Laman web jurnal: https://ejournal.unama.ac.id/index.php/processor

Jurnal Processor

P-ISSN: 1907-6738 | E-ISSN: 2528-0082

Implementasi Metode Enkripsi dan Dekripsi Steganografi pada Gambar Digital dalam Aplikasi Berbasis WEB

Reyhan Mochamad Fabian[1*], Yosua Adriel Tamba [2], Muhammad Rifki Lathif[3], Muhammad Rafi Pasya Martadisastra[4], Salsabila Nida Azzahra[5], Deden Pradeka[6], Zahra Khaerunnisa[7]

[1234567]Program Studi Teknik Komputer, Kampus UPI di Cibiru, Universitas Pendidikan Indonesia, Jl. Pendidikan No.15, Cibiru Wetan, Kec. Cileunyi, Kabupaten Bandung, Jawa Barat 40625, Indonesia.
*Penulis Korespondensi, Email: yosuaadriel@upi.edu

Abstrak−Pengiriman dan penerimaan pesan melalui teknologi informasi sering menghadapi ancaman serangan siber yang berpotensi mengakibatkan modifikasi atau pencurian informasi sensitif, terutama dalam lingkungan perusahaan. Untuk mengatasi risiko tersebut, teknik kriptografi dan steganografi telah menjadi solusi efektif dalam melindungi data selama transmisi. Penelitian ini bertujuan untuk mengimplementasikan metode enkripsi dan dekripsi berbasis steganografi pada gambar digital melalui aplikasi berbasis web, dengan menggunakan pendekatan Least Significant Bit (LSB). Metode ini dirancang untuk menyembunyikan pesan rahasia dalam gambar tanpa mempengaruhi kualitas visualnya secara signifikan. Penelitian dilakukan menggunakan pendekatan kuantitatif dengan eksperimen yang bertujuan mengembangkan dan menguji perangkat lunak berbasis web. Hasil pengujian menunjukkan bahwa metode yang dikembangkan memiliki margin error sangat kecil, yaitu 0.000220, berdasarkan perhitungan *Mean Squared Error* (MSE). Selain itu, nilai *Peak Signal-to-Noise Ratio* (PSNR) sebesar 84.7 membuktikan bahwa kualitas gambar hasil steganografi sangat mendekati gambar aslinya. Temuan ini menunjukkan bahwa perangkat lunak yang dikembangkan tidak hanya efektif dalam menyembunyikan informasi, tetapi juga mampu menjaga kualitas visual gambar dengan sangat baik. Penelitian ini memberikan kontribusi signifikan terhadap pengembangan solusi keamanan data berbasis web, sekaligus menawarkan pendekatan praktis untuk melindungi informasi sensitif dalam era digital.

Kata Kunci: Enkripsi; Deskripsi; Steganografi; Gambar Digital; Aplikasi Web; Keamanan Data.

Abstract−The sending and receiving of messages through information technology often faces the threat of cyber-attacks that could potentially result in the modification or theft of sensitive information, especially in corporate environments. To address such risks, cryptography and steganography techniques have become effective solutions in protecting data during transmission. This research aims to implement a steganography-based encryption and decryption method on digital images through a web-based application, using the Least Significant Bit (LSB) approach. This method is designed to hide secret messages in images without significantly affecting their visual quality. The research was conducted using a quantitative approach with experiments aimed at developing and testing web-based software.The test results show that the developed method has a very small margin of error, which is 0.000220, based on the calculation of Mean Squared Error (MSE). In addition, the Peak Signal-to-Noise Ratio (PSNR) value of 84.7 proves that the quality of the steganography image is very close to the original image. These findings show that the developed software is not only effective in hiding information, but also able to maintain the visual quality of the image very well. This research makes a significant contribution to the development of web-based data security solutions, while offering a practical approach to protecting sensitive information in the digital age.

Keywords: Encryption; Decryption; Steganography; Digital Images; Web Applications; Data Security.

1. PENDAHULUAN

Dalam era globalisasi, perkembangan teknologi komunikasi berkembang dengan sangat cepat. Peran teknologi komunikasi memiliki dampak besar pada aktivitas sehari-hari seseorang, karena memudahkan dalam mendapatkan, mencari, dan berbagi informasi dengan orang lain [1]. Perkembangan teknologi saat ini telah melaju dengan sangat cepat, mempermudah individu untuk berbagi data dengan efisien [2]. Namun, semakin canggih teknologi komputer, semakin besar pula potensi ancaman terhadap keamanannya [3-5]. Ancaman ini semakin relevan seiring dengan meningkatnya risiko serangan siber yang menyasar proses komunikasi digital.

Penggunaan teknologi informasi dalam proses pengiriman dan penerimaan pesan memiliki risiko terhadap serangan siber. Para pelaku kejahatan sering memanfaatkan kelemahan sistem untuk menyusupi dan mengubah isi pesan tersebut [6-8]. Hal ini dapat mengakibatkan kerugian bagi pengguna, terutama jika pesan yang akan dikirim

https://doi.org/10.33998/processor.2026.21.1.2054

Submitted: 10 Januari 2025; Reviewed: 01 September 2025; Accepted; 29 November April 2025; Published: 30 April 2026

mengandung informasi yang tidak dipublikasikan, terutama bagi kalangan perusahaan [9]. Oleh karena itu, proses transmisi dan penerimaan data atau komunikasi menjadi rentan terhadap risiko keamanan [10]. Diperlukan sebuah sistem yang mampu melindungi informasi yang dikirim melalui jaringan internet.

Salah satu teknik yang diterapkan untuk melindungi keamanan data yaitu kriptografi dan steganografi [11]. Kriptografi merupakan teknik yang digunakan untuk mengirim pesan rahasia kepada penerima dengan metode merubah informasi menjadi format yang tidak bisa dimengerti oleh pihak ketiga atau individu dengan niat buruk, seperti peretas. Meskipun pihak ketiga dapat mengakses aliran data, pesan tetap terlindungi berkat sistem pengamanan yang digunakan [12]. Pada kriptografi, terdapat dua prinsip dasar, yaitu proses enkripsi dan proses dekripsi.

Enkripsi adalah teknik untuk melindungi data atau pesan yang akan dikirimkan dengan mengubah bentuk atau format aslinya menggunakan algoritma tertentu. Tujuannya adalah memastikan bahwa hanya pengirim dan penerima yang berwenang dapat memahami isi data atau pesan tersebut [13]. Sementara itu, dekripsi adalah proses yang berlawanan dengan enkripsi, yaitu mengembalikan bentuk pesan yang telah disamarkan menjadi informasi aslinya [14]. Dalam kriptografi, informasi yang dapat dipahami oleh manusia disebut sebagai *plaintext*, sedangkan informasi yang telah disamarkan dan tidak dapat dibaca disebut *ciphertext* [15]. Metode steganografi adalah metode untuk menyamarkan pesan atau informasi rahasia dalam sebuah media, seperti video, gambar, audio, teks atau lainnya, sehingga keberadaan pesan tersebut tidak terdeteksi [16]. Metode steganografi yang diterapkan dalam penelitian ini yaitu *Least Significant Bit* (LSB).

Penelitian steganografi oleh Sabrina menunjukkan bahwa aplikasi berbasis Android yang dirancang mampu menyembunyikan pesan rahasia dalam citra digital secara efektif. Pengujian ketahanan citra membuktikan bahwa pesan yang disisipkan dapat diekstrak dengan sempurna, bahkan setelah citra mengalami gangguan seperti cropping. Hasil ini menegaskan bahwa metode steganografi yang digunakan berhasil menjaga kerahasiaan pesan tanpa menarik perhatian pihak ketiga, sehingga aplikasi ini memberikan keamanan dalam pengolahan informasi dan mendukung komunikasi yang aman [17]. Penelitian steganografi oleh Wijayanti dan Romadlon menunjukkan bahwa aplikasi yang diuji berbasis citra digital. Metode *Least Significant Bit* untuk memasukkan pesan rahasia pada citra digital diimplementasikan menggunakan bahasa pemrograman *Python*. Pengujian dilakukan untuk membandingkan metode *Least Significant Bit, Most Significant Bit*, dan *Pixel Value Differencing*. Hasil penelitian mengungkapkan bahwa metode *Least Significant Bit* menghasilkan nilai *Peak Signal-to-Noise Ratio* dan *Structural Similarity Index* yang lebih tinggi serta nilai *Mean Squared Error* yang lebih rendah dibandingkan dengan metode *Most Significant Bit* dan *Pixel Value Differencing* [18].

Penelitian steganografi oleh Fattah menunjukkan bahwa aplikasi berbasis *Visual Basic* 2008. Pengujian dilakukan untuk memastikan keamanan dan kerahasiaan data dalam proses penyisipan pesan. Hasil ini menegaskan bahwa metode steganografi yang digunakan adalah algoritma Ezstego yang dikombinasikan dengan kriptografi Elgamal untuk menyisipkan pesan dalam image GIF [19]. Penelitian steganografi oleh Endar Nirmala mengungkapkan bahwa metode LSB yang diintegrasikan dengan algoritma kriptografi AES digunakan untuk memasukkan pesan teks ke dalam gambar digital berbasis Android. Hasil penelitian menunjukkan bahwa kombinasi metode ini efektif dalam menyembunyikan dan mengenkripsi pesan tanpa mengubah citra secara signifikan, sehingga perbedaan antara gambar sebelum dan sesudah penyisipan hampir tidak terlihat. Aplikasi yang dikembangkan dalam penelitian ini bernama "StegoKripto" yang dapat mengenkripsi pesan teks dan menyembunyikannya dalam gambar berformat .jpg dan .png, memberikan proteksi ganda untuk keamanan pesan rahasia dalam komunikasi bisnis. [20].

Penelitian steganografi oleh Gilbijatno dan Kasih menunjukkan bahwa aplikasi berbasis web. Pengujian dilakukan untuk menganalisis karakteristik metode *End of File*. Hasil ini menegaskan bahwa metode steganografi yang digunakan mampu menyembunyikan pesan teks dalam citra gambar tanpa mengubah secara signifikan tampilan citra tersebut [21]. Kelima penelitian menunjukkan bahwa metode steganografi seperti LSB dan Ezstego efektif dalam menyembunyikan pesan dalam citra digital tanpa merusak kualitas gambar. LSB memberikan hasil terbaik dalam kualitas citra, sementara berbagai platform seperti Android, Python, dan Web menunjukkan fleksibilitas aplikasi steganografi yang aman dan efektif.

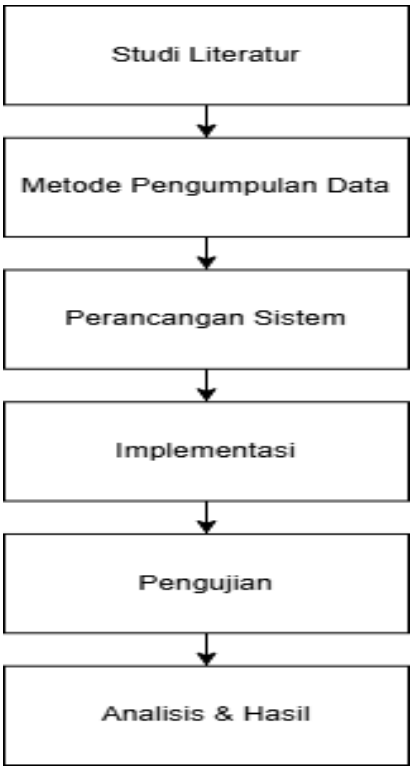
Tujuan dari penelitian ini adalah untuk mengimplementasikan metode enkripsi dan dekripsi kriptografi serta steganografi pada gambar digital dalam sebuah aplikasi berbasis web, dengan menggunakan metode *Least Significant Bit* (LSB) untuk menyembunyikan pesan rahasia dalam gambar tanpa mengubah kualitas gambar secara signifikan. Penelitian ini bertujuan untuk memastikan bahwa informasi yang dikirim melalui aplikasi tetap terlindungi dan terjaga kerahasiaannya, meskipun melalui media yang rentan terhadap serangan. Dengan demikian, diharapkan penelitian ini dapat memberikan dampak atau peran penting pada pengembangan teknologi keamanan data digital, khususnya dalam konteks pengiriman informasi yang aman melalui aplikasi berbasis web.

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini menggunakan pendekatan eksperimen berbasis kuantitatif untuk mengembangkan dan menguji metode enkripsi-dekripsi berbasis steganografi pada gambar yang diimplementasikan ke website. Penelitian ini dilaksanakan dengan mengikuti tahapan-tahapan sistematis seperti pada gambar berikut.



Gambar 1. Tahapan Penelitian

2.2 Studi Literatur

2.2.1 Citra Digital

Citra digital merupakan representasi visual elektronik yang dihasilkan dari konversi berbagai bentuk media seperti publikasi cetak, gambar fisik, atau konten multimedia audiovisual. Transformasi dari format analog ke digital ini disebut dengan istilah digitalisasi. Digitalisasi adalah teknik konversi yang mengubah informasi visual, tekstual, atau audio dari wujud fisik menjadi format data elektronik yang dapat disimpan secara digital [22].

2.2.2 Steganografi pada Gambar

Steganografi merupakan teknik komunikasi rahasia yang dirancang untuk menyamarkan informasi, dengan istilah yang berasal dari bahasa Yunani yang bermakna terselubung atau tidak terlihat (*covered*). Teknik ini berfungsi untuk menanamkan data ke dalam media pembawa lainnya, seperti file gambar atau dokumen elektronik, sehingga informasi tersebut tidak tampak oleh pihak yang tidak berkepentingan karena telah terkamuflase dalam wadah digital tertentu. Implementasi steganografi membutuhkan dua komponen utama pertama adalah berkas gambar original yang belum mengalami perubahan, disebut sebagai cover image, dan kedua adalah data rahasia yang akan disembunyikan, yang dapat berupa *plaintext*, *ciphertext*, file visual lain, atau berbagai jenis informasi digital yang mampu diintegrasikan ke dalam *bit-stream*. Hasil penggabungan antara *cover image* dan data tersembunyi menghasilkan *stego-image*. Selain itu, *stego-key* (kata sandi khusus) dapat dimanfaatkan dalam proses *decoding* untuk mengekstrak pesan yang terselubung. Berbagai format berkas yang lazim diaplikasikan dalam steganografi meliputi jpg, gif, bmp, wav, mp3, pdf, dan dokumen teks [23].

2.2.3 Least Significant Bit (LSB)

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

Implementasi penelitian ini menerapkan teknik Steganografi dengan menggunakan pendekatan Least Significant Bit (LSB). Pendekatan ini merupakan cara yang sederhana untuk menanamkan data atau informasi ke dalam file digital. Ketika media digital seperti gambar mengalami proses konversi yang membangun kembali pesan identik dengan versi aslinya (*lossless compression*) ke format JPEG yang bersifat *lossy compression*, kemudian apabila proses tersebut diulang akan merusak data yang tertanam dalam LSB. Dalam susunan binernya, terdapat bit dengan nilai paling signifikan yang dikenal sebagai *Most Significant Bit (MSB)* dan bit dengan nilai paling tidak signifikan *(LSB)* [23-25].

2.2.4 Peak Signal to Noise Ratio (PSNR) dan Mean Signal Error (MSE)

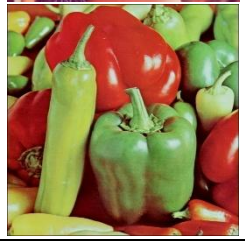
Kualitas pada gambar memiliki rumus untuk menentukan besar galat-nya, yaitu melalui rumus PSNR dan MSE. PSNR merupakan formula untuk mengetahui *noise* atau derau dari suatu citra. Nilai PSNR dependen berdasarkan MSE. Kedua rumus tersebut memiliki hubungan yang berbanding terbalik, semakin besar nilai MSE, maka akan semakin kecil nilai PSNR dan sebaliknya. Satuan dari PSNR adalah desibel atau umum dikenal dengan dB. Citra bisa dikatakan memiliki kualitas yang baik jika nilai PSNR-nya semakin besar, sebaliknya jika semakin kecil nilai PSNR, maka kualitas gambar yang dihasilkan bisa dikatakan buruk [26].

$$PSNR = 10\log_{10}(\frac{R^2}{MSE})$$

2.3 Metode Pengumpulan Data

Objek yang digunakan pada penelitian ini menggunakan tiga berkas citra dalam format Portable Network Graphics dengan ukuran dan resolusi yang dapat dilihat pada tabel 1.

Tabel 1. Sampel Berkas Citra

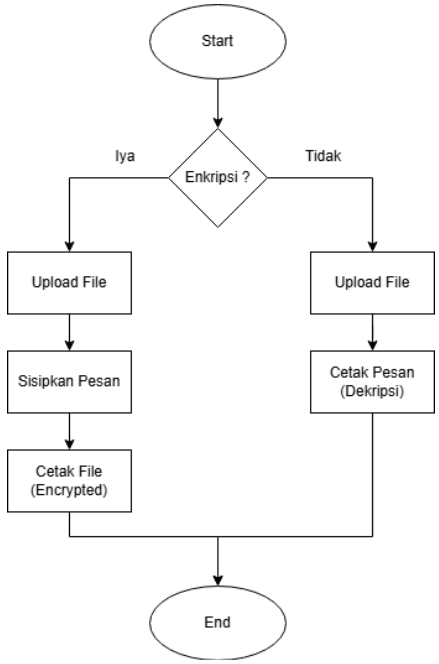
No	Jenis Gambar	Format Berkas	Resolusi
1		PNG	678 x 900
2		PNG	512x512
3		PNG	512x512

Ketiga sampel citra tersebut dipilih sebagai data uji untuk memvalidasi fungsionalitas aplikasi steganografi yang telah dikembangkan. Pemilihan sampel didasarkan pada variasi karakteristik visual yang berbeda, dimana Citra 1 menampilkan gambar landscape dengan gradasi warna natural dan tekstur rumput yang kompleks, Citra 2 berupa portrait manusia dengan area skin tone yang relatif smooth, dan Citra 3 menampilkan objek dengan kontras warna

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

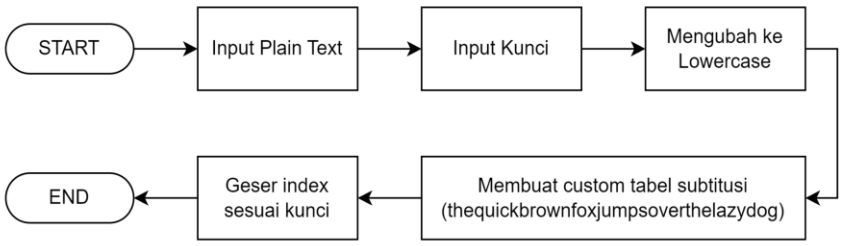
yang tinggi. Variasi ini bertujuan untuk menguji kemampuan aplikasi dalam melakukan proses embedding dan extraction pesan rahasia pada berbagai kondisi gambar dengan tingkat kompleksitas tekstur yang berbeda. Format PNG dipilih karena sifat *lossless compression* yang dapat mempertahankan integritas pixel secara utuh [27], sehingga proses penyembunyian dan pengambilan data rahasia dapat dilakukan dengan akurasi tinggi tanpa degradasi kualitas gambar. Penggunaan resolusi yang bervariasi juga dimaksudkan untuk mengevaluasi performa aplikasi pada file dengan ukuran berbeda, mulai dari resolusi tinggi (678x900) hingga resolusi standar (512x512), guna memastikan aplikasi dapat berfungsi optimal pada berbagai kondisi ukuran file gambar yang umum digunakan.

2.4 Perancangan Sistem



Gambar 3. Diagram Alir Program

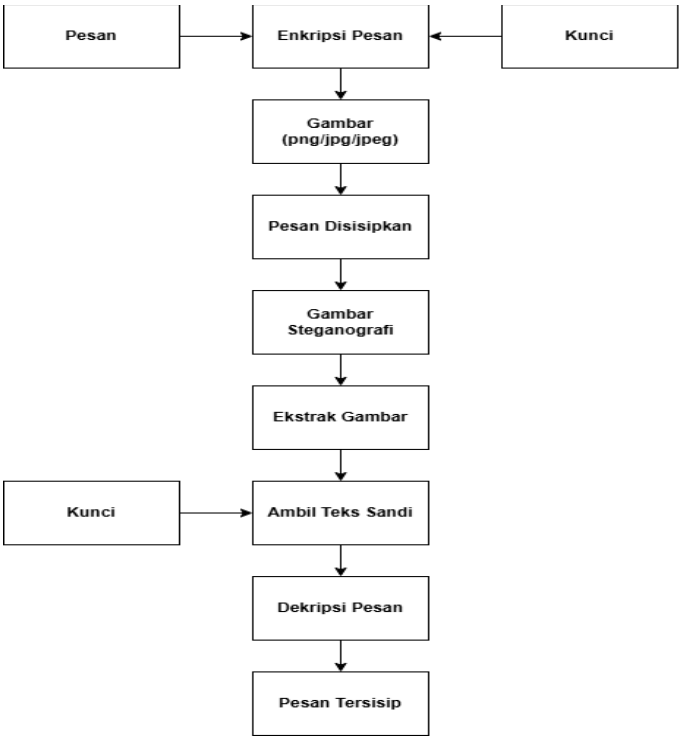
Pada aplikasi akan dirancang seperti pada gambar 3, dimana pengguna akan memilih salah satu dari dua fitur yaitu enkripsi atau dekripsi. Jika memilih dekripsi, maka pengguna dapat mengunggah file yang ingin disisipkan dan setelah itu file yang telah terenkripsi akan termuat dan dapat diunduh oleh pengguna. Sementara pada dekripsi, pengguna akan diminta untuk mengunggah berkas yang diduga tersisip pesan menggunakan metode Steganografi, setelah berkas terunggah pesan yang tersisip akan termuat.



Gambar 4. Diagram Alir Enkripsi Substitution Table

Pada enkripsi pesannya, pertama teks biasa yang diinput akan diubah semua ke *lowercase*. Hal tersebut karena pada ASCII, karakter dengan huruf *uppercase* dan *lowercase* memiliki nilai yang berbeda. Setelah itu teks yang diinput akan dilakukan *shifting* atau pergeseran sejauh ke kanan berdasarkan tabel substitusi yang dibuat yaitu (*thequickbrownfoxjumpsoverthelazydog*). Tabel tersebut digunakan sebagai basis pergeserannya. Setelah digeser, pesan akan diubah ke biner.

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026



Gambar 5. Diagram Proses Enkripsi Dekripsi Steganografi

Tahap enkripsi dimulai dengan menyisipkan pesan yang telah dienkripsi pada Gambar 4 ke dalam gambar dengan menggunakan *key* berupa pergeseran ke kanan sejauh lima. Setelah proses penyisipan selesai, gambar yang mengandung pesan tersebut akan dihasilkan sebagai output. Sementara pada tahap dekripsi, proses dimulai dengan mengambil gambar steganografi yang berisi pesan tersembunyi. Langkah pertama adalah mengekstrak gambar untuk memisahkan data utama. Selanjutnya, *ciphertext* (pesan terenkripsi) diambil dari gambar tersebut menggunakan *key* sebagai kunci akses. Setelah *ciphertext* diperoleh, proses dekripsi dilakukan untuk mengembalikan pesan ke bentuk aslinya. Akhirnya, pesan yang telah tersisip akan berhasil diekstrak dan siap untuk digunakan.

2.5 Implementasi

Pada penelitian ini, implementasi yang digunakan pada Steganografinya menggunakan LSB yang menggunakan tabel substitusi berisikan "*thequickbrownfoxjumpsoverthelazydog*", tabel substitusi tersebut dirancang untuk menghilangkan karakter duplikasi dan memberikan struktur alfabet unik yang digunakan dalam proses enkripsi dan dekripsi. Proses enkripsi dilakukan pergeseran (*shift)* sebanyak *key* pada indeks setiap karakter dalam tabel substitusi. Jika sebuah karakter didapat pada input, karakter tersebut akan digeser sejauh *key* indeks berdasarkan tabel substitusi yang digunakan sebagai basisnya. Misalnya, pada input terdapat karakter "t" maka karakter tersebut akan digeser sejauh *key* berdasarkan tabel substitusi akan menjadi karakter "i".

Sebaliknya, pada proses dekripsi, data biner diekstraksi dari piksel gambar, kemudian dikonversi kembali menjadi teks menggunakan tabel substitusi yang sama dengan perhitungan indeks yang telah dikurangi pergeseran (*shift*). Pendekatan ini memastikan bahwa pesan dapat dikembalikan ke bentuk aslinya dengan akurasi tinggi. Kombinasi antara tabel substitusi, metode shift, dan LSB memberikan tingkat keamanan tambahan dalam penyembunyian dan pengamanan pesan pada citra digital yang diimplementasikan melalui antarmuka berbasis web.

2.6 Pengujian

Pada gambar yang telah dilakukan penyisipan data menggunakan teknik Steganografi, akan dilakukan pengujian untuk mengevaluasi kualitas hasil penyisipan tersebut. Metode penghitungan yang digunakan pada penelitian ini adalah nilai PSNR (*Peak Signal-to-Noise Ratio*), yang bertujuan untuk mengukur tingkat gangguan atau derau yang terjadi akibat proses penyisipan data. Nilai PSNR yang dihasilkan akan dianalisis untuk menentukan apakah kualitas gambar yang dimodifikasi tetap memiliki kualitas yang baik atau mengalami penurunan kualitas yang drastis. Selain itu, pengujian juga dilakukan terhadap mekanisme pergeseran data yang diterapkan dalam aplikasi.

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

Proses ini bertujuan untuk memastikan bahwa data yang disisipkan telah bergeser sesuai dengan aturan yang ditetapkan, yaitu sejauh 5 posisi dalam *substitution table*, sehingga akurasi dan konsistensi dari algoritma yang digunakan dapat terjamin.

3. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan *file* gambar sebagai citra sampul dan teks pesan yang akan diamankan menggunakan teknik enkripsi *caesar cipher* untuk disisipkan kedalam *file* gambar tersebut menggunakan algoritma LSB (*Least Significant Bit*). Pada bagian ini, pengujian dilakukan menggunakan studi kasus yang dimana pengguna ingin menyisipkan pesan "bahaya" kedalam sebuah gambar yang di enkripsi menggunakan *Caesar Cipher* dengan *key* 5 dan *thequickbrownfoxjumpsoverthelazydog* yang digunakan sebagai tabel subtitusi.

Tabel 1. Tabel Substitusi

Alfabet	Index
t	0
h	1
e	2
q	3
u	4
i	5
c	6
k	7
b	8
r	9
o	10
w	11
n	12
f	13
x	14
j	15
m	16
p	17
s	18
v	19
l	20
a	21
z	22
y	23
d	24
g	25

3.1 Enkripsi Plaintext

Proses enkripsi *plaintext* akan dilakukan per huruf sampai didapatkan hasil berupa *ciphertext*. Berikut adalah proses enkripsi *plaintext* "bahaya" menggunakan *Caesar Cipher*.

A. Karakter pesan pertama = "b"

   b = 8 => 8 + 5 = 13 (f)

B. Karakter pesan kedua = "a"

   a = 21 => 21 + 5 = 26 mod (26) = 0 (t)

C. Karakter pesan ketiga = "h"

   h = 1 => 1 + 5 = 6 (c)

D. Karakter pesan kedua = "a"

   a = 21 => 21 + 5 = 26 mod (26) = 0 (t)

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

E. Karakter pesan kedua = “y”

y = 23 => 23 + 5 = 28 mod (26) = 2 (e)

F. Karakter pesan kedua = “a”

a = 21 => 21 + 5 = 26 mod (26) = 0 (t)

Setelah proses enkripsi menggunakan *Caesar Cipher*, didapatkan hasil enkripsi dari kata “bahaya” adalah “ftctet”. Selanjutnya, setiap karakter huruf dari hasil ini akan diubah dari pesan *cipher* ke biner. Berikut adalah proses pengubahan *ciphertext* ke dalam bentuk biner.

A. Karakter cipher pertama = “f”

“f” memiliki kode ASCII 102 => biner = 01100110

B. Karakter cipher kedua = “t”

“t” memiliki kode ASCII 116 => biner = 01110100

C. Karakter cipher ketiga = “c”

“c” memiliki kode ASCII 99 => biner = 01100011

D. Karakter cipher kedua = “t”

“t” memiliki kode ASCII 116 => biner = 01110100

E. Karakter cipher kedua = “e”

“e” memiliki kode ASCII 101 => biner = 01100101

F. Karakter cipher kedua = “t”

“t” memiliki kode ASCII 116 => biner = 01110100

Hasil pengubahan *cipher text* ke dalam bentuk biner adalah 01100110 01110100 01100011 01110100 01100101 01110100 dengan panjang 48 bit.

3.2 Penyisipan Pesan

Metode penyisipan pesan yang digunakan adalah metode LSB. Pada bagian ini, hasil dari enkripsi akan diubah jadi bilangan biner yang nantinya akan disisipkan kedalam file gambar. Sebelum menyisipkan pesan, piksel *file* gambar akan diubah kedalam bilangan biner terlebih dahulu yang nantinya LSB dari bilangan tersebut akan digantikan dengan bit pesan yang sudah di enkripsi. Sebagai contoh, pada kasus ini penyisipan pesan akan dilakukan pada lima piksel awal pada Gambar 4. Proses penyisipan pesan *ciphertext* kedalam *file* gambar dapat dilihat pada Tabel 2.

Tabel 2. Proses Penyisipan Bit-Pesan Ke Piksel Gambar

Nilai Piksel Gambar	**Konversi Dalam Biner**	**Bit Pesan**	**Hasil Penyisipan (Biner)**	**Hasil Penyisipan**
Piksel -1				
R = 166	10100110	0	10100110	R = 166
G = 125	1111101	1	1111100	G = 124
B = 112	1110000	1	1110001	B = 113
Piksel -2				
R = 166	10100110	0	10100110	R = 166
G = 125	1111101	0	1111100	G = 124
B = 112	1110000	1	1110001	B = 113

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

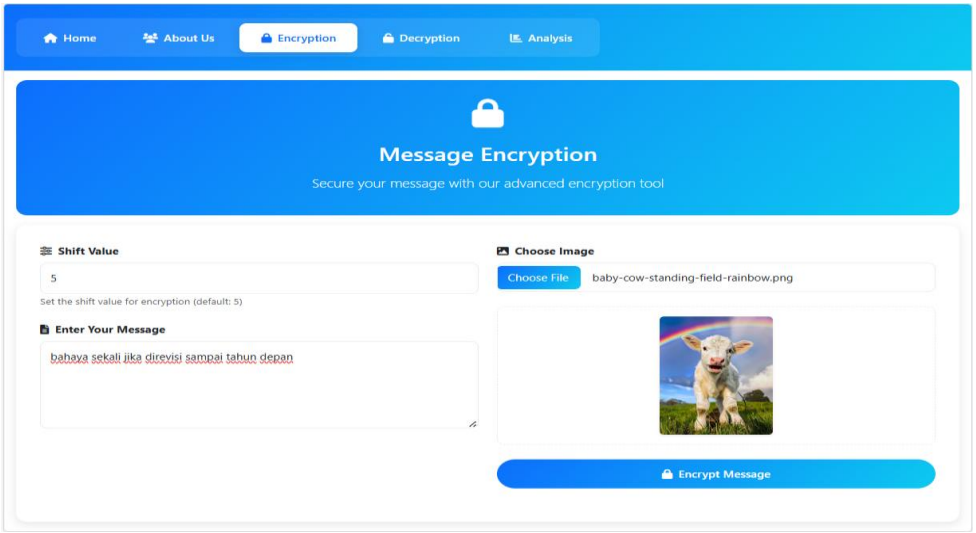
Piksel		-3						
R	=	160	10100000	1	10100001	R	=	161
G	=	134	10000110	0	10000110	G	=	134
B = 120			1111000	0	1111000	B = 120		
Piksel		-4						
R	=	160	10100000	1	10100001	R	=	161
G	=	134	10000110	1	10000111	G	=	135
B = 120			1111000	1	1111001	B = 121		
Piksel		-5						
R	=	160	10100000	0	10100000	R	=	160
G	=	134	10000110	1	10000111	G	=	135
B = 120			1111000	0	1111000	B = 120		

3.3 Implementasi Aplikasi

Pada tahap implementasi aplikasi, rancangan tahapan untuk proses enkripsi dan dekripsi *caesar cipher*, serta penyisipan hasil enkripsi ke dalam *file* gambar diimplementasikan pada perangkat lunak berbasis web yang halaman utamanya dapat dilihat pada Gambar 8.

Gambar 8. Halaman Utama Web

Dengan halaman untuk memulai proses enkripsi ditampilkan pada Gambar 6.

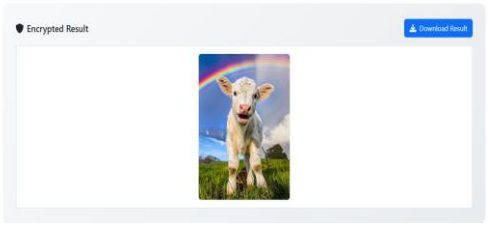


Gambar 9. Halaman Enkripsi Web

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

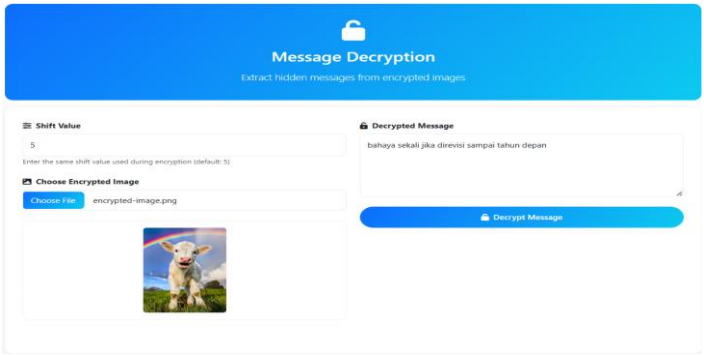
Pada halaman ini, proses enkripsi dan penyisipan pesan dapat dilakukan. Proses tersebut meliputi pengubahan format *file* gambar biasa menjadi *file* gambar yang berisi pesan berupa *ciphertext* yang disisipkan pada setiap piksel *file* gambar tersebut. Proses penyisipan pesan pada gambar dimulai dengan pengguna yang mengunggah sebuah gambar dan memasukan pesan yang ingin dienkripsi. Pesan ini kemudian akan dienkripsi menggunakan metode *caesar cipher* yang dimana setiap karakter dalam *plaintext* akan digeser sejumlah posisi tertentu (dalam kasus ini digeser sejauh 9 ke kanan) di tabel substitusi yang dapat dilihat pada Tabel 1.

Setelah pesan dienkripsi, *ciphertext* atau hasil dari enkripsi tersebut akan diubah kedalam bentuk biner yang kemudian pesan biner ini disisipkan ke dalam gambar yang diunggah menggunakan metode LSB (*Least Significant Bit*) dimana bit paling tidak signifikan dari setiap piksel gambar akan diubah berdasarkan bilangan biner hasil enkripsi. Setelah pesan berhasil disipkan, gambar yang memuat pesan dapat disimpan dan ditampilkan kembali pada pengguna. Proses enkripsi dan penyisipan pesan dapat dilihat pada Gambar 7, dimana pesan berhasil disisipkan ke dalam gambar tanpa mengubah penampilannya secara nyata.



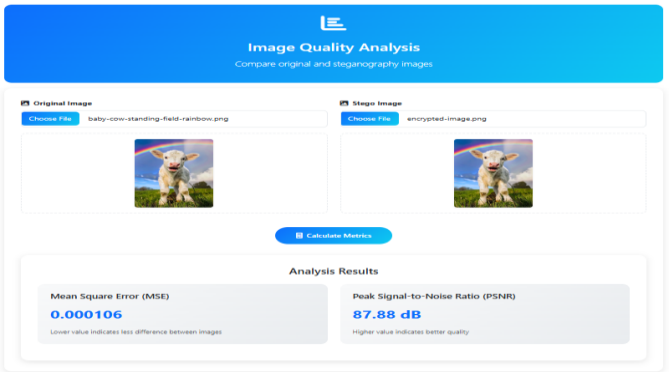
Gambar 10. Hasil Enkripsi

Selain proses enkripsi, proses dekripsi juga dapat dilakukan. Proses dekripsi dimulai dengan mengunggah *file* gambar yang memuat pesan yang telah dienkripsi. Proses ini kemudian dilanjutkan dengan pembacaan piksel-piksel gambar terutama pada bagian LSB dari setiap piksel warna yang telah berubah selama proses enkripsi. Bit-bit tersebut kemudian akan disusun kembali dan dikonversi menjadi *ciphertext*, lalu *ciphertext* tersebut akan didekripsi kembali menjadi *plaintext* dengan membalikan pergeseran yang diterapkan selama proses enkripsi. *Plaintext* ini kemudian akan ditampilkan seperti yang dapat dilihat pada Gambar 8.



Gambar 11. Hasil Dekripsi

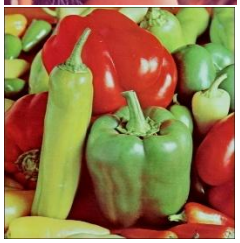
3.4 Pengujian Hasil



Gambar 12. Hasil Pengujian MSE & PSNR

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

Tabel 3. Hasil MSE dan PSNR

No	Jenis Gambar	Format Berkas	Format Berkas	Masukkan Teks	MSE (*Mean Squared Error)*	PSNR (Peak Signal-to-Noise Ration)
1		PNG	678 x 900	bahaya sekali jika direvisi sampai tahun depan	0.000106	87.88 dB
2		PNG	512x512	bahaya sekali jika direvisi sampai tahun depan	0.000256	84.06 dB
3		PNG	512x512	bahaya sekali jika direvisi sampai tahun depan	0.000237	84.39 dB

Berdasarkan hasil perhitungan MSE dan PSNR yang diperoleh, dapat diketahui bahwa hasil enkripsi memiliki margin error yang sangat kecil yakni sebesar 0.000106. Hal ini menunjukan bahwa pada proses steganografi, tingkat error yang dihasilkan sangat kecil atau tidak signifikan. Selain itu, nilai PSNR yang mencapai 87.88 dB menunjukan bahwa kualitas gambar hasil steganografi yang sangat baik dan mendekati kualitas gambar asli. Hasil ini menunjukan bahwa steganografi yang dibangun pada perangkat lunak ini dapat menyembunyikan informasi secara efektif dengan menjaga kualitas visual gambar di saat yang bersamaan. Namun, perlu diperhatikan bahwa algoritma kriptografi yang digunakan merupakan algoritma yang umum digunakan, Oleh karena itu, untuk potensi celah keamanan dapat memberikan keuntungan bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan penipuan [23].

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan metode enkripsi dan dekripsi berbasis steganografi pada gambar digital menggunakan teknik *Least Significant Bit* (LSB) dalam aplikasi berbasis web. Hasil penelitian menunjukkan bahwa metode ini efektif dalam melindungi data sensitif selama proses transmisi, dengan tetap mempertahankan kualitas visual gambar. Pengujian menggunakan parameter *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) menunjukkan bahwa tingkat *error* yang dihasilkan sangat kecil dan kualitas gambar setelah proses steganografi mendekati gambar aslinya. Hal ini membuktikan bahwa metode yang dikembangkan mampu menyembunyikan pesan dengan baik tanpa memberikan dampak signifikan pada kualitas gambar, sehingga dapat digunakan sebagai solusi untuk mengamankan data dalam berbagai aplikasi digital.

Penelitian ini menunjukkan bahwa metode yang dikembangkan dapat diterapkan pada gambar dengan resolusi bebas tanpa batasan tertentu. Uji coba telah dilakukan pada berbagai resolusi gambar, dan hasilnya menunjukkan konsistensi performa metode steganografi. Namun, terdapat keterbatasan pada ukuran file gambar yang dapat digunakan. Ukuran gambar yang terlalu besar tidak dapat diolah oleh sistem karena keterbatasan memori dan waktu proses. Oleh karena itu, aplikasi ini lebih optimal untuk diterapkan pada gambar dengan ukuran file yang moderat. Keterbatasan ini memberikan peluang bagi penelitian selanjutnya untuk meningkatkan efisiensi

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

pengolahan file berukuran besar, misalnya dengan optimasi algoritma atau penggunaan teknologi komputasi yang lebih kuat. Selain itu, pengembangan sistem yang mendukung berbagai format file dan kemampuan menangani ukuran file besar secara efektif dapat memperluas cakupan penerapan metode ini, sehingga lebih fleksibel dan sesuai untuk kebutuhan di berbagai konteks keamanan data digital.

REFERENCES

[1] C. A. Cholik, "Perkembangan Teknologi Informasi Komunikasi / ICT dalam Berbagai Bidang", Jurnal Fakultas Teknik UNISA Kuningan, vol. 2, no. 2, pp. 39–46, May. 2021.

[2] R. Pratiwi, L. C. Utami, R. B. Sakti, and N. Triase, "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher", Bulletin of Information Technology, vol. 3, no. 4, pp. 367–373, Dec. 2022.

[3] F. Alfiah, R. Sudarji, and D. T. Al Fatah, "Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake", ADI Bisnis Digital Interdisiplin Jurnal, vol. 1, no. 1, pp. 22–34, Jun. 2020.

[4] S. Zanero and V. Reding, *Security of Cyber-Physical Systems*. 2022. doi: 10.3390/books978-3-0365-4145-7.

[5] Data Hiding and Its Applications: Digital Watermarking and Steganography. (2022). MDPI eBooks. https://doi.org/10.3390/books978-3-0365-2937-0

[6] Digital Forensics and Watermarking: 21st International Workshop, IWDW 2022, Guilin, China, November 18-19, 2022, Revised Selected Papers. (2023). https://doi.org/10.1007/978-3-031-25115-3

[7] Disclosure of Software Supply Chain Risks. (2022). https://doi.org/10.7249/pea2072-1

[8] A. M. Pratama, Syaiful , and M. F. Rahman, "Keamanan Data dan Informasi". Kaizen Media Publishing, 2024.

[9] M. F. Bahari, "Analisa Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response", Jurnal Sains dan Teknologi Informasi, vol. 1, no. 2, pp. 49–53, March. 2022.

[10] Ismail and Muh. Syahrir, "Sistem keamanan pesan email menggunakan algoritma kriptografi klasik", Jurnal Ilmiah Sistem Informasi dan Teknik Informatika, vol. 4, no. 1, pp. 47–57, Apr. 2021.

[11] D. A. Akmal, D. M. Dhani, and F. Syahila, "Kombinasi Kriptografi Modern Dalam Keamanan Pesan Teks", Saturnus : Jurnal Teknologi dan Sistem Informasi, vol. 2, no. 3, pp. 119–128, Jul. 2024.

[12] A. Thahara and I. T. Siregar, "Implementasi Kriptografi untuk keamanan Data dan Jaringan menggunakan Algoritma DES", Jurnal Rekayasa Teknologi Informasi (JURTI), vol. 5, no. 1, p. 31, Jun. 2021.

[13] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," INVOTEK: Jurnal Inovasi Vokasional dan Teknologi, vol. 20, no. 1, pp. 27–36, Feb. 2020.

[14] N. A. Nanda, S. Maria, D. F. Nasution, M. Sari, and I. Gunawan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data", Jurnal Media Informatika, vol. 4, no. 2, pp. 90–93, Jun. 2023.

[15] Maulyanda , S. F. Pane, and R. M. Awangga, "Cryptography: Perancangan Middleware Web Service Encryptor menggunakan Triple Key MD5. Base64, dan AES," Jurnal Tekno Insentif, vol. 15, no. 2, pp. 65–75, Oct. 2021.

[16] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital," Voteteknika, vol. 11, no. 1, pp. 63–63, Mar. 2023.

[17] Fakhria Nur Sabrina, "Aplikasi Steganografi Pada Media Gambar Menggunakan Algoritma Least Significan Bit," Jurnal Tera, vol. 1, no. 2, pp. 185–201, Sept. 2021.

[18] D. E. Wijayanti and W. Romadlon, "Keamanan Pesan Menggunakan Kriptografi dan Steganografi Least Significant Bit pada File Citra Digital," Euler Jurnal Ilmiah Matematika Sains dan Teknologi, vol. 10, no. 2, pp. 181–192, Oct. 2022.

[19] M. A. Fattah, "Penerapan Steganografi Pada Image GIF Menggunakan Metode Ezstego dan Elgamal," TIN: Terapan Informatika Nusantara, vol. 1, no. 3, pp. 118–122, Aug. 2020.

[20] Nirmala, E. (2020). Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) Dan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Informatika Universitas Pamulang, 5(1), 36-47.

[21] A. A. Gilbijatno and P. Kasih, "Sistem Keamanan Data Teks dengan Steganografi Citra Gambar Menggunakan Algoritma End Of File," Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi), vol. 4, no. 3, pp. 197–204, Jul. 2020.

[22] Siregar, A. C., Poetro, B. S. W., Octariadi, B. C., Robet, R., & Sucipto, S. (2025). Buku Ajar Pengolahan Citra Digital. PT. Green Pustaka Indonesia.

[23] Reksiyano, R. D., & Andarsyah, R. (2025). Teknik Rahasia Menyembunyikan Gambar Keamanan Tingkat Tinggi dengan Steganografi. Penerbit Buku Pedia.

[24] Abdillah, M. O., Pane, O. A., & Lubis, F. R. A. (2023). Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB). Jurnal Sains Dan Teknologi (JSIT) Vol, 3(01).

[25] Adhimah, L. F., Nurhafiyah, I., Muntahar, A. A., Kristiaji, F., & Mustofa, D. (2023). Implementasi aplikasi steganografi berbasis web menggunakan algoritma LSB dan BPCS. KOMPUTA: Jurnal Ilmiah Komputer dan Informatika, Vol. 12, No. 2, Okt. 2023.

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026

[26] Pradeka, D., Adiwilaga, A., Agustini, D. A. R., Suheryadi, A., & Nuriman, R. (2023). Design and Build an Assessment Platform by Inserting Moodle-Based Cryptographic Methods. *Jurnal Nasional Teknologi dan Sistem Informasi*, *9*(3), 264–270. https://doi.org/10.25077/TEKNOSI.v9i3.2023. 264-270

[27] Maolana, A. (2024). Analisis Perbandingan Hasil Kompresi Citra Format PNG Dengan SVG Untuk Penyimpanan File Gambar. Dinamik, 29(1), 13-18.

https://doi.org/10.33998/processor.2026.21.1.2054
Submitted: 10 Januari 2025; Reviewed: 01 Septembere 2025; Accepted; 29 November 2025; Published: 30 April 2026