KETIK : Jurnal Informatika
ISSN: 3026-183X (Media Online)
Vol. 02, No. 06, Juli 2025 Hal. 15-23
Publisher: Faatuatua Media Karya
jurnal.faatuatua.com/index.php/KETIK
DOI: doi.org/10.70404/ketik.v2i04.305

Penerapan Keamanan Pesan Menggunakan Algoritma Triangle Chain Cipher Dan LSB ke Dalam Citra RGB

Frinto Tambunan[1*], Yudi[2], Ratna Sri Hayati[3]

[1]Bisnis Digital (Universitas Satya Terra Bhinneka), Indonesia, e-mail: frintoaja@gmail.com*
[2]Sistem Informasi (Universitas Potensi Utama), Indonesia, e-mail: yudimkom@gmail.com
[3]Bisnis Digital (Universitas Satya Terra Bhinneka), Indonesia, e-mail: ratnasrihayati@satyaterrabhinneka.ac.id
**coressponding author)*

Info Artikel

Diajukan: 14-Juli-2025
Diterima: 19-Juli 2025
Diterbitkan: 22-Juli-2025

Kata Kunci:
Sistem;
Kriptografi;
Steganografi;
Triangel Chain Chipper;
LSB.

Keywords:
System;
Cryptography;
Steganography;
Triangel Chain Chipper;
LSB.

Abstrak

Keamanan data saat ini adalah hal yang terpenting dalam sebuah sistem informasi. Memungkinkan munculnya suatu teknik-teknik yang baru yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Saat ini teknik yang digunakan untuk mengancam keamanan data selalu setingkat lebih maju dari pada teknik yang digunakan untuk mengamankan data. Karena itu timbul suatu gagasan yang dapat menimbulkan permasalahan tersebut, yakni untuk membuat suatu sistem keamanan yang mampu melindungi data yang dianggap penting dengan cara menyandikan data sehingga sulit untuk dideteksi oleh pihak yang tidak berhak. Dalam masalah keamanan, ilmu kriptografi sangat penting untuk dikembangkan dan diterapkan. Menggabungkan metode kriptografi dengan steganografi bertujuan untuk menghasilkan sebuah sistem keamanan yang lebih baik dibanding hanya menggunakan satu metode saja. Maka dari itu, dibuatlah sebuah aplikasi untuk mengamankan pesan yang bersifat rahasia untuk digunakan pada perangkat desktop. Algoritma Triangle Chain Cipher dengan algoritma LSB untuk menghasilkan tingkat kerahasiaan pesan yang lebih baik.

Abstract

Data security is currently the most important thing in an information system. Allows the emergence of new techniques that are misused by certain parties that threaten the security of the information system. Currently, the techniques used to threaten data security are always a step ahead of the techniques used to secure data. Because of that, an idea emerged that could cause this problem, namely to create a security system capable of protecting data deemed important by encoding the data so that it was difficult for unauthorized parties to detect it. In security issues, cryptography is very important to be developed and applied. Combining cryptographic methods with steganography aims to produce a security system that is better than using only one method. Therefore, an application was made to secure messages that are confidential for use on desktop devices. Triangle Chain Cipher algorithm with LSB algorithm to produce a better level of message confidentiality.

1. PENDAHULUAN

Seiring majunya Perkembangan Teknologi, untuk saat ini telah banyak teknik yang dilakukan untuk menjaga keamanan pesan yang dirahasiakan. Maka dari itu ilmu kriptografi dan steganografi sangat penting untuk dikembangkan dan diterapkan pada aplikasi keamanan pesan. Kriptografi yaitu mengubah pesan menjadi sesuatu yang tidak bisa dibaca. Sedangkan steganografi adalah penyisipan pesan rahasia dalam suatu file.

Kriptografi berasal dari kata Yunani "krypto," yang berarti tersembunyi, dan "graphein," yang berarti menulis. Secara harfiah, kriptografi adalah seni atau ilmu menyembunyikan informasi melalui berbagai teknik penyandian[1]. Tujuan utamanya adalah menjaga kerahasiaan pesan sehingga hanya

pihak yang berhak dapat membacanya, sementara pihak yang tidak berwenang tidak dapat mengakses atau memahaminya.

Dalam *era digital*, ketika informasi dapat dengan mudah dipindahkan dan diakses secara elektronik, penting untuk memiliki metode kriptografi yang kuat dan dapat diandalkan. Kriptografi tidak hanya menjadi alat pertahanan terhadap serangan dan ancaman siber, tetapi juga mendukung kepercayaan dan keandalan di tengah-tengah masyarakat yang semakin bergantung pada teknologi informasi[2].

Steganografi merupakan seni atau ilmu menyembunyikan informasi rahasia dalam suatu medium yang tampaknya biasa, sehingga orang yang tidak berwenang tidak dapat menyadari keberadaan informasi tersebut[3]. Berbeda dengan kriptografi yang fokus pada penyandian informasi, steganografi bertujuan untuk menyembunyikan keberadaan pesan itu sendiri.

Dalam konteks steganografi digital, media yang umumnya digunakan adalah gambar, audio, atau video. Teknik ini dapat diterapkan dalam berbagai bidang, termasuk keamanan data, hak cipta, dan keamanan komunikasi. Dengan menggunakan steganografi, pesan rahasia dapat disembunyikan di dalam file multimedia sehingga tidak terlihat oleh mata manusia atau alat deteksi biasa[4].

Menyandikan pesan merujuk pada proses mengubah teks atau data menjadi bentuk yang sulit dipahami tanpa pengetahuan kunci atau algoritma yang benar. Tujuan utama dari penyandian pesan adalah untuk mencegah akses tidak sah dan pemahaman oleh pihak yang tidak berhak. Dengan menyandikan pesan, informasi yang dikirim atau disimpan dapat dijaga kerahasiaannya, bahkan jika jatuh ke tangan pihak yang tidak diinginkan[5].

Ada beberapa alasan mengapa perlunya menyandikan pesan. Pertama, kerahasiaan pesan memainkan peran sentral dalam melindungi privasi individu, bisnis, dan entitas lainnya. Data pribadi, informasi bisnis, dan rahasia industri harus tetap aman dari mata yang tidak berhak melihatnya. Tanpa lapisan keamanan yang tepat, informasi tersebut dapat dieksploitasi dan disalahgunakan.

Kedua, menyandikan pesan penting untuk menjaga integritas data. Dengan mencegah perubahan atau manipulasi yang tidak sah, penyandian memastikan bahwa informasi yang diterima atau disimpan tetap sesuai dengan yang asli. Ini menjadi krusial dalam mencegah serangan seperti perusakan data atau perubahan informasi yang dapat merugikan keputusan bisnis atau kepercayaan publik.

Terakhir, menyandikan pesan juga diperlukan untuk memastikan keaslian dan otentikasi informasi. Dalam dunia yang terhubung secara global, kemungkinan ancaman identitas dan pemalsuan informasi semakin meningkat. Dengan menggunakan teknik penyandian yang tepat, dapat dihindari risiko identitas palsu dan keaslian pesan dapat dipertahankan.

Pada penelitian ini algoritma kriptografi dan algoritma steganografi yang akan digunakan untuk mengamankan sebuah pesan rahasia adalah algoritma *Triangle Chain Cipher* dengan algoritma *Least Significant Beast* (LSB). Dimana Triangle Chain Cipher adalah merupakan cipher yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara random dan panjang kunci sepanjang plainteks yang akan dienkripsi[6]. Tetapi pada algoritma kriptografi rantai segitiga pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai. Sedangkan algoritma LSB merupakan penyembunyian pesan yang dilakukan mengganti bit-bit data yang kurang berarti dalam segmen citra dengan bit-bit rahasia pada bit terakhir[7].

2. METODE PENELITIAN

Pentingnya keamanan informasi dalam dunia digital mendorong pengembangan metode-metode yang efektif untuk melindungi dan menyembunyikan data sensitif. Dua pendekatan utama yang banyak digunakan dalam konteks ini adalah steganografi dan kriptografi. Metode penelitian yang diterapkan dalam steganografi dan kriptografi menjadi kunci untuk mengembangkan teknik-teknik yang lebih kuat dan efisien dalam melindungi informasi.

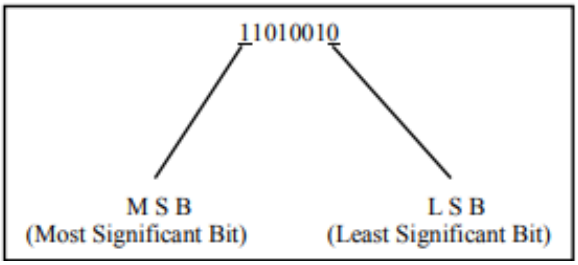
Steganografi, sebagai seni menyembunyikan informasi di dalam medium yang tampaknya biasa, telah berkembang pesat seiring dengan kemajuan teknologi[8]. Penyembunyian pesan dalam gambar, audio, atau video menjadi semakin kompleks, melibatkan berbagai teknik seperti *least significant bit* (LSB) *hiding*, *transform domain techniques*, dan metode-metode inovatif lainnya. Metode penelitian dalam steganografi tidak hanya berfokus pada penemuan cara baru untuk menyembunyikan informasi, tetapi juga pada upaya memahami kelemahan teknik-teknik yang ada dan mengembangkan cara untuk mendeteksinya. Penelitian ini esensial dalam meningkatkan daya tahan steganografi terhadap serangan dan pengembangan solusi perlindungan yang lebih baik.

Kriptografi berkaitan erat dengan penyandian pesan untuk melindungi kerahasiaan, integritas, dan otentikasi data. Metode penelitian dalam kriptografi melibatkan pengembangan algoritma enkripsi yang tangguh, studi keamanan komputasi kuantum, dan eksplorasi konsep baru seperti homomorphic encryption[9]. Penelitian ini tidak hanya mengejar penciptaan metode penyandian yang kuat, tetapi juga

menangani tantangan keamanan yang berkembang, termasuk serangan komputasi kuantum yang dapat mengancam kriptografi konvensional[10].

2.1 Metode LSB (Least Significant Bit)

Least Significant Bit adalah salah satu metode untuk menyembunyikan pesan dalam media digital dengan cara menyisipkan pesan tersebut pada satu bit paling kanan ke pixel file obyek(Yusfrizal, 2019). Metode yang paling sering digunakan adalah dengan modifikasi LSB (Least Significant Bit) pada citra penampung. Pada susunan bit didalam sebuah byte, ada bit yang paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang significant atau LSB[11].



Gambar 1. Sampel Susunan Bit pada LSB dan MSB

Sebuah citra adalah kumpulan dari titik-titik yang disebut pixel. Pada citra warna 24 bit, setiap pixel berukuran 3 Byte dimana setiap byte mewakili warna dari setiap komponen Red, Green, dan Blue. Misalkan terdapat 2 pixel, dimana nilai intensitas setiap warna pada setiap pixel setelah dikonversikan kedalam biner memberikan nilai biner sebagai berikut :

(00100111 11101001 11001000)
(00100111 11001000 11101001)

Untuk menyisipkan sebuah karakter “C” dengan bilangan biner 01000011 (kode ASCII 67) kedalam 2 pixel citra warna tersebut. Setiap 2 byte dari pesan yang dimulai dari MSB disisipkan dalam 2 bit LSB setiap byte citra warna. Hasil penyisipannya memberikan nilai pixel baru sebagai berikut

(00100101 11101000 11001000)
(00100111 11001000 11101001)

2.2 Metode Triangle Chiper

Algoritma kriptografi triangle chain atau umumnya dikenal dengan sebutan rantai segitiga merupakan cipher yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara random dan panjang kunci sepanjang plainteks yang akan dienkripsi. Tetapi pada algoritma kriptogarfi rantai segitiga pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai[12].
Proses enkripsi dilakukan dua kali dalam pola matrix segitiga pertama dan segitiga kedua.

1. Matriks Enkripsi Segitiga PertamaBaris Ke-1:
   M [1j] = P[j] + (K * R[1]) Mod 256
   Baris ke-2 dan seterusnya untuk nilai j≥ i :
   M [i j] = M [i-1], j + (K * R[i]) Mod 256

Sehingga nilai ciphertextyang diperoleh dengan M [i j] pada nilai j = (N+i) –N2.

2. Matriks Enkripsi Segitiga Keduauntuk Baris Ke-1 :
   M[1j] = P[j] + (K * R[1]) Mod 256
   untuk baris ke-2 dan seterusnya untuk nilaij≤ (N+1)-i :
   M [i j] = M [i-1], j + (K * R[i]) Mod 256

Sehingga nilai ciphertextyang diperoleh dengan M [i j] = [(N+1) –i, j]

Proses dekirpsi dilakukan dengan pola segitiga terbalik dengan proses enkripsi.

1. Matriks dekripsi segitiga pertamauntuk baris ke-1:
   M1j = C [j] –(K * (R[1])) Mod 256
   untuk baris ke-2:j ≤ (N+1) –i
   M[ij] = M[i-1], j –(K * (R[i])) Mod 256

Sehingga nilai plaintextdiperoleh dengan M [ij] = [(n+1)-i, i]

2. Matriks dekripsi segitiga keduauntuk baris ke-1:
   M1j = C [j] –(K* (R[1])) Mod 256
   untuk baris ke-2, nilai j ≥ i

M[ij] = C[i-1], j –(K * (R[i])) Mod 256

Sehingga nilai plaintext diperoleh dengan M[ij] pada nilai j = [i, (n+i)-N].

Keterangan :

P = Plainteks
N = Jumlah karakter plainteks
M = Matriks Penampung hasil penyandian
K = Kunci
R = Row (baris perkalian faktor pengali dengan kunci)
i = Indeks faktor pengali
j = Indeks karakter plainteks

3. HASIL DAN ANALISIS

3.1 Pembahasan

Studi kasus perhitungan menggunakan algoritma *Triangle Chain Cipher* dapat dilihat sebagai berikut :

Plainteks : NUR
Kunci : 3

Simbol	N	U	R
ASCII	78	85	82

M11 = (P[1] + (3 * R[1])) mod 256
= (N + (3 * 1)) mod
= (78 + 3) mod 256
= 81 (Q)

M12 = (P[2] + (3 * R[1])) mod 256
= (U + (3 * 1)) mod
= (85 + 3) mod 256
= 88 (X)

M13 = (P[3] + (3 * R[1])) mod 256
= (R + (3 * 1)) mod
= (82 + 3) mod 256
= 85 (U)

	j1	j2	j3
0	N	U	R
i1	Q	X	U
i2			
i3			

M22 = (M12 + (3 * 2) mod 256
= (X + (3 * 2)) mod
= (88 + 6) mod 256
= 94 (^)

M23 = (M13 + (3 * 2) mod 256
= (U + (3 * 2)) mod
= (85 + 6) mod 256
= 91 ([ )

	j1	j2	j3
0	N	U	R
i1	Q	X	U
i2		^	[
i3			

M33 = (M23 + (3 * 3) mod 256
= ([+ (3 * 3)) mod
= (91 + 9) mod 256
= 100 (d)

	j1	j2	j3
0	N	U	R
i1	Q	X	U
i2		^	[
i3			D

Hasil enkripsi segitiga pertama adalah **Q ^ d**. Hasil tersebut akan di enkripsi lagi pada segitiga kedua sebagai berikut :

M11 = (P[1] + (3 * R[1])) mod 256

M12 = (P[2] + (3 * R[1])) mod 256

= (Q + (3 * 1)) mod
= (81 + 3) mod 256
= 84 (T)

= (^ + (3 * 1)) mod
= (94 + 3) mod 256
= 97 (a)

M13 = (P[3] + (3 * R[1])) mod 256
= (d + (3 * 1)) mod
= (100 + 3) mod 256
= 103 (g)

	j1	j2	j3
0	Q	^	D
i1	T	A	G
i2			
i3			

M21 = (M11 + (3 * 2) mod 256
= (T + (3 * 2)) mod
= (84 + 6) mod 256
= 90 (Z)

M22 = (M12 + (3 * 2) mod 256
= (a + (3 * 2)) mod
= (97 + 6) mod 256
= 103 (g)

	j1	j2	j3
0	Q	^	D
i1	T	A	G
i2	Z	G	
i3			

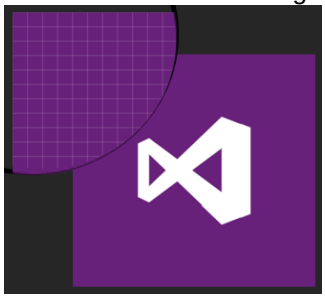
M31 = (M21 + (3 * 3) mod 256
= (Z + (3 * 3)) mod
= (90 + 9) mod 256
= 99 (c)

	j1	j2	j3
0	Q	^	D
i1	T	A	G
i2	Z	G	
i3	C		

Hasil enkripsi segitiga kedua adalah **c g g** hasil tersebut merupakan hasil enkripsi plainteks NUR dengan kunci 3. Selanjutnya hasil enkripsi tersebut akan disisipkan pada sebuah *file* gambar.

3.2 Penyisipan Algoritma LSB

Misalnya ada sebuah gambar dan salah satu bagiannya di zoom untuk dilihat nilai pixelnya. Dimana nilai RGB dari tiap pixel akan di ubah ke dalam bentuk biner sebagai berikut.



Gambar 2. Pixel pada sebuah gambar

R	G	B	R	G	B	R	G	B
01101000	00100001	01111010	01101000	00100001	01111010	01101000	00100001	01111010
01101000	00100001	01111010	01101000	00100001	01111010	01101000	00100001	01111010
01101000	00100001	01111010	01101000	00100001	01111010	01101000	00100001	01111010

Pesan yang akan disisipkan adalah **cgg**, yang merupakan hasil enkripsi dari plaintext NUR dengan kunci 3 menggunakan algoritma Triangle Chain Cipher maka sebelum proses penyisipan pesan tersebut akan diubah ke dalam bentuk biner sehingga dihasilkan :

c :	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**1**
g :	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**
g :	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**

Algoritma LSB ketentuan penyisipan pesan adalah mengganti *bit* ke 8, 16 dan 24 setiap pixel gambar dengan nilai biner dari pesan yang akan disisipkan, sehingga berdasarkan ketentuan tersebut hasil penyisipan dapat dilihat pada bit gambar yang ditebalkan (*bold*).

R	G	B	R	G	B	R	G	B
0110100**0**	0010000**1**	0111101**1**	0110100**0**	0010000**0**	0111101**0**	0110100**1**	0010000**1**	0111101**0**
0110100**1**	0010000**1**	0111101**0**	0110100**0**	0010000**1**	0111101**1**	0110100**1**	0010000**0**	0111101**1**
0110100**1**	0010000**0**	0111101**0**	0110100**1**	0010000**1**	0111101**1**	01101000	00100001	01111010

Gambar yang dihasilkan adalah sebagai berikut :

Gambar 3. Susunan Bit pada Gambar RGB

Tidak terdapat perbedaan yang tampak antara gambar awal dengan gambar yang telah disisipkan pesan dikarenakan hanya mengubah bit paling akhir sehingga tidak dapat dibedakan secara kasat mata.

3.3 Ekstraksi Algoritma LSB

Proses pengambilan pesan menggunakan algoritma LSB adalah dengan mengambil nilai tiap-tiap bit paling kanan dari nilai biner *pixel* gambar. Sehingga dari hasil penyisipan pesan, dari proses pengambilan tiap-tiap bit paling kanan akan dihasilkan nilai :

0	**1**	**1**	**0**	**0**	**0**	**1**	**1**	: c
0	**1**	**1**	**0**	**0**	**1**	**1**	**1**	: g
0	**1**	**1**	**0**	**0**	**1**	**1**	**1**	: g

Hasil yang di dapat dari ekstraksi pesan menggunakan algoritma LSB adalah **cgg**. Selanjutnya hasil tersebut akan di dekripsi menggunakan algoritma *Triangle Chain Cipher*.

3.4 Dekripsi Algoritma *Triangle Chain Cipher*

Selanjutnya dilakukan proses dekripsi menggunakan *ciphertext* **c g g** dengan kunci 3. Prosesnya dapat dilihat di bawah ini :

M11 = (C[1] - (3 * R[1])) mod 256
= (c - (3 * 1)) mod
= (99 - 3) mod 256
= 96 (`)

M12 = (C[2] - (3 * R[1])) mod 256
= (g - (3 * 1)) mod
= (103 - 3) mod 256
= 100 (d)

M13 = (C[3] - (3 * R[1])) mod 256
= (g - (3 * 1)) mod
= (103 - 3) mod 256
= 100 (d)

M14

	j1	j2	j3
0	C	D	G
i1	`	D	D
i2			
i3			

M21 = (M11 - (3 * 2) mod 256
= (` - (3 * 2)) mod
= (96 - 6) mod 256
= 90 (Z)

M22 = (M12 - (3 * 2) mod 256
= (d - (3 * 2)) mod
= (100 - 6) mod 256
= 94 (^)

	j1	j2	j3
0	C	D	G
i1	`	A	D
i2	Z	^	
i3			

M31 = (M21 - (3 * 3) mod 256
= (Z - (3 * 3)) mod
= (90 - 9) mod 256
= 81 (Q)

	j1	j2	j3
0	C	D	G
i1	`	A	D
i2	Z	^	
i3	Q		

Hasil dekripsi segitiga pertama adalah **Q ^ d**. Hasil tersebut akan di dekripsi kembali pada segitiga kedua sebagai berikut :

M11 = (C[1] - (3 * R[1])) mod 256
= (Q - (3 * 1)) mod
= (81 - 3) mod 256
= 78 (N)

M12 = (C[2] - (3 * R[1])) mod 256
= (^ - (3 * 1)) mod
= (94 - 3) mod 256
= 91 ([ )

M13 = (C[3] - (3 * R[1])) mod 256
= (d - (3 * 1)) mod
= (100 - 3) mod 256
= 97 (a)

	j1	j2	j3
0	Q	^	D
i1	N	[	A
i2			
i3			

M22 = (M12 - (3 * 2) mod 256
= ([- (3 * 2)) mod
= (91 - 6) mod 256
= 85 (U)

M23 = (M13 - (3 * 2) mod 256
= (a - (3 * 2)) mod
= (97 - 6) mod 256
= 91 ([ )

	j1	j2	j3
0	Q	^	D
i1	N	[	A
i2		U	[
i3			

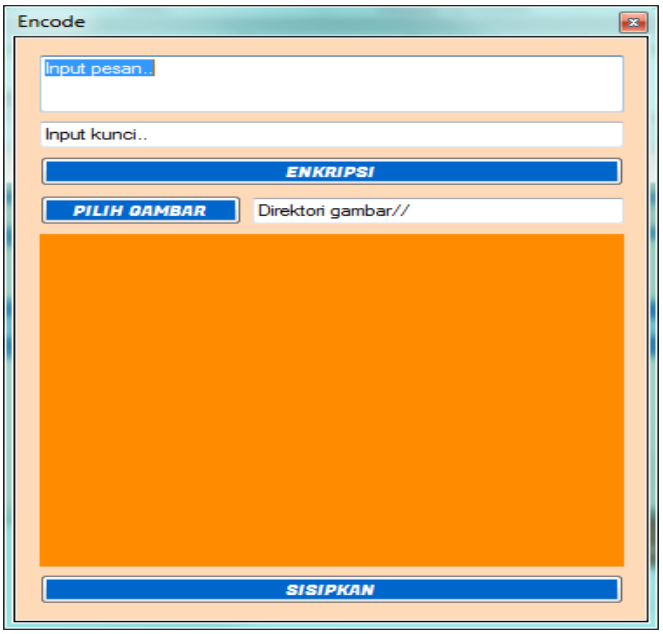
M33 = (M23 - (3 * 3) mod 256
= ([- (3 * 3)) mod
= (91 - 9) mod 256
= 82 (R)

	j1	j2	j3
0	Q	^	D
i1	N	[	A
i2		U	[
i3			R

Hasil dekripsi segitiga kedua adalah **NUR** dan ini merupakan hasil dekripsi *ciphertext* **cgg** dengan kunci 3.

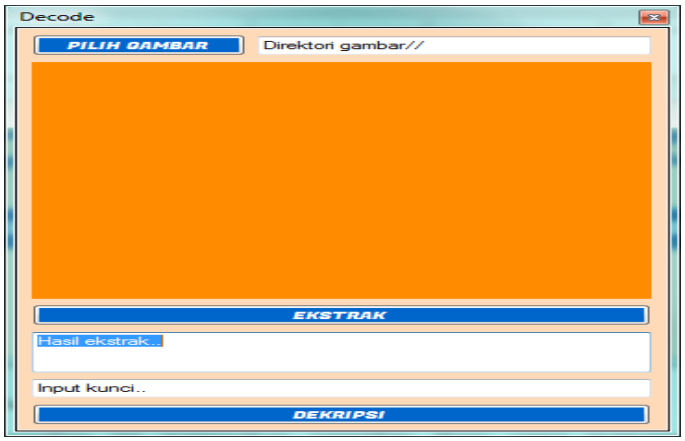
3.5 Hasil

1. Tampilan *Form Encode*
   Formencode digunakan untuk melakukan proses enkripsi pesan dan menyisipkan pesan hasil enkripsi ke dalam sebuah gambar. Gambar tampilan *FormEncode* ditunjukkan pada gambar 4 :



Gambar 4. Tampilan *FormEncode*

2. Tampilan *Form Decode*
   Form decode ini digunakan untuk melakukan proses ekstrak pesan yang terdapat pada gambar dan proses dekripsi pesan yang telah di ekstrak. Gambar tampilan *FormDecode* ditunjukkan pada gambar 5 :



Gambar 5. Tampilan *Form Decode*

Kelebihan dan kekurangan dari hasil rancangan tentang aplikasi keamanan pesan menggunakan algoritma *TriangleChainCipher* dan LSB berbasis *desktop* yang telah dibangun dapat penulis simpulkan sebagai berikut :

1. Kelebihan Aplikasi
   a. Aplikasi ini dapat digunakan untuk melakukan enkripsi pesan dan menyisipkan pesan hasil enkripsi ke dalam sebuah gambar.
   b. Dengan aplikasi yang dihasilkan dari penelitian ini pengguna juga dapat melakukan proses ektrak dan dekripsi pesan yang terdapat pada sebuah gambar.
2. Kekurangan dari aplikasi yang dirancang :
   a. Belum terdapat fitur yang dapat digunakan untuk mengirimkan gambar yang telah disisipkan pesan secara langsung dari aplikasi.
   b. Aplikasi ini belum dapat digunakan pada perangkat lain selain komputer maupun laptop.

4. KESIMPULAN

Berdasarkan hasil pambahasan dan uji coba yang telah dilakukan, dapat disimpulkan :

1. Aplikasi yang dihasilkan dari penelitian ini dapat digunakan untuk mengamankan sebuah pesan rahasia dengan proses enkripsi dan menyisipkan hasil enkripsi ke dalam gambar.

2. Untuk mengamankan pesan rahasia pada penelitian ini digunakan algoritma Triangle Chain Cipher dan algoritma LSB.
3. Algoritma Triangle Chain Cipher digunakan untuk proses enkripsi dan dekripsi pesan sedangkan algoritma LSB digunakan untuk proses penyisipan dan ekstrak pesan pada gambar.

UCAPAN TERIMAKASIH

Kami mengucapkan terima kasih kepada seluruh yang telah meluangkan waktu untuk berpartisipasi dalam penelitian ini, sehingga data yang diperlukan dapat terkumpul dengan baik. Kami mengapresiasi masukan berharga dari editor dan reviewer yang membantu memperbaiki kualitas naskah ini hingga layak diterbitkan.

REFERENSI

[1] D. S. Purwanti *et al.*, "Perancangan Penerapan Algoritma AES 256 Untuk Keamanan Database Aplikasi Manajemen Siswa," *STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer,* vol. 4, no. 2, pp. 111–119, May 2025, doi: 10.55123. (**Available**)

[2] A. B. Musfiroh, "CITRA RGB (RED, GREEN & BLUE), Biner, Dan Grayscale Dalam Image Processing Hilal Untuk Penentuan Awal Bulan Kamariah," *Uin Walisongo Semarang*, 2023. (**Available**)

[3] W. S. Negoro, A. H. Azhar, R. A. Destari, and A. Syahrini, "Edukasi Pengolahan Citra Digital Untuk Pendeteksian Dan Informasi Pengetahuan Yang Tersembunyi Pada Citra," *STIKOM Tunas Bangsa, Pematangsiantar.*, 2024. (**Available**)

[4] Manurung, Rodiyah Aini, Sutarman, Efendi, and Syahril, "Comparative Analysis of the Performance of Four Symmetric Algorithms on Digital File Security," *JITE (Journal of Informatics and Telecommunication Engineering)*, Jan. 2025, doi: 10.31289/jite.v8i2.13978. (**Available**)

[5] N. Mevian Deaz, J. Jumadi, and A. Al Akbar, "Implementasi Keamanan Pada Citra Digital Menggunakan Algoritma Least Congruential Generator Dan Least Significant BiT," 2025. [Online]. (**Available**)

[6] M. R. Fahlevvi, D. Satria, A. Putra, and W. Ariandi, "Algoritma AES128-CBC (Advanced Encryption Standard) Untuk Enkripsi Dan Dekripsi Berkas Dokumen PT. Adiarta Muzizat," 2025. (**Available**)

[7] 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, doi: 10.34312/euler.v10i2.16646. (**Available**)

[8] R. P. Putra, J. Jumadi, and D. Lianda, "Pengolahan Citra Digital Untuk Mengidentifikasi Tingkat Kematangan Buah Kelapa Sawit Berdasarkan Warna Rgb Dan Hsv Dengan Menggunakan Metode Self Organizing Map (SOM)," Feb. 2024. (**Available**)

[9] Mahrizal, M. Dedek, and Ihsan, "Perancangan Aplikasi Penyisipan Pesan Pada Pixel Citra Menggunakan Metode End Of File," 2019. (**Available**)

[10] F. Tambunan and E. N. Purba, "Penyembunyian Pesan Chyper Kedalam Gambar Berwarna," *Methomika Jurnal Manajemen Informatika dan Komputerisasi Akuntansi*, vol. 4, no. 1, pp. 22–26, Apr. 2020, doi: 10.46880/jmika.Vol4No1.pp22-26. (**Available**)

[11] V. I. Anggraini and K. Kunci, "Implementasi Algoritma Triangle Chain Cipher Dan Gost Pada Pengamanan Citra Digital," *Bulletin of Information Technology (BIT)*, vol. 2, no. 3, pp. 118–128, 2021. (**Available**)

[12] M. Afsari, A. Damaiyanti, and N. Sa'adah, "Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1381. (**Available**)