoritma AES Dengan Implementasi Parallel Dalam Pengamanan Data Digital

Author: Nur Wulan, Siti Sundari, Rapna Dewi

ISNN: 2964-1950

Optimasi Algoritma AES Dengan Implementasi Parallel Dalam Pengamanan Data Digital

Nur Wulan [1], Siti Sundari[2], Rapna Dewi[3*]
[1,2,3]Universitas Harapan Medan, Indonesia
[1]Nurwulanstth@gmail.com, [2]Sundaristth@gmail.com, [3]rapnadewi99@gmail.com

Abstrak

Pengamanan data digital adalah perlindungan terhadap data yang bersifat privat untuk mencegah akses yang tidak di inginkan terhadap komputer *database*, maupun *website*. Pada penelitian ini menggunakan teknik kriptografi yang merupakan sebuah cara untuk mengamankan data. Mengapa data digital perlu diamankan, karena dapat mencegah potensi kerugian material, mengurangi resiko penyalahgunaan data, dan memperkecil tindakan kriminal.Pada penelitian ini terdapat akan melakukan optimasi algoritma AES yang sebelumnya proses Algoritma AES memiliki memiliki tingkat kompleksitas waktu yang linear, dimana semakin besar jumlah blok N yang diproses maka juga akan meningkatkan waktu eksekusi. Perancangan pada penelitian ini menggunakan *unified modelling language* dan *mysql* sebagai *database*. Tujuan dari penelitian ini Mengimplementasikan algoritma parallel AES untuk proses enkripsi – dekripsi data digital dan Menganalisis dan memberikan rekomendasi terhadap algoritma yang akan digunakan kedepannya dengan mempertimbangkan hasil perbandingan yang didapat.

Kata kunci : *Keamanan, Digital, AES*

Abstract

Digital data security is the protection of private data to prevent unwanted access to computer databases or websites. In this study, cryptographic techniques are used which is a way to enter data. Why data needs to be digital, it can prevent potential loss, reduce data risk, and reduce crime. In this study, we will optimize the AES algorithm, the AES algorithm has a linear speed, where the greater the number of N blocks to be executed, the higher the execution time. The design in this study uses a unified modeling language and mysql as a database. The purpose of this study is to implement the parallel AES algorithm for the encryption and decryption process of digital data and analyze and provide recommendations for the algorithm that will be used in the future by considering the comparison results obtained.

Keywords : *Security, Digital, Advanced Encryption Standart (AES)*

1. PENDAHULUAN

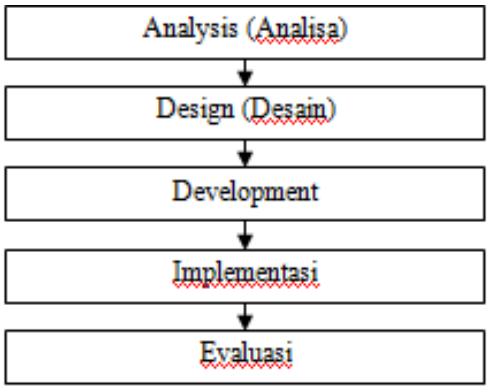
Data adalah aset terbesar dari setiap organisasi bisnis dan pemeliharaan data yang tepat adalah perhatian utama setiap organisasi. [1] Perkembangan teknologi informasi semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media. Komunikasi yang melibatkan pengiriman dan penerimaan pesan dengan memanfaatkan kemajuan teknologi informasi rentan terhadap pelaku kejahatan komputer yang memanfatkan celah keamanan untuk mendeteksi dan memanipulasi pesan. [2] Pentingnya nilai informasi pada setiap aspek dapat memungkinkan adanya usaha pemindah alihan atau pencurian informasi ataupun data oleh pihak yang tidak berwenang. Media penyimpanan dan penyebaran data atau informasi yang digunakan menjadi salah satu alasan rentannya data atau informasi mudah diambil oleh pihak yang kurang bertanggung jawab. [3] Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika dalam mengamankan suatu informasi atau pesan asli (Plainteks) menjadi sebuah teks tersembunyi (Chiperteks) dan kemudian di ubah menjadi pesan asli kembali. Kriptografi mempunyai tiga unsur penting yaitu pembangkitan kunci, enkripsi dan deskipsi. [4] AES merupakan sistem penyandian blok yang bersifat non-feistel kerena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128. Penyandian AES menggunakan proses yang berulang disebut dengan ronde. jumlah ronde yang digunakan oleh AES tergantung panjang kunci yang digunakan. [5] Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun password untuk mengakses sesuatu. Dengan mengenkrip paket data yang lalu lalang di Internet, walaupun seseorang dapat menangkap paket-paket data tersebut, tetap saja tidak dapat memahami artinya. [6] Algoritma AES termasuk dalam jenis algoritma Kriptografi yang sifatnya simetri dan cipherblock. Dengan algoritma ini mempergunakan kunci yang sama

saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Algoritma AES mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun AES mempunyai ukuran blok dan tetap sebesar 128, 192, 256 bit. [7] Untuk mengetahui apakah suatu algoritma kriptografi dapat mengamankan data dengan baik dapat dilihat dari segi lamanya waktu proses pembobolan untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer yang semakin canggih, maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, AES (Advanced Encryption Standard) merupakan algoritma cipher yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. [8] Dari dokumen terenkripsi akan dilakukan initial round dengan menambahkan chiper key sehingga akan menghasilkan data untuk dilakukan standard round sebanyak N putaran, mulai dari membagi byte (byte sub), operasi menggeser baris (shift row), mencampur kolom (mix coloumn) dan menambahkan round key yang diproduksi dengan operasi XOR Round Key setiap putarannya. Setelah itu finalisasi putaran dengan melakukan proses terhadap byte sub, shift row dan menambah ulang round key ke-N dan hasil akhirnya berupa chipertext. [9] Untuk menghadapi permasalahan diatas maka dirasakan perlu untuk membuat suatu sistem keamanan. Salah satu cara untuk meningkatkan keamanan pesan adalah dengan menggunakan kriptografi. [10]

Berdasarkan permasalahan yang dimiliki algoritma AES biasa atau serial yang memiliki tingkat kompleksitas waktu yang tidak efektif dan banyak sekali penyalahgunaan data dan penyebaran informasi yang dilakukan secara sengaja atau tidak, maka penulis bermaksud untuk membuat enkripsi dan dekripsi data menggunakan algoritma AES.

2. METODOLOGI PENELITIAN

Dalam menyelesaikan penelitian ini terdapat metode penelitian yang digambarkan pada gambar 1 berikut ini.



Gambar 1. Metodologi Penelitian

Adapun penjelasan tahapan metode penelitian pada gambar 1, dapat dijelaskan sebagai berikut:

1. Analysis (Analisa)
   Mempersiapkan dan menganalisa kebutuhan dari software yang akan dikerjakan. Informasi dan insight yang diperoleh dapat berupa dari hasil wawancara, survei, studi literatur, observasi, hingga diskusi.
2. Design (Desain)
   Pembuatan desain aplikasi sebelum masuk pada proses coding. Tujuan dari tahap ini, supaya mempunyai gambaran jelas mengenai tampilan dan antarmuka yang kemudian akan dieksekusi oleh programmer.
3. Development
   Development kode program dengan menggunakan berbagai *tools* dan bahasa pemrograman sesuai dengan kebutuhan. Pada tahap implementasi ini lebih berfokus pada hal teknis, dimana hasil dari desain perangkat lunak akan diterjemahkan ke dalam bahasa pemrograman melalui *programmer* atau *developer*.
4. Implementasi
   Implementasi sistem bertujuan untuk mengetahui apakah perangkat lunak sudah sesuai dengan desain, dan fungsionalitas dari aplikasi apakah berjalan dengan baik atau tidak. Jadi, dengan adanya tahap pengujian,

maka dapat mencegah terjadinya kesalahan, bug, atau *error* pada program sebelum masuk pada tahap produksi.

5. Evaluasi

Pengoperasian dan perbaikan dari aplikasi. Setelah dilakukan pengujian sistem, maka akan masuk pada tahap produk dan pemakaian perangkat lunak oleh pengguna (*user*).

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini memerlukan beberapa tahapan yang akan diperoleh untuk mencapai hasil rancangan yang baik dan sesuai. Beberapa tahapan tersebut akan dijelaskan sebagai berikut.

3.1 Analisa dan Perancangan Sistem

Pembuatan sistem ini adalah bertujuan membuat aplikasi pengamanan pada data citra digital dengan menggunakan Metode AES (Advanced Encryption Standard)pada data teks. Sistem yang dapat mengamankan data *file*teks dengan maksimal sesuai dengan proses metode yang digunakan. Desain dan implementasi sistem mengamankan *file*teks ini meliputi desain data, deskripsi sistem, desain proses dan implementasi dan semua yang diperlukan dalam aplikasi *steganography* yang dirancang penulis.

3.2 Analisa Input

Analisis Input Dalam sistem *steganography* untuk mengamankan *file* teks yang akan diimplementasikan dalam aplikasi, *file* yang akan diamankan berupa *file* teks. Fungsi nya untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik *steganography* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas. Untuk memperoleh hasil yang maksimal dalam mengamankan pesan lewat *file*teks.

3.3 Analisis Kebutuhan Non Fungsional

Spesifikasi kebutuhan non fungsional adalah spesifikasi yang rinci tentang kebutuhan sistem ketika diimplementasikan. Kebutuhan sistem adalah kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan sebagai pendukung untuk membuat program.

3.3.1 Analisis Perangkat Keras

Perangkat keras adalah sebuah komponen atau unsur peralatan yang digunakan untuk mengimplementasikan sistem *steganography* pada *file* teks. Adapun perangkat keras yang digunakan secara optimal memerlukan spesifikasi minimum komputer sebagai berikut:

1. Processor core i3
2. Kapasitas RAM 4Gb
3. Monitor 1080
4. Keyboard dan Mouse

Secara keseluruhan spesifikasi perangkat keras komputer yang ada sudah memenuhi syarat kebutuhan perangkat lunak yang akan diaplikasikan.

3.3.2 Kebutuhan Perangkat Lunak

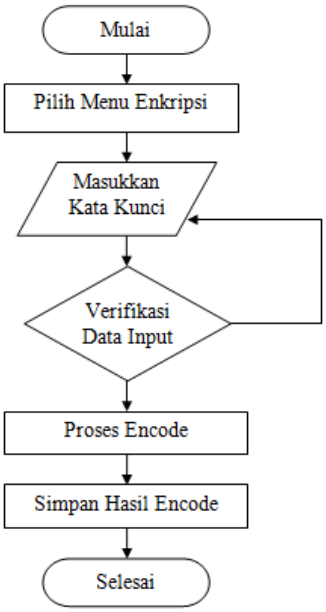
Perangkat lunak adalah beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya. Secara luas perangkat lunak dapat diartikan sebagai suatu produser pengoprasian. Adapun perangkat lunak yang digunakan secara optimal memerlukan spesifikasi minimum komputer sebagai berikut:

1. Windows 7 64 bit
2. Notepad ++

3.4 Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem menggunakan pemodelan UML *(Unified Modelling Language)* sehingga dapat memudahkan dalam penerapan sistem. Umlmerupakan model secara visual untuk sarana perancangan sistem berorientasi objek dan menerapkan perancangan interface, input, output, dan *database*. Dalam pembuatan sistem ini penulis menggunakan beberapa perangkat lunak diantaranya yaitu mozila sebagai web browser dan menggunakan bahasa pemrograman. PHP, MySQL sebagai *database* management system.

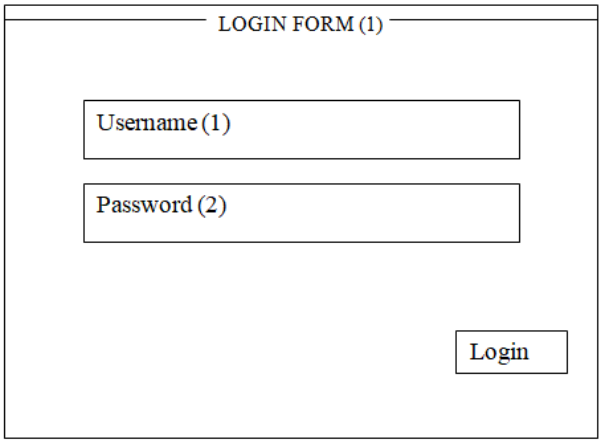
3.5 Flowchart



Gambar 2. Flowchart

1. Desain Form Login user

Desain *form login user* merupakan desain yang pertama sekali muncul ketika aplikasi dijalankan, *login* user yang pertama yang harus dilakukan oleh user adalah masuk kehalaman *login* /halaman tampilan utama sistem *steganography* pada *file* teks menggunakan algortima *Dynamic cell spreading*Kemudian melakukan pengisian *username* dan *password* pada *form login*. Jika *username* dan *pasword* yang di masukan salah, Maka sistem akan menampilkan *form login* kembali dan melakukan pengisian *username* dan *password* lagi. Dan jika benar maka sistem akan menampilkan halaman menu utama dan selanjutnya user dapat mengakses menu-menu yang disediakan sistem sesuai *level* masing- masing. Dengan begitu user bisa memulai penyisipan teks pada video. Berikut desain *form* menu *loginuser* yang dirancang penulis, lihat pada Gambar 3:



Gambar 3. Perancangan Desain Form Login user

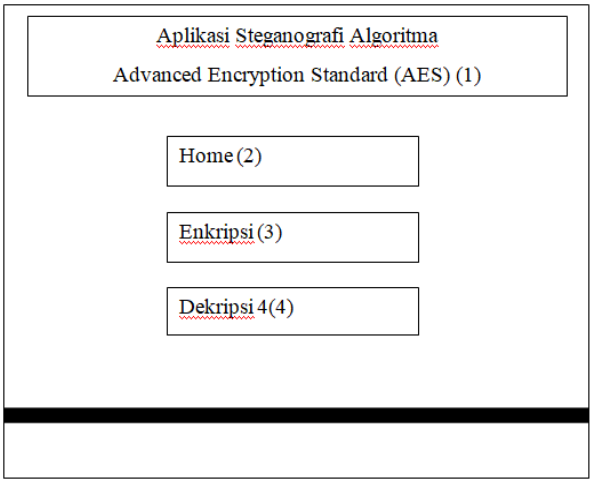
Adapun keterangan pada Gambar 3 adalah sebagai berikut :

1. Menu tampilan pada menu *login form* terdiri dari kolom *username , pasword , dan button login*.

2. Isi username dan *password* dengan benar lalu klik button login untuk mulai masuk untuk mengakses menu yang disediakan sistem.
3. Pada bagian login sistem akan melakukan proses login dengan mencocokan data pada database dengan melakukan proses authentifikasi terhadap username dan password

2. Desain Form Menu Utama

Desain *form* menu utama *user* menampilkan semua *form* yang ada pada *user*. Berikut adalah desain *form* menu utama *user* yang dirancang penulis, lihat pada Gambar 4:



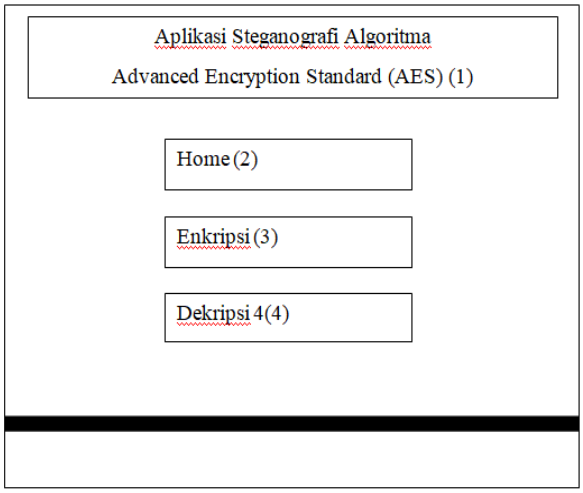
Gambar 4. Perancangan Tampilan Menu Utama

Adapun keterangan Gambar 4 adalah sebagai berikut:

1. Tampilan Utama
2. Menu tampilan pada menu utama tampilan *user* terdiri dari home, enkripsi dan dekripsi
3. Menu enkripsi berfungsi untuk melakukan pengamanan terhadap data citra digital yaitu teks
4. Menu dekripsi berfungsi untuk melihat isi dari pesan yang sudah disisipkan

3. Desain Menu Enkripsi

Desain enkripsi akan menampilkan semua *form* yang akan digunakan untuk proses enkripsi. Berikut adalah desain menu enkripsi yang dirancang penulis, lihat pada Gambar 5:



Gambar 5. Perancangan Tampilan Menu Utama

Adapun keterangan Gambar 5 adalah sebagai berikut:

1. Tampilan Utama
2. Menu tampilan pada menu utama tampilan *user* terdiri dari home, enkripsi dan dekripsi
3. Menu enkripsi berfungsi untuk melakukan pengamanan terhadap data citra digital yaitu teks
4. Menu dekripsi berfungsi untuk melihat isi dari pesan yang sudah disisipkan

2 Tampilan Sistem User

Pada tampilan sistem *user* yang berfungsi sebagai sistem yang digunakan oleh *user* untuk melihat *system* Algoritma *Advanced Encryption Standart* untuk pengamanan citra digital. Berikut ini adalah tampilan yang terdapat pada sistem *user*:

1. Tampilan login

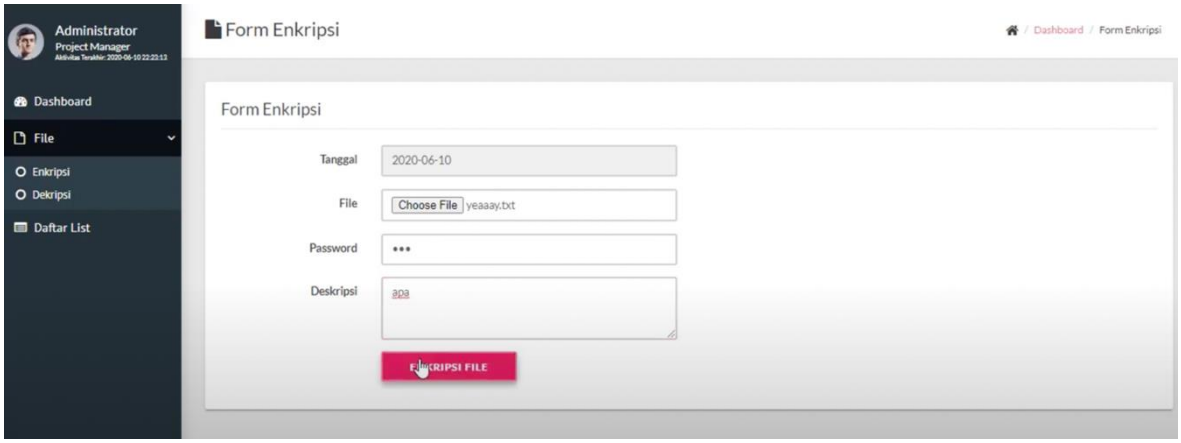
Pada menu tampilan login akan menampilkan *form login* seperti form *username* dan *password* Seperti pada gambar 6 berikut ini:

Gambar 6. Tampilan Menu login

Keterangan gambar 6 akan menjelaskan proses untuk dapat masuk kedalam system Algoritma *Advanced Encryption Standard* untuk pengamanan citra digital, pengguna harus memasukan *username* dan *password* kemudian database akan melakukan pemeriksaaan atau validasi data apakah username dan *password* yang dimasukan sudah sesuai dengan database, apabila sesuai pengguna akan langsung masuk kemenu utama dan apabila validasi salah pengguna harus memasukan *password* dan *username* kembali. Pada proses login user harus mengingat dengan baik data username dan *password* sehingga tidak terjadi kesulitan dalam melakukan *login*.

2. Menu enkripsi

Pada tampilan ini akan menampilkan semua menu dari sistem yang menerapkan sistem Algoritma *Advanced Encryption Standard* untuk pengamanan citra digital. menu enkripsi terdapat *form form* yang dapat melakukan enkripsi data digital. Berikut ini isi dari menu enkripsi yang akan ditampilkan pada gambar 7 berikut ini



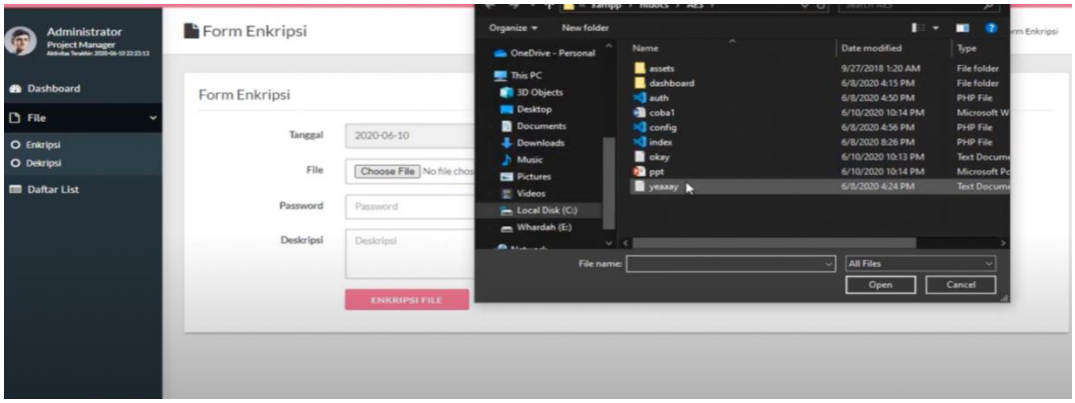
Gambar 7. Tampilan Menu Utama Enkripsi

Keterangan gambar 7 akan menjelaskan:

1. Pada menu enkripsi terdapat *form* tanggal, *file*, *password* dan dekripsi
2. Pada *form file* berfungsi memasukan data citra digital yang akan di amankan
3. Pada *form password* berfungsi sebagai keamanan untuk mengamankan *file*
4. Menu dekripsi merupakan merupakan menu yang betujuan sebagai deskripsi dari suatu *file*

3. Tampilan menu input enkripsi

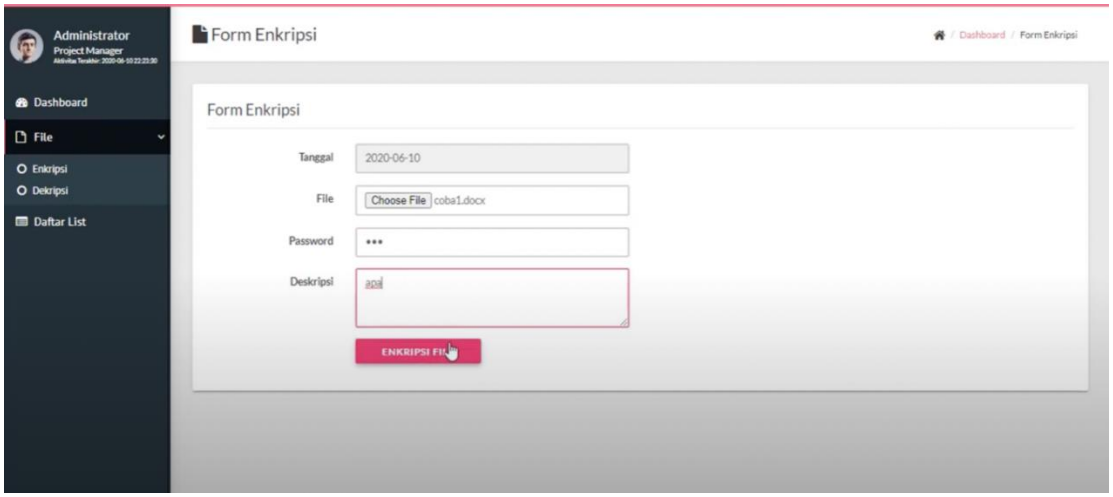
Pada tampilan ini akan menampilkan *browser file* dari penyimpanan internal untuk dilakukan keamanan data citra digital menerapkan *system Algoritma Advanced Encryption Standard*. Menu enkripsi terdapat *form form* yang dapat melakukan enkripsi data digital. Berikut ini isi dari menu enkripsi yang akan ditampilkan pada gambar 8 berikut ini :



Gambar 8. Menu Utama Input Enkripsi

4. Tampilan Input Enkripsi

Pada tampilan *input* enkripsi akan menampilkan *form input* enkripsi seperti *file*, *password* dan deskripsi. Berikut ini tampilan menu input data enkripsi seperti pada gambar 9 berikut ini:

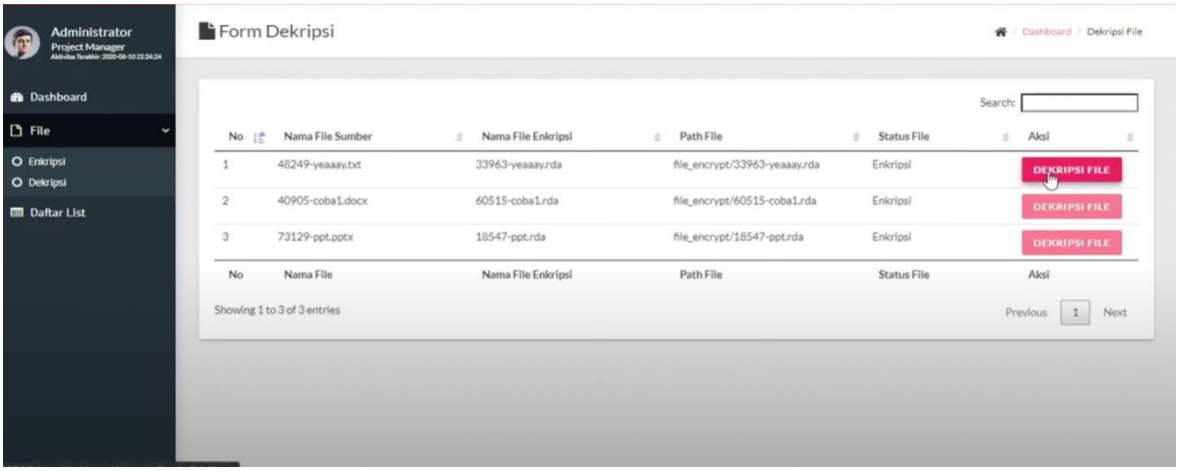


Gambar 9. Menu input data enkripsi

5. Tampilan daftar deskripsi

Pada tampilan ini akan menampilkan daftar data data citra digital yang sudah dilakukan enkripsi oleh algoritma AES. Berikut ini tampilan seperti pada gambar 10 berikut ini:

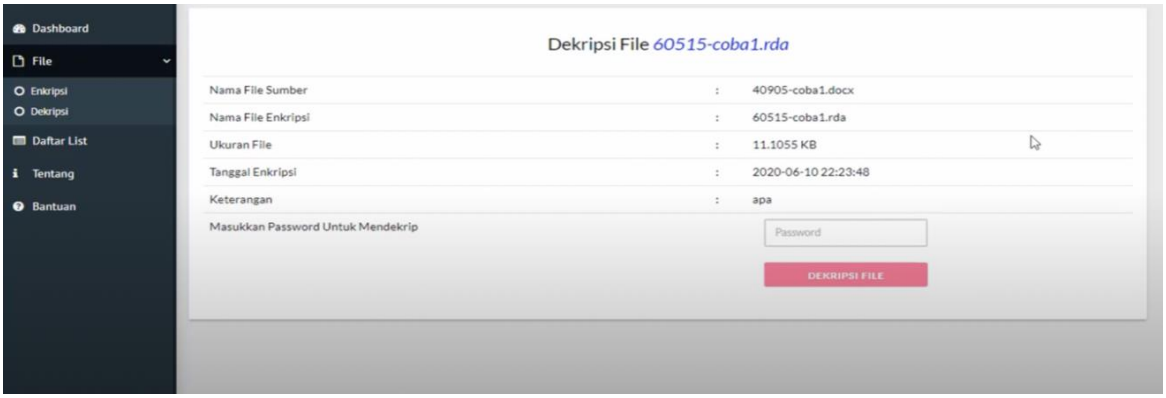
ISNN: 2964-1950



Gambar 10. Tampilan Menu daftar deskripsi

6. Tampilan Dekripsi File

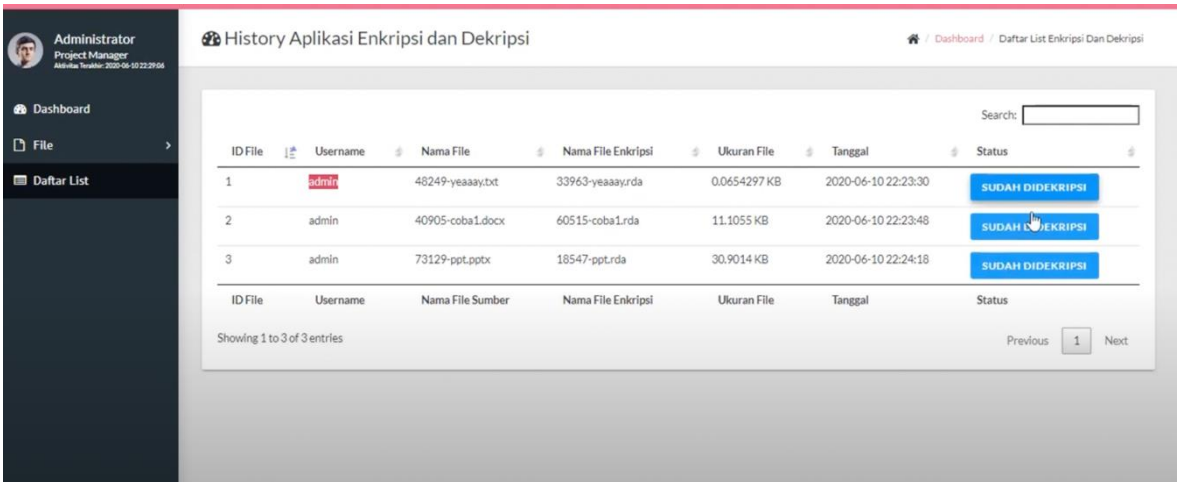
Pada tampilan dekripsi akan menampilkan data data dari dekripsi *file* yang berfungsi untuk melihat *file* data citra digital. Berikut ini tampilan menu dekripsi *file* seperti pada gambar 11 berikut ini:



Gambar 11. Tampilan Menu dekripsi file

7. Tampilan Menu Daftar File Dekripsi

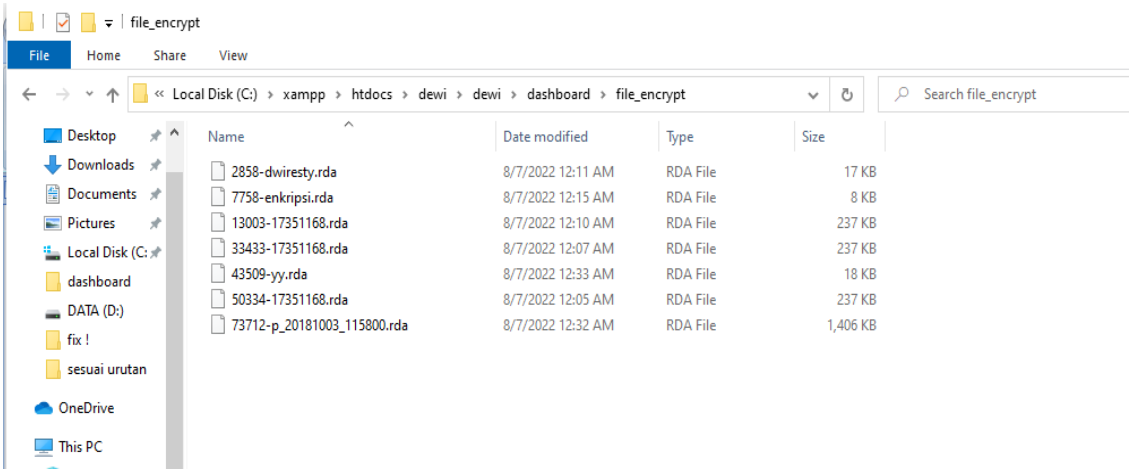
Pada tampilan menu daftar *file* yang sudah dilakukan dekripsi akan menampilkan keseluruhan data yang sudah dilakukan dekripsi. Berikut ini tampilan dekripsi seperti pada gambar 12 berikut ini:



Gambar 12. Tampilan Menu data dekripsi

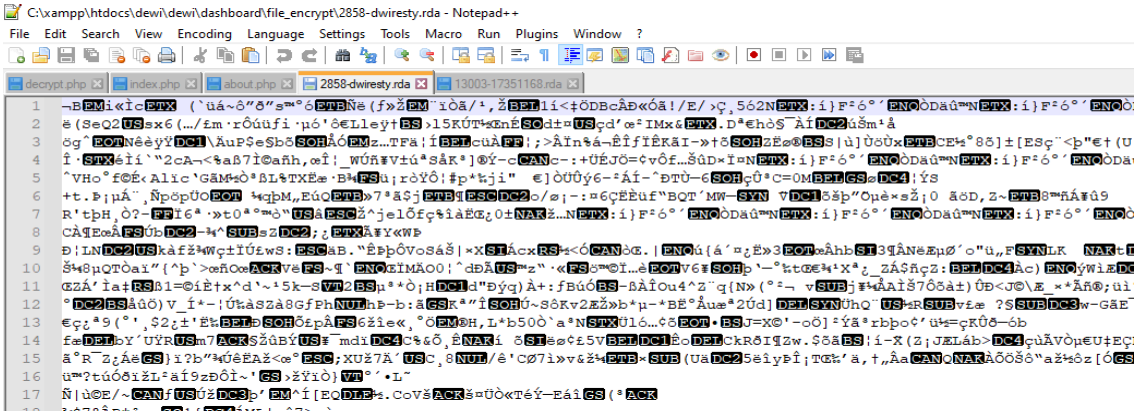
8 Tampilan Setelah Data Dienkripsi

Pada tampilan menu daftar file yang sudah dienkripsi. Berikut adalah tampilan data setelah dienkripsi :



Gambar 13 Tampilan Menu data dekripsi

9 Tampilan Data Terenkripsi



Gambar 14. Tampilan Data Terenkripsi

3.6 Pengujian Sistem

Pada tahap pengujian sistem, pembangunan sistem untuk mendukung system *Algoritma Advanced Encryption Standard* untuk pengamanan citra digital. Berdasarkan dari hasil studi kasus pada bab sebelumnya yang diuji menemukan kesalahan yang ada. Pengujian yang dilakukan bertujuan untuk mengetahui apakah Algoritma Advanced Encryption Standard untuk pengamanan citra digital yang dibangun telah sesuai yang diinginkan atau tidak.

3.6.1 Pengujian BlackBox

Pada tahap pengujian blackbox, pembangunan pembangunan system Algoritma Advanced Encryption Standard untuk pengamanan citra digital. Berikut ini adalah tahapan pengujian blackbox yang dimulai dengan rencana sesuai dengan pengujian pembangunan aplikasi dengan mendapatkan kasus dan hasil.

3.6.1.1 Rencana Pengujian

Rencana pengujian dilakukan dengan tujuan agar pengujian sistem dapat dilakukan dengan baik dan sesuai dengan tujuan pengujian blackbox, yaitu pengujian fungsional yang ada dalam pembangunan system Algoritma Advanced Encryption Standard untuk pengamanan citra digital. dapat dilihat pada tabel sebagai berikut:

Tabel 1. Rencana Pengujian

No	Komponen yang diuji	Skenario	Pengujian
1	Login	-Isi username -Isi password -Pilih tombol login -	Black Box
2	Halaman Input enkripsi	Isi key Isi plain teks	Black Box
3	Halaman dekripsi	Input password	Black Box

3.6.1.2 Kasus Dan Hasil Uji Data Benar pada Pengujian

Pada pengujian pembangunan system Algoritma Advanced Encryption Standard untuk pengamanan citra digital dan benar yang telah dilakukan dapat disimpulkan sebagai berikut:

Tabel 2 Hasil Pengujian

No	Data masukan	Hasil Yang diharapkan	Hasil Pengujian	Pengamatan
1	Isi username: Admin Isi password: admin	-masuk kehalaman utama	(√) Berhasil ( ) Gagal	Diterima
2	Isi username: Admin Isi password: A123	-login gagal, silahkan isi username kembali	() Berhasil (√) Gagal	diterima
3	Isi key Isi plain teks	Enkripsi	(√) Berhasil ( ) Gagal	Diterima
4	Isi key	enkripsi	() Berhasil (√) Gagal	Diterima
5	Input password	dekripsi	(√) Berhasil ( ) Gagal	diterima
6	password kosong	dekripsi	() Berhasil (√) Gagal	diterima

4. KESIMPULAN

Dalam uraian rangkaian mulai dari proses pembuatan system Algoritma Advanced Encryption Standard untuk pengamanan citra digital maka dapat ditarik beberapa kesimpulan penting antara lain:

1. Algoritma Sistem yang dapat dimanfaatkan untuk proses enkripsi dan dekripsi file dengan berbagai macam ukuran dan jenis file, menggunakan algoritma AES.
2. Ukuran file lampiran hasil enkripsi tidak dipengaruhi oleh format file lampiran, tetapi dipengaruhi oleh ukuran awal file lampiran. Semakin besar ukuran file dan semakin panjang kunci AES yang digunakan maka semakin besar ukuran file enkripsi yang dihasilkan.
3. Pada saat proses dekripsi maka memerlukan komputasi lebih banyak jika dibandingkan dengan proses enkripsi, sehingga kebutuhan waktu proses dekripsi menjadi lebih lama dibandingkan dengan proses enkripsi.

DAFTAR PUSTAKA

[1] N. I. Putri, R. Komalasari, and Z. Munawar, "Pentingnya Keamanan Data Dalam Intelijen Bisnis," *J. Sist. Inf.*, vol. 1, no. 2, pp. 41–49, 2020.

[2] S. Anwar, M. I. Komputer, and U. B. Luhur, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi Lsb Dan Algoritma Kriptografi Aes," *Semin. Nas. Teknol. Inf. dan Multimed. 2017,*

pp. 37–42, 2017.

[3] D. Darwis, R. Prabowo, and N. Hotimah, “Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, p. 389, 2018, doi: 10.25126/jtiik.201854727.

[4] D. Nurnaningsih and A. A. Permana, “Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes),” *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[5] A. M. Hasibuan, “Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone,” *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 1, pp. 29–35, 2017, doi: 10.54367/means.v2i1.20.

[6] A. F. Marisman and A. Hidayati, “Pembangungan Aplikasi Pembanding Kriptografi dengan Caesar Cipher dan Advance Ecryption Standard(AES) untuk File Teks,” *J. Penelit. Komun. dan Opini Publik*, vol. 19, no. 3, pp. 213–222, 2015.

[7] R. Rahmawati and D. Rahardjo, “Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi grafi AES 128 BIT pada SMK PGRI 15 Jakarta,” *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. April, pp. 67–74, 2016.

[8] V. Yuniati, G. Indriyanta, and A. Rachmat C., “Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File,” *J. Inform.*, vol. 5, no. 1, 2011, doi: 10.21460/inf.2009.51.69.

[9] Y. D. Setyaningrum, W. Wijanarto, and A. Rohmani, “Penerapan Algoritma AES pada Dokumen Penting Yang Disisipkan Dalam Citra Berbasis Algoritma LSB Dan Sobel,” *JOINS (Journal Inf. Syst.*, vol. 4, no. 2, pp. 178–189, 2019, doi: 10.33633/joins.v4i2.3099.

[10] I. Suryanto, C. Suhery, and Y. Brianorman, “Pengembangan Aplikasi Chat Messenger dengan Metode Advanced Encryption Standard (AES) pada Smartphone,” *J. Coding Sist. Komput. Untan*, vol. 03, no. 2, pp. 1–10, 2017.