HOAQ: JURNAL TEKNOLOGI INFORMASI, Volume 16 Nomor 1, Mei 2025, p59-67
p-ISSN: 2337-5280, e-ISSN: 26207427
DOI: https://doi.org/10.52972/hoaq.vol16no1

IMPLEMENTASI ALGORITMA *TRIPLE DES* UNTUK ENKRIPSI DAN DEKRIPSI GAMBAR DIGITAL DALAM FORMAT TEKS BERBASIS *WEBSITE*

Stefani Marlisa Us'Olin[1], Gregorius Fallo[2] , Andreas R. A. Djawa Ngoa[3]
[1,2,3]*Program Studi Teknologi Informasi, Universitas Timor*
Jl. El Tari , Kefamenanu – Nusa Tenggara Timur, Indonesia
Email: [1]stefanymarlisa03@gmail.com, [2]fallogege@gmail.com, [3]andreasngoa24@gmail.com

ABSTRAK

Keamanan data digital, khususnya gambar digital, menjadi aspek krusial dalam proses pertukaran informasi melalui jaringan internet. Penelitian ini bertujuan untuk merancang dan mengembangkan sebuah sistem berbasis web yang mengimplementasikan algoritma *Triple Data Encryption Standard (Triple DES)* dalam proses enkripsi dan dekripsi citra digital. Sebelum dilakukan proses kriptografi, citra digital terlebih dahulu dikonversi ke dalam format representasi teks menggunakan metode encoding *Base64*. Sistem dikembangkan menggunakan metode *Waterfall* serta teknologi *HTML*, *CSS*, *JavaScript*, dan pustaka *CryptoJS*. Hasil implementasi menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan tingkat keakuratan yang tinggi, selama kunci yang digunakan sesuai. Berdasarkan pengujian, sistem menunjukkan sensitivitas signifikan terhadap perubahan kunci dan terdapat peningkatan ukuran file akibat proses konversi. Selain itu, sistem telah diuji terhadap potensi serangan kriptografi umum dan dilengkapi mekanisme keamanan tambahan, seperti pembatasan percobaan kunci. Dengan demikian, sistem ini dapat dijadikan solusi efektif dalam menjaga kerahasiaan citra digital selama proses transmisi data secara daring.

Kata kunci: *Triple DES*, enkripsi gambar, dekripsi gambar, *Base64*, keamanan data, sistem berbasis web.

ABSTRACT

The security of digital data, particularly digital images, is a critical concern in the process of information exchange over internet-based networks. This study aims to design and develop a web-based system that implements the Triple Data Encryption Standard (Triple DES) algorithm for the encryption and decryption of digital images. Prior to the cryptographic process, the digital image is first converted into a text-based representation format using the Base64 encoding method. The system was developed using the Waterfall model along with HTML, CSS, JavaScript technologies, and the CryptoJS library. Implementation results indicate that the system can perform encryption and decryption processes with a high degree of accuracy, provided the correct key is used. Testing revealed that the system exhibits significant sensitivity to changes in the key, as well as an increase in file size due to the conversion process. Additionally, the system was evaluated against common cryptographic attacks and is equipped with enhanced security mechanisms, such as key input attempt limitations. Therefore, this system offers an effective solution for preserving the confidentiality of digital images during online data transmission.

Keywords: Triple DES, image encryption, image decryption, Base64, data security, web-based system

1. PENDAHULUAN

Di era digital saat ini, pertukaran data melalui internet telah menjadi hal yang umum di berbagai sektor. Pengguna dapat dengan mudah membagikan berbagai jenis informasi seperti dokumen, video, dan gambar digital. Namun, meskipun proses ini memberikan kemudahan dan efisiensi, terdapat risiko yang cukup besar terhadap keamanan data. Ancaman seperti penyadapan, pencurian, atau perubahan data oleh pihak yang tidak berwenang sering terjadi. Situasi ini berpotensi mengganggu kerahasiaan dan integritas informasi, terutama jika data yang dikirim bersifat pribadi atau rahasia[1].

Ancaman seperti pencurian data, penyalahgunaan informasi, dan tindakan peretasan merupakan isu yang signifikan dalam konteks keamanan informasi dan menuntut penanganan secara khusus serta sistematis. Tanpa adanya sistem perlindungan yang memadai, data berupa gambar digital yang dikirimkan melalui jaringan sangat rentan terhadap akses atau modifikasi oleh pihak yang tidak memiliki otorisasi. Kondisi tersebut dapat membahayakan aspek kerahasiaan dan integritas informasi yang dikandung dalam data tersebut [2]. Oleh karena itu, penerapan metode kriptografi dipandang sebagai salah satu pendekatan yang efektif untuk menjaga keamanan data digital, termasuk data dalam bentuk citra [3].

Kriptografi adalah bidang ilmu yang menitikberatkan pada perlindungan data melalui metode penyandian, dengan tujuan memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki wewenang atau

otorisasi. Dalam konteks ini, data yang belum melalui proses penyandian dikenal sebagai *plaintext*, sedangkan data yang telah mengalami proses penyandian disebut *ciphertext*. Proses konversi dari *plaintext* menjadi *ciphertext* disebut sebagai enkripsi (*encryption*), sementara proses untuk mengembalikan *ciphertext* ke bentuk aslinya disebut dekripsi (*decryption*) [4].

Salah satu algoritma kriptografi simetris yang umum digunakan adalah *Triple Data Encryption Standard (Triple DES)*. Algoritma ini merupakan pengembangan dari *Data Encryption Standard (DES)* dengan menerapkan proses enkripsi sebanyak tiga tahap, di mana masing-masing tahap menggunakan kunci yang berbeda untuk meningkatkan tingkat keamanan. Pendekatan ini dirancang untuk meningkatkan tingkat keamanan secara signifikan dibandingkan dengan *DES* konvensional. *Triple DES* beroperasi pada blok data berukuran 64-bit dan menggunakan panjang kunci efektif sebesar 168-bit, sehingga memberikan ketahanan yang lebih kuat terhadap serangan *brute force* [5].

Dalam upaya mengamankan citra digital, algoritma *Triple DES* dapat digunakan untuk mengenkripsi gambar yang sebelumnya telah diubah ke dalam format teks, seperti *Base64*, dengan menggunakan kunci rahasia. Proses dekripsi hanya dapat dilakukan secara tepat apabila menggunakan kunci yang identik dengan kunci yang dipakai pada saat proses enkripsi. Pendekatan ini berfungsi untuk mencegah akses oleh pihak yang tidak berwenang serta memastikan perlindungan terhadap integritas dan kerahasiaan data [6].

Meskipun algoritma *Triple DES* telah banyak diterapkan dalam pengamanan data berbasis teks maupun dokumen, penerapannya secara spesifik terhadap data citra digital berbasis web masih tergolong terbatas [7]. Mayoritas penelitian sebelumnya lebih memfokuskan kajian pada aspek kriptografi teks atau perlindungan dokumen, tanpa memberikan perhatian yang cukup terhadap pemanfaatan algoritma ini dalam pengamanan data visual berbentuk citra. Dengan demikian, masih terdapat peluang yang luas untuk mengembangkan suatu sistem yang mampu menjalankan proses enkripsi dan dekripsi terhadap citra digital secara daring, dengan memanfaatkan algoritma *Triple DES* sebagai mekanisme pengaman data [8].

Penelitian ini memberikan kontribusi dalam pengembangan solusi keamanan data digital, khususnya dalam konteks perlindungan citra digital, melalui implementasi algoritma *Triple DES* pada sistem berbasis web. Sistem yang dirancang memungkinkan pengguna untuk melakukan proses enkripsi terhadap gambar yang telah dikonversi ke dalam format teks (*Base64*), serta mendekripsinya kembali dengan menggunakan kunci yang identik guna merekonstruksi gambar ke bentuk aslinya. Selain itu, sistem dilengkapi dengan fitur untuk mengunduh hasil enkripsi dalam bentuk teks, yang dapat dimanfaatkan untuk pertukaran data secara aman. Berdasarkan hasil pengujian, sistem menunjukkan tingkat sensitivitas yang tinggi terhadap perbedaan kunci, yang mencerminkan tingkat keamanan yang kuat dalam mencegah akses tidak sah terhadap data.

Kebaruan dari penelitian ini terletak pada integrasi proses enkripsi citra digital ke dalam format teks dengan memanfaatkan algoritma *Triple DES* dalam sebuah platform berbasis web yang dapat diakses secara langsung tanpa memerlukan instalasi perangkat lunak tambahan. Selain itu, penelitian ini juga menyertakan pengujian sensitivitas kunci melalui berbagai uji coba langsung, yang merupakan aspek yang masih jarang dibahas secara mendetail dalam penelitian-penelitian terdahulu. Dengan demikian, sistem yang dikembangkan menawarkan solusi yang praktis sekaligus aman untuk menjaga kerahasiaan citra digital selama proses transmisi data secara daring.

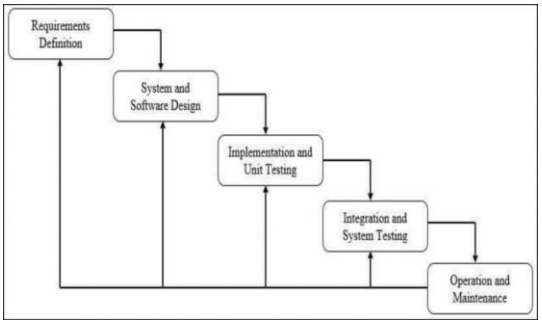
Penelitian ini memiliki tujuan untuk merancang serta mengembangkan sebuah sistem berbasis web yang mengaplikasikan algoritma Triple DES dalam proses enkripsi dan dekripsi pada citra digital. Melalui sistem ini, pengguna dapat meningkatkan tingkat keamanan data visual dengan cara mengonversi gambar ke dalam format teks (*Base64*), kemudian melakukan enkripsi menggunakan kunci rahasia, serta mendekripsinya kembali ke bentuk semula apabila kunci yang digunakan sesuai. Sistem yang dikembangkan diharapkan mampu menjadi solusi yang efektif dan andal dalam menjaga kerahasiaan citra digital, khususnya selama proses transmisi data melalui jaringan internet.

2. METODE PENELITIAN

Penelitian ini bertujuan untuk mengevaluasi kinerja sistem enkripsi dan dekripsi citra digital yang dikembangkan pada platform berbasis web. Pendekatan yang digunakan dalam penelitian ini adalah kuantitatif dengan metode eksperimental, yang mengintegrasikan dua aspek utama, yakni pengembangan perangkat lunak dan penerapan algoritma kriptografi *Triple DES* sebagai komponen utama dalam perancangan sistem yang diusulkan [8].

Metode Pengembangan Perangkat Lunak

Dalam penelitian ini, metode *Waterfall* digunakan sebagai kerangka kerja utama dalam pengembangan perangkat lunak. Model ini dipilih karena memiliki tahapan yang sistematis dan terstruktur, sehingga sesuai dengan karakteristik proyek yang telah memiliki kebutuhan sistem yang jelas dan terdefinisi sejak awal [9]. Model pengembangan sistem ditunjukkan pada Gambar 1.



Gambar 1. Model Waterfall

Metode Waterfall dalam pengembangan perangkat lunak meliputi sejumlah tahapan yang dilaksanakan secara berurutan, yaitu analisis kebutuhan (*requirement*), perancangan sistem (*system design*), pengkodean (*coding*), pengujian (*testing*), penerapan (*deployment*), dan pemeliharaan (*maintenance*) [10]. Berikut adalah uraian rinci dari setiap tahapan dalam metode *Waterfall*.

Tahap awal dalam pengembangan sistem adalah analisis kebutuhan, di mana permasalahan utama yang diidentifikasi adalah kurangnya tingkat keamanan dalam proses pertukaran gambar digital. Solusi yang diusulkan berupa pengembangan sistem kriptografi untuk melakukan enkripsi dan dekripsi gambar dengan memanfaatkan algoritma *Triple DES*.

Setelah kebutuhan sistem dianalisis, tahap berikutnya adalah desain sistem. Pada fase ini, penulis merancang struktur aplikasi yang akan dibangun, meliputi pembuatan *use case diagram*, desain antarmuka pengguna, serta diagram alir yang menggambarkan proses enkripsi dan dekripsi.

Pada tahap implementasi, pengembangan sistem dilaksanakan dengan menggunakan teknologi *HTML, CSS*, dan *JavaScript* untuk membangun antarmuka pengguna. Selain itu, pustaka *CryptoJS* dimanfaatkan untuk mengimplementasikan algoritma *Triple DES* dalam sistem. Proses dimulai dengan pengunggahan gambar oleh pengguna, yang kemudian dikonversi ke dalam format teks melalui encoding *Base64*. Selanjutnya, sistem meminta pengguna untuk memasukkan kunci rahasia yang akan digunakan sebagai parameter dalam proses enkripsi. Teks hasil konversi gambar dienkripsi menggunakan algoritma *Triple DES*, dan outputnya disimpan dalam bentuk *file* teks *(.txt)* yang dapat diunduh oleh pengguna.

Dalam proses dekripsi, pengguna harus mengunggah file teks yang merupakan hasil dari enkripsi serta memasukkan kunci yang identik dengan kunci yang digunakan saat proses enkripsi. Sistem kemudian akan mengubah data tersebut kembali ke bentuk gambar aslinya. Mekanisme ini dirancang untuk menjaga keamanan gambar dan memastikan bahwa hanya pihak yang memiliki kunci yang benar yang dapat mengakses informasi tersebut.

Setelah tahap pengembangan selesai, dilakukan proses pengujian untuk memastikan bahwa sistem beroperasi sesuai dengan kebutuhan fungsional yang telah ditentukan. Pengujian dilakukan menggunakan berbagai *file* gambar dengan variasi ukuran dan format yang berbeda, serta menggunakan beberapa variasi kunci enkripsi.

Tahap terakhir adalah pemeliharaan sistem, yang bertujuan untuk memastikan sistem tetap berfungsi dengan baik secara berkelanjutan serta menangani perbaikan jika ditemukan kesalahan (*bug*) atau jika dibutuhkan peningkatan dan pengembangan di kemudian hari.

Penelitian ini mengadopsi metode *Waterfall* karena dinilai paling sesuai untuk pengembangan sistem yang memiliki kebutuhan serta alur kerja yang telah terdefinisi secara jelas sejak tahap awal. Berbeda dengan pendekatan agile yang lebih tepat diterapkan pada pengembangan sistem yang bersifat dinamis dan fleksibel terhadap perubahan, metode *Waterfall* memungkinkan pencapaian hasil sistem yang lebih stabil, terstruktur, dan mudah diuji. Selain itu, pemilihan metode ini juga dimaksudkan untuk mengatasi keterbatasan dalam penelitian sebelumnya, yang belum mencakup pengujian sensitivitas kunci secara komprehensif dan belum menyediakan sistem kriptografi berbasis web yang dapat diakses dan digunakan secara langsung tanpa memerlukan instalasi tambahan.

Berbeda dengan penelitian terdahulu yang hanya berfokus pada pengujian fungsionalitas dasar algoritma kriptografi, penelitian ini mengembangkan pendekatan dengan menambahkan pengujian sensitivitas kunci secara menyeluruh serta membangun sistem yang dapat diakses dan digunakan langsung melalui platform web tanpa memerlukan instalasi tambahan. Pendekatan ini menjadikan implementasi sistem lebih praktis dan memberikan tingkat keamanan yang lebih tinggi dalam penerapan nyata.

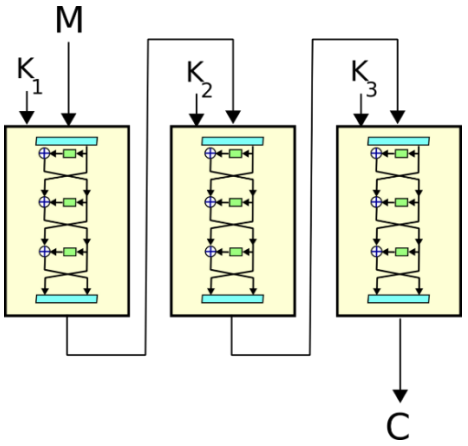
Metode Kriptografi *Triple DES*

Algoritma *Triple Data Encryption Standard (Triple DES)* merupakan pengembangan dari algoritma *Data Encryption Standard (DES)* yang bertujuan untuk meningkatkan keamanan pada kriptografi simetris. Berbeda dengan *DES* yang melakukan enkripsi satu kali menggunakan kunci sepanjang 56 bit, algoritma *Triple DES* menerapkan proses enkripsi sebanyak tiga kali secara berurutan dengan menggunakan tiga kunci berbeda, masing-masing berukuran 56 bit, sehingga menghasilkan total panjang kunci efektif sebesar 168 bit [7]. Dengan struktur tersebut, *Triple DES* dirancang untuk mengatasi kelemahan keamanan pada *DES*, khususnya yang berkaitan dengan kerentanan terhadap serangan *brute force*.

Algoritma *Triple DES* terdiri dari tiga tahap yang masing-masing mengimplementasikan algoritma DES secara berurutan, yaitu:

1. Tahap pertama, *plaintext* yang dimasukkan diproses menggunakan kunci pertama (K1) melalui algoritma *DES*, sehingga menghasilkan *ciphertext* awal.
2. Tahap kedua, *ciphertext* awal tersebut kemudian diproses dengan kunci kedua (K2). Pada tahap ini dilakukan proses dekripsi (atau enkripsi, tergantung pada mode operasi) menggunakan algoritma *DES*, sehingga menghasilkan *ciphertext* antara kedua.
3. Tahap ketiga, *ciphertext* antara kedua diproses menggunakan kunci ketiga (K3) melalui algoritma *DES* dengan proses enkripsi, sehingga menghasilkan *ciphertext* akhir (C) [5][11].

Ilustrasi dari proses enkripsi dan dekripsi menggunakan algoritma *Triple DES* ditunjukkan pada Gambar 2 berikut.



Gambar 2. Algoritma *3DES*

Pada pemilihan kunci ada tiga kunci yang digunakan dalam algoritma 3DES:

a. K1, K2, K3 adalah kunci yang bersifat saling bebas

K1 ≠ K2 dan K3 = K1

b. K1 dan K2 adalah kunci yang bersifat bebas, dan K3 sama K1

K1 ≠ K2 dan K3 = K1

Algoritma *3DES* sangat bergantung pada panjang kunci yang digunakan, sehingga dianggap lebih aman daripada algoritma *DES* [12].

```
// Enkripsi Triple DES
function tripleDESEncrypt(P, K1, K2, K3):
   Step1 = DES_Encrypt(P, K1)
   Step2 = DES_Decrypt(Step1, K2)
   C = DES_Encrypt(Step2, K3)
   return C

// Dekripsi Triple DES
function tripleDESDecrypt(C, K1, K2, K3):
   Step1 = DES_Decrypt(C, K3)
   Step2 = DES_Encrypt(Step1, K2)
   P = DES_Decrypt(Step2, K1)
   return P

// Jika hanya menggunakan dua kunci:
// K3 = K1
```

Dalam penelitian ini, algoritma *Triple DES* diimplementasikan untuk melakukan enkripsi terhadap gambar digital yang sebelumnya telah dikonversi ke dalam format teks (*Base64*) pada platform berbasis web. Hanya pengguna yang memiliki kunci enkripsi yang sesuai yang dapat melakukan proses dekripsi dan mengembalikan data ke bentuk gambar asli. Pendekatan ini menjadikan sistem sebagai solusi yang efektif dalam menjaga kerahasiaan gambar selama proses pertukaran data secara daring.

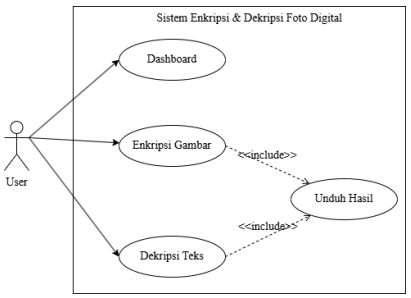
Rancangan Sistem Dan Alur Proses

Rancangan sistem ini bertujuan untuk menjelaskan bagaimana sistem bekerja dari segi fungsionalitas pengguna serta alur proses enkripsi dan dekripsi data gambar digital. Sistem yang dikembangkan merupakan aplikasi berbasis web yang memungkinkan pengguna untuk menerapkan algoritma *Triple DES* dalam proses enkripsi dan dekripsi gambar digital. Sebelum dienkripsi, gambar terlebih dahulu dikonversi ke dalam format teks

(*Base64*), kemudian dilakukan proses enkripsi guna menjaga kerahasiaan data. Proses dekripsi dilaksanakan untuk mengembalikan data terenkripsi ke bentuk gambar asli dengan menggunakan kunci yang sama.

1. Use case diagram

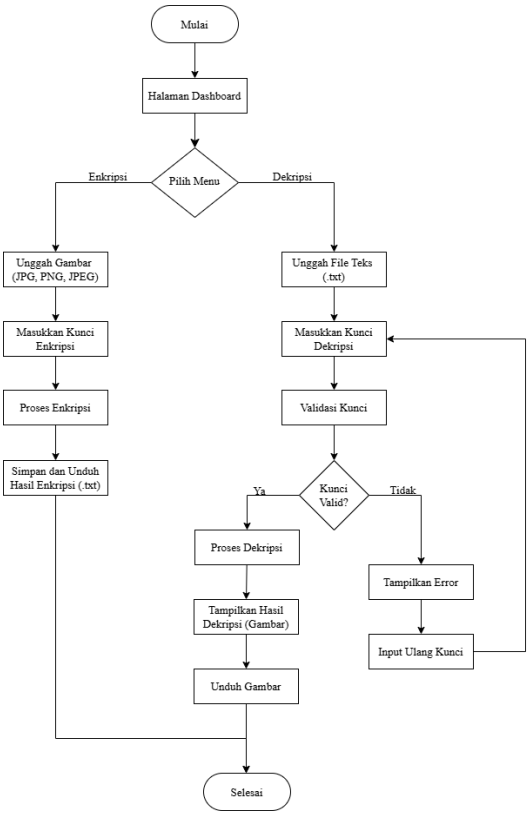
Use case diagram menggambarkan interaksi antara fitur-fitur sistem dengan pengguna sebagai aktor utama dalam sistem tersebut [8]. Pengguna memiliki akses penuh terhadap seluruh fitur yang tersedia dalam sistem, termasuk mengunggah gambar untuk proses enkripsi, melakukan enkripsi dengan memasukkan kunci rahasia, mengunduh hasil enkripsi dalam format file *.txt*, serta melakukan dekripsi terhadap file *.txt* tersebut untuk mengembalikan gambar ke bentuk aslinya. Gambaran lengkap mengenai interaksi antara pengguna dan sistem dapat dilihat pada Gambar 3 yang memperlihatkan *use case diagram* sistem.



Gambar 3. *Use Case Diagram*

2. *Flowchart* proses sistem

Flowchart digunakan untuk memvisualisasikan alur proses sistem secara menyeluruh, mulai dari tahap enkripsi hingga dekripsi. Diagram ini berfungsi untuk menggambarkan logika proses serta tahapan-tahapan yang dijalankan oleh pengguna maupun sistem. Alur kerja sistem secara rinci, mulai dari proses enkripsi hingga dekripsi, dapat dilihat pada *flowchart* yang disajikan dalam Gambar 4.



Gambar 4. *Flowchart* Diagram

3. HASIL DAN PEMBAHASAN

Setelah melewati tahapan pengembangan sistem menggunakan metode *Waterfall*, diperoleh hasil berupa aplikasi berbasis web yang mampu melakukan proses enkripsi dan dekripsi gambar digital dalam format teks dengan memanfaatkan algoritma *Triple DES*.

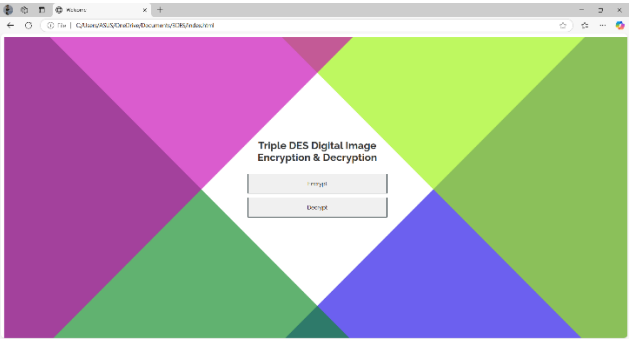
Implementasi Sistem

Sistem enkripsi dan dekripsi berbasis web telah berhasil dikembangkan dengan mengimplementasikan algoritma *Triple DES*. Implementasi ini memungkinkan pengguna untuk mengunggah gambar digital, mengonversinya ke format teks *Base64*, serta melakukan proses enkripsi dan dekripsi menggunakan kunci rahasia yang dimasukkan oleh pengguna. Selain itu, pengguna dapat mengunduh hasil enkripsi dalam bentuk file teks (*.txt*) dan mengembalikan file tersebut ke bentuk gambar asli melalui proses dekripsi.

Berikut ini dijelaskan secara rinci mengenai halaman-halaman yang terdapat pada sistem:

1. Tampilan *Dashboard*

Dashboard merupakan halaman utama yang muncul saat pengguna mengakses sistem. Pada halaman ini tersedia menu navigasi yang memudahkan pengguna dalam memilih fitur yang akan digunakan, yaitu menu Encrypt untuk mengenkripsi gambar menjadi format teks, serta menu Decrypt untuk mengembalikan teks terenkripsi menjadi gambar asli. Ilustrasi tampilan halaman *dashboard* dapat dilihat pada Gambar 5.



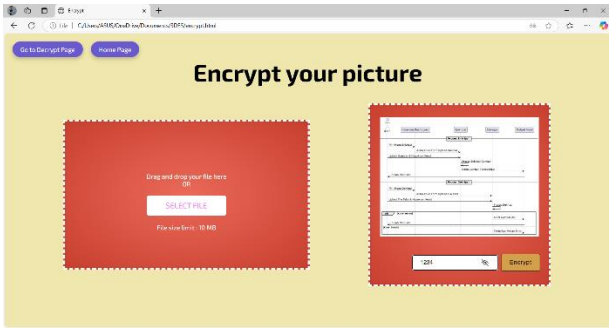
Gambar 5. Halaman *Dashboard*

2. Menu Encrypt

Proses enkripsi gambar dilaksanakan pada halaman ini melalui tahapan sebagai berikut:

1) Pengguna mengunggah gambar yang akan dienkripsi.
2) Sistem menampilkan kolom input untuk memasukkan kunci enkripsi, di mana pengguna wajib menginputkan kunci rahasia sebagai parameter enkripsi.
3) Setelah kunci dimasukkan, pengguna menekan tombol *Encrypt*, sehingga sistem melakukan proses enkripsi gambar menggunakan algoritma *Triple DES*.
4) Hasil enkripsi akan ditampilkan dalam bentuk teks terenkripsi dan dapat diunduh sebagai *file* berformat *.txt*.

Sistem ini dirancang untuk memastikan bahwa hanya pengguna yang memiliki kunci enkripsi yang benar dapat melakukan proses dekripsi dan mengembalikan gambar ke bentuk aslinya. Tampilan proses enkripsi dapat dilihat pada Gambar 6.



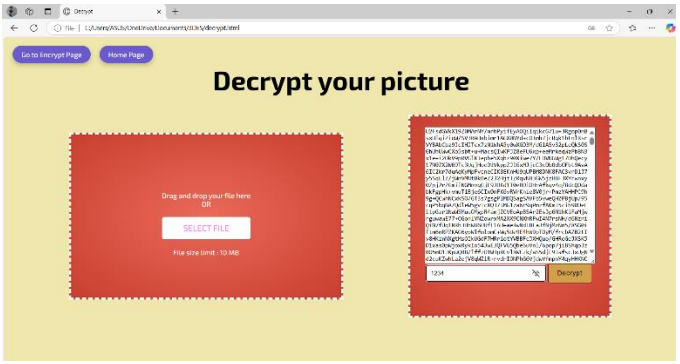
Gambar 6. Halaman Menu Enkripsi

3. Menu Decrypt

Pada halaman ini, pengguna dapat melakukan proses dekripsi terhadap file teks (*.txt*) yang sebelumnya telah dienkripsi, guna mengembalikannya ke format gambar asli. Proses dekripsi dilakukan melalui tahapan berikut:

1) Pengguna mengunggah file teks *(.txt)* hasil enkripsi sebelumnya.
2) Sistem meminta pengguna untuk memasukkan kunci enkripsi yang digunakan pada proses enkripsi.
3) Setelah kunci dimasukkan, pengguna menekan tombol Decrypt, kemudian sistem akan mengonversi teks terenkripsi tersebut kembali ke format gambar asli.
4) Gambar hasil dekripsi akan ditampilkan pada layar dan dapat diunduh dalam format gambar.

Sistem ini dirancang untuk memastikan bahwa proses dekripsi hanya dapat dilakukan apabila kunci yang digunakan sesuai, sehingga menjaga keamanan dan kerahasiaan data. Tampilan proses dekripsi dapat dilihat pada Gambar 7.



Gambar 7. Halaman Menu Dekripsi

Pengujian Sistem

Setelah sistem enkripsi dan dekripsi berbasis web berhasil diimplementasikan, dilakukan serangkaian pengujian guna memastikan fungsionalitas serta kinerja sistem berjalan sesuai dengan harapan[2].

Pengujian ini bertujuan untuk memverifikasi bahwa gambar yang telah dienkripsi dapat dikembalikan ke bentuk aslinya tanpa mengalami perubahan, selama kunci enkripsi yang digunakan tetap konsisten. Tahapan pengujian meliputi:

1) Mengunggah berbagai gambar dengan ukuran yang bervariasi untuk diuji dalam proses enkripsi.
2) Melakukan enkripsi gambar menggunakan algoritma *Triple DES* dengan penggunaan kunci yang berbeda-beda.
3) Melakukan dekripsi terhadap file teks hasil enkripsi guna memastikan bahwa gambar asli dapat dipulihkan secara utuh.

Tabel 1. Hasil Pengujian Enkripsi

Nama *File*	***Password***	**Ukuran *File***	**Waktu (ms)**	***Output***	**Keterangan**
Perpustakaan.JPG	1234	250KB	182 ms	encrypted_image.txt	Berhasil
Anggota.JPG	YOOLIN	502KB	230 ms	encrypted_image(1).txt	Berhasil
Photobooth.PNG	45532	410KB	195 ms	encrypted_image(2).txt	Berhasil
Enkripsi1.JPG	0000	2.176KB	600 ms	encrypted_image(3).txt	Berhasil
Dekripsi1.PNG	95733	750KB	430 ms	encrypted_image(4).txt	Berhasil

Tabel 2. Hasil Pengujian Dekripsi

Nama *File*	***Password***	**Ukuran *File***	**Waktu (ms)**	***Output***	**Keterangan**
encrypted_image.txt	1234	556KB	210 ms	Perpustakaan.JPEG	Berhasil
encrypted_image(1).txt	YOOLIN	1.069KB	260 ms	Anggota.JPEG	Berhasil
encrypted_image(2).txt	8996663	540KB	225 ms	-	Gagal
encrypted_image(3).txt	0000	3.181KB	300 ms	Enkripsi1.JPG	Berhasil
encrypted_image(4).txt	95733	943KB	245 ms	Dekripsi1.PNG	Berhasil

Analisis Pengujian:

Pengujian dilakukan pada lima *file* gambar dengan ukuran yang bervariasi menggunakan algoritma Triple DES. Hasil pengujian menunjukkan bahwa rata-rata waktu proses enkripsi mencapai 287,4 milidetik, dengan waktu tercepat sebesar 182 milidetik (pada file *Perpustakaan.JPG* berukuran 250 KB) dan waktu terlama sebesar 600 milidetik (pada file *Enkripsi1.JPG* berukuran 2.176 KB). Sedangkan pada proses dekripsi, rata-rata waktu yang diperlukan adalah 248 milidetik, dengan *waktu* tercepat 210 milidetik dan waktu terlama 300 milidetik.

Teramati adanya korelasi positif antara ukuran file dengan durasi proses enkripsi maupun dekripsi, di mana *file* dengan ukuran lebih besar memerlukan waktu pemrosesan yang lebih lama.

Dari segi ukuran file, konversi gambar ke format *Base64* menyebabkan peningkatan ukuran *file* secara signifikan. Sebagai contoh, *file Perpustakaan.JPG* meningkat dari 250 KB menjadi 556 KB (kenaikan sebesar 122,4%), dan file *Anggota.JPG* dari 502 KB menjadi 1.069 KB (kenaikan sebesar 112,9%). Secara rata-rata, peningkatan ukuran *file* setelah proses enkripsi dari kelima data uji mencapai 95,8%, yang menjadi pertimbangan penting terkait efisiensi penyimpanan data.

Pada proses dekripsi, tingkat keberhasilan mencapai 80%, dimana 4 dari 5 *file* berhasil dikembalikan ke bentuk asli dengan benar. Satu *file* gagal didekripsi akibat ketidaksesuaian *password*, yaitu *encrypted_image(2).txt*, yang menggunakan password "45532" saat enkripsi, namun mencoba didekripsi menggunakan *password* "8996663". Kejadian ini menegaskan bahwa sistem memiliki sensitivitas tinggi terhadap keakuratan kunci enkripsi, yang merupakan aspek krusial dalam menjaga keamanan sistem kriptografi.

Keamanan terhadap Serangan Kriptografi Umum

Sistem telah dievaluasi terhadap potensi serangan *brute force* dan *known plaintext attack* sebagai bagian dari upaya penguatan keamanan. Untuk mengantisipasi serangan *brute force*, sistem menerapkan pembatasan jumlah percobaan memasukkan kunci melalui mekanisme penundaan (*delay*) dan pemblokiran akses sementara setelah sejumlah input kunci yang gagal. Selain itu, proses enkripsi dilengkapi dengan penambahan komponen acak, seperti *Initialization Vector (IV)* atau *salt*, yang menghasilkan *ciphertext* berbeda meskipun *plaintext* dan kunci yang digunakan sama. Implementasi tersebut secara signifikan mengurangi risiko keberhasilan *known plaintext* attack serta meningkatkan ketahanan dan keamanan enkripsi secara menyeluruh.

Pemilihan algoritma *Triple DES* dalam penelitian ini didasarkan pada kesesuaian dengan kebutuhan sistem yang dikembangkan, meskipun secara umum *Advanced Encryption Standard (AES)* lebih efisien dan diakui sebagai standar kriptografi modern. *Triple DES* dipilih karena telah terbukti memiliki kehandalan dalam berbagai aplikasi industri serta didukung oleh pustaka implementasi yang stabil dan mudah digunakan pada lingkungan pengembangan web, seperti *CryptoJS*. Selain itu, algoritma ini lebih mudah diintegrasikan dan diujikan dalam konteks pengembangan prototipe sistem atau lingkungan pendidikan, di mana kebutuhan akan tingkat keamanan setara industri bukan merupakan prioritas utama. Sebaliknya, algoritma kriptografi asimetris seperti *RSA* kurang optimal untuk enkripsi data berukuran besar, seperti gambar digital, karena performanya yang relatif lebih lambat.

Dengan konfigurasi yang telah diperkuat serta penerapan langkah-langkah mitigasi terhadap potensi serangan, algoritma *Triple DES* tetap menjadi pilihan yang relevan untuk pengamanan gambar digital dalam sistem ini. Hal ini terutama berlaku sebagai solusi praktis dalam pengembangan sistem berbasis web yang mampu menyeimbangkan antara aspek keamanan dan kemudahan implementasi.

4. SIMPULAN

Berdasarkan hasil penelitian, telah berhasil dikembangkan sebuah sistem enkripsi dan dekripsi citra digital berbasis web dengan menggunakan algoritma *Triple DES*. Sistem ini memungkinkan konversi citra menjadi teks *(Base64)*, kemudian dilakukan proses enkripsi, dan selanjutnya dapat dikembalikan ke bentuk asli melalui proses dekripsi, selama kunci yang digunakan konsisten. Hasil pengujian menunjukkan bahwa sistem memiliki sensitivitas tinggi terhadap perubahan kunci, yang menunjukkan kapabilitas sistem dalam menjaga kerahasiaan data. Ditemukan pula bahwa durasi proses dan ukuran file meningkat seiring dengan besarnya ukuran citra yang diproses. Sistem ini juga telah dilengkapi dengan fitur pengamanan terhadap serangan *brute force* dan *known plaintext attack*, serta antarmuka yang ramah pengguna. Meskipun algoritma *Triple DES* bukan merupakan algoritma kriptografi paling mutakhir, pemanfaatannya dinilai tepat untuk pengembangan prototipe sistem berbasis web yang menekankan aspek kepraktisan dan kemudahan implementasi. Untuk pengembangan lebih lanjut, disarankan integrasi algoritma kriptografi yang lebih modern seperti *Advanced Encryption Standard (AES)* dan penambahan fitur otentikasi pengguna guna meningkatkan lapisan keamanan data.

DAFTAR PUSTAKA

[1] B. P. Pratama and W. Haryono, "Perancangan aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple DES Berbasis Web," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 4, pp. 204–212, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA/index

[2] H. A. Gunawan, Z. Arifin, and I. F. Astuti, "Keamanan Login Web Menggunakan Metode 3Des Berbasis Teknologi Quick Response Code," *J. Ilm. Ilmu Komput. Inform. Mulawarman*, vol. 9, no. 2, pp. 18–23, 2014, doi: 10.30872/jim.v9i2.126.

[3] R. Aulia and H. Dafitri, "Aplikasi Keamanan Dokumen Teks Menggunakan Algoritma Triple DES dan Blowfish," *Semin. Nas. Teknol. Inf. Komun. Pap.*, vol. 1, no. 1, pp. 346–354, 2022.

[4] M. A. Putra, D. I. Mulyana, R. A. Amalia, and M. Mirsandi, "Perancangan Aplikasi Enkripsi

& Deskripsi pada Dokumen dengan Algoritma Triple DES Berbasis Web," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 57–69, Feb. 2022, doi: 10.47709/jpsk.v2i01.1354.

[5] A. Nurhayati, F. Heryanti, and R. Hakim, "Perancangan Pengamanan Data Berbasis Teks Menggunakan Triple DES," *J. ICT*, vol. 2, no. 3, pp. 27–36, 2011.

[6] A. W. Mendrofa, N. B. Nugroho, and J. Halim, "Implementasi Keamanan Data Penjualan Produk Pada PT. Trans Sumatra Andalan Suzuki Menggunakan Metode Triple DES," *J. Cyber Tech*, no. x, 2021, doi: 10.53513/jct.v1i1.4478.

[7] M. A. Dinni, "Aplikasi Kriptografi File Citra Digital Menggunakan Algoritma Triple DES (Triple Data Encryption Standard)," Skripsi, Institut Teknologi Nasional Malang, Malang, Jawa Timur, Indonesia, 2012.

[8] M. Alda and M. I. Rifki, "Implementasi Metode Triple Des pada Aplikasi Keamanan Pesan Berbasis Mobile," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 7, no. 1, p. 17, 2022, doi: 10.31328/jointecs.v7i1.3281.

[9] S. De Beny and M. R. Yusuf, "Perancangan Website Laporan Data UMKM Provinsi Nusa Tenggara Timur Menggunakan Javascript dan Node.JS," *HOAQ (High Educ. Organ. Arch. Qual. J. Teknol. Inf.*, vol. 15, no. 1, pp. 43–50, May 2024, doi: 10.52972/hoaq.vol15no1.p43-50.

[10] Y. D. Serpiela, E. S. Bata, and T. A. Setyarini, "Layanan Informasi Berbasis Website di Desa Kaiwatu Maluku Barat Daya.," *HOAQ (High Educ. Organ. Arch. Qual. J. Teknol. Inf.*, vol. 13, no. 1, pp. 55–62, Feb. 2023, doi: 10.52972/hoaq.vol13no1.p55-62.

[11] L. Y. Sipayung and M. Purba, "Data Security Analysis with Triple DES Cryptographic Algorithm," vol. 6, no. 4, pp. 285–294, 2023, doi: 10.35335/idss.v6i4.198.

[12] Z. Basim and Painem, "Implementasi Kriptografi Algoritma Rc4 dan 3Des dan Steganografi dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop pada SMK As-Su'Udiyyah," *Skanika*, vol. 3, no. 4, pp. 54–60, 2020.