

Pesan yang Dirahasiakan Menggunakan Algoritma Feal dan Caesar Chiper Disisipkan ke Dalam Gambar Menggunakan Metode *Least Significan Bit* (LSB)

Confidential Messages Using the Feal and Caesar Chiper Algorithms are Inserted into Images Using the Least Significant Bit (LSB) Method

Sofia Lorenta Parhusip^{a,1}, Ria Eka Sari^{b,2}

^{a,b}, Informatika, Universitas Potensi Utama, Jl. K.L Yos Sudarso KM 6,5 No.3-4 Tanjung Mulia,
Medan, 20241, Indonesia
shopialorenta11@gmail.com ¹, ladiespure@gmail.com ²

ABSTRAK

Pesan yang merupakan aset bernilai seharusnya dilindungi agar aman. Karena pesan adalah hasil pengolahan data menjadi bentuk yang lebih berguna bagi yang menerimanya yang menggambarkan suatu fakta yang digunakan sebagai alat bantu untuk pengambilan suatu keputusan. Pentingnya sebuah pesan sehingga pesan hanya boleh diakses oleh orang-orang tertentu. Apabila sebuah pesan penting yang bersifat rahasia dicuri oleh pihak yang tidak diizinkan akan berbahaya bagi pemilik pesan. Sebuah pesan yang di curi dapat dapat dikembangkan kembali menjadi bentuk yang lebih berguna. Oleh karena itu dibutuhkan adanya teknik untuk sebuah pesan penting yang bersifat rahasia sehingga pihak yang tidak diizinkan tidak dapat mengetahui isi pesan yang dicuri. Peneliti menambahkan algoritma Caesar Cipher untuk memperkuat hasil enkripsi algoritma FEAL. Namun untuk menggunakan steganografi maka membutuhkan metode yang tepat, oleh karena itu peneliti menggunakan metode least significant bit. Least Significant Bit (LSB) dipergunakan untuk menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam cover dengan bit-bit data rahasia.

Kata Kunci : Kerahasiaan, Pesan, FEAL, Caesar Chiper, Gambar, LSB

ABSTRACT

Messages which are valuable assets should be protected to be safe. Because the message is the result of processing data into a form that is more useful for those who receive it, which describes a fact that is used as a tool to help make a decision. The importance of a message so that the message can only be accessed by certain people. If an important, confidential message is stolen by an unauthorized party, it will be dangerous for the message owner. A stolen message can be redeveloped into a more useful form. Therefore, it is necessary to have a technique for an important message that is confidential so that unauthorized parties cannot find out the contents of the stolen message. Researchers added the Caesar Cipher algorithm to strengthen the encryption results of the FEAL algorithm. However, to use steganography you need the right method, therefore researchers use the least significant bit method. Least Significant Bit (LSB) is used to hide data by replacing the least significant data bits in the cover with secret data bits.

Keywords : Confidentiality, Message, FEAL, Caesar Chiper, Image, LSB

Info Artikel :

Disubmit: 16 Februari 2024

Direview: 26 Maret 2024

Diterima : 14 April 2024

Copyright © 2024 - Journal UPU. All rights reserved..

1. PENDAHULUAN

Pesan yang merupakan aset bernilai seharusnya dilindungi agar aman. [1]. Karena pesan adalah hasil pengolahan data menjadi bentuk yang lebih berguna bagi yang menerimanya yang menggambarkan suatu fakta yang digunakan sebagai alat bantu untuk pengambilan suatu keputusan. Pentingnya sebuah pesan sehingga pesan hanya boleh diakses oleh orang-orang tertentu. Apabila sebuah pesan penting yang bersifat rahasia dicuri oleh pihak yang tidak diizinkan akan berbahaya bagi pemilik pesan. Sebuah pesan yang dicuri dapat dapat dikembangkan kembali menjadi bentuk yang lebih berguna. [2]. Oleh karena itu dibutuhkan adanya teknik untuk sebuah pesan penting yang bersifat rahasia sehingga pihak yang tidak diizinkan tidak dapat mengetahui isi pesan yang dicuri. Teknik yang dapat digunakan yaitu dengan merahasiakan sebuah pesan dengan kriptografi. [3]. Penggunaan kriptografi membutuhkan sebuah metode yang dapat mengubah pesan yang asli menjadi pesan rahasia dengan baik. Untuk itu peneliti menggunakan metode FEAL. [4]. Peneliti menambahkan algoritma *Caesar Cipher* untuk memperkuat hasil enkripsi algoritma FEAL[5]. Namun untuk menggunakan steganografi maka membutuhkan metode yang tepat, oleh karena itu peneliti menggunakan metode *least significant bit*. *Least Significant Bit* (LSB) dipergunakan untuk menyembunyikan data dengan mengganti *bit-bit* data yang paling tidak berarti di dalam *cover* dengan *bit-bit* data rahasia. [6]. Dengan adanya penyandian pesan dan kemudian pesan yang tersandi disisipkan kedalam sebuah gambar, maka pesan yang bersifat rahasia tidak akan dengan mudah diketahui oleh pihak yang tidak diinginkan. [7]. Berdasarkan penelitian yang dilakukan oleh Fadillah et al (2022) mengenai Implementasi Algoritma Fast Encryption Algorithm (FEAL) Dan Algoritma Fibonacci Mengamankan File Teks, Fadillah, dkk menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk mengamankan file teks. Sedangkan penelitian penulis menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk kerahasiaan pesan teks. Berdasarkan penelitian yang dilakukan oleh Ismail, Syahrir (2021) mengenai Sistem Keamanan Pesan Email Menggunakan Algoritma Kriptografi Klasik, Ismail dan Syahrir menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk mengamankan pesan email. [8]. Sedangkan penelitian penulis menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk kerahasiaan pesan teks yang akan disisipkan ke dalam gambar. Berdasarkan penelitian yang dilakukan oleh Siregar (2020) mengenai Pengamanan Pesan Teks Menggunakan Algoritma FEAL dan RSA Pada Aplikasi Android, Siregar menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk mengamankan pesan teks. Sedangkan penelitian penulis menggunakan algoritma Fast Encryption Algorithm (FEAL) untuk kerahasiaan pesan teks yang akan disisipkan ke dalam gambar. [9]. Berdasarkan penelitian yang dilakukan oleh Mira et al (2022) mengenai Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks, Mira et al menggunakan algoritma Caesar Cipher untuk mengamankan pesan teks. Sedangkan penelitian penulis menggunakan algoritma Caesar Cipher untuk kerahasiaan pesan teks yang akan disisipkan ke dalam gambar. Berdasarkan penelitian yang dilakukan oleh Ziliwu et al (2020) mengenai Implementasi Caesar Cipher Pada Algoritma Kriptografi Dalam Penyandian Pesan Whatsapp, Ziliwu et al menggunakan algoritma Caesar Cipher untuk penyandian pesan. [10]. Sedangkan penelitian penulis menggunakan algoritma Caesar Cipher untuk kerahasiaan pesan teks yang akan disisipkan ke dalam gambar. Berdasarkan penelitian yang dilakukan oleh Hermansa et al (2020) mengenai Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra, Ziliwu et al menggunakan algoritma Caesar Cipher untuk pengamanan pesan yang akan disisipkan ke dalam gambar menggunakan EOF. Sedangkan penelitian penulis menggunakan algoritma Caesar Cipher untuk kerahasiaan pesan teks yang akan disisipkan ke dalam gambar menggunakan LSB. Berdasarkan penelitian yang dilakukan oleh Apriyansyah et al (2020) mengenai Implementasi Sistem Keamanan Pesan Teks Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB), Apriyansyah et al menggunakan metode Least Significant Bit untuk keamanan pesan teks. Sedangkan

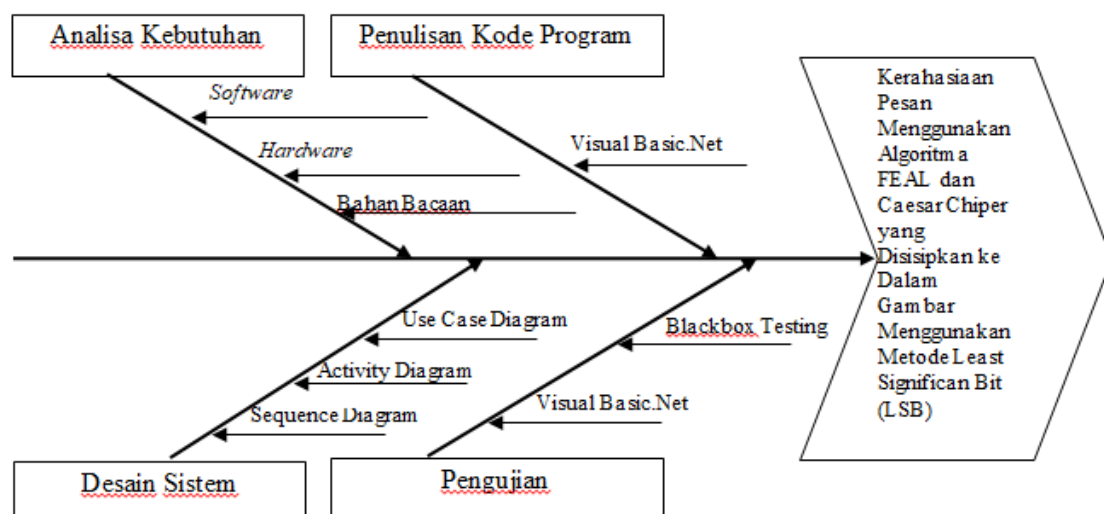
penelitian penulis menggunakan metode Least Significant Bit untuk penyisipan pesan rahasia ke dalam gambar.

Berdasarkan penelitian yang dilakukan oleh Hakim et al (2021) mengenai Steganografi Citra Digital Menggunakan Metode Least Significant Bit (LSB), Hakim et al menggunakan metode Least Significant Bit untuk citra digital. Sedangkan penelitian penulis menggunakan metode Least Significant Bit untuk penyisipan pesan rahasia ke dalam gambar. Berdasarkan penelitian yang dilakukan oleh Sitio (2020) mengenai Penyisipan Pesan dengan Metode Least Significant Bit Pada Objek Citra Digital Yang Terdeteksi Tepi Dengan Sobel, Sitio menggunakan metode Least Significant Bit untuk objek citra digital. Sedangkan penelitian penulis menggunakan metode Least Significant Bit untuk penyisipan pesan rahasia ke dalam gambar.

2. METODE

Pesan yang merupakan aset bernilai seharusnya dilindungi agar aman. Karena pesan adalah hasil pengolahan data menjadi bentuk yang lebih berguna bagi yang menerimanya yang menggambarkan suatu fakta yang digunakan sebagai alat bantu untuk pengambilan suatu keputusan. Pentingnya sebuah pesan sehingga pesan hanya boleh diakses oleh orang-orang tertentu. Apabila sebuah pesan penting yang bersifat rahasia dicuri oleh pihak yang tidak diizinkan akan berbahaya bagi pemilik pesan. Sebuah pesan yang di curi dapat dapat dikembangkan kembali menjadi bentuk yang lebih berguna. Oleh karena itu dibutuhkan adanya teknik untuk sebuah pesan penting yang bersifat rahasia sehingga pihak yang tidak diizinkan tidak dapat mengetahui isi pesan yang dicuri. Teknik yang dapat digunakan yaitu dengan merahasiakan sebuah pesan dengan kriptografi. Penggunaan kriptografi membutuhkan sebuah metode yang dapat mengubah pesan yang asli menjadi pesan rahasia dengan baik. Untuk itu peneliti menggunakan metode FEAL. Peneliti menambahkan algoritma Caesar Cipher untuk memperkuat hasil enkripsi algoritma FEAL. Namun untuk menggunakan steganografi maka membutuhkan metode yang tepat, oleh karena itu peneliti menggunakan metode least significant bit. Least Significant Bit (LSB) dipergunakan untuk menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam cover dengan bit-bit data rahasia. Dengan adanya penyandian pesan dan kemudian pesan yang tersandi disisipkan kedalam sebuah gambar, maka pesan yang bersifat rahasia tidak akan dengan mudah diketahui oleh pihak yang tidak diinginkan. Dengan latar belakang diatas maka penulis mengambil judul “Kerahasiaan Pesan Menggunakan Algoritma FEAL dan Caesar Chiper yang Disisipkan ke Dalam Gambar Menggunakan Metode Least Significan Bit (LSB)”.

A. Metode Pengumpulan Data



Gambar 1. Diagram *Fish Bone* Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan, Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian. Peneliti juga menentukan *software* dan *hardware* yang akan digunakan untuk membuat penelitian.
2. Desain Sistem, Untuk mendesain sistem peneliti menggunakan beberapa pemodelan UML yaitu *use case diagram*, *activity diagram* dan *sequence diagram*.
3. Penulisan Kode Program Dalam penulisan kode program, peneliti menggunakan bahasa pemrograman *Visual Basic.Net*.
4. Pengujian program dilakukan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik. Pengujian dengan teori menggunakan *blackbox testing* dan pengujian dengan praktek menggunakan *visual basi.net*.
5. Hasil, Pada tahapan ini aplikasi implementasi algoritma Kerahasiaan Pesan Menggunakan Algoritma FEAL dan Caesar Chiper yang Disisipkan ke Dalam Gambar Menggunakan Metode *Least Significan Bit* (LSB).

3. HASIL DAN PEMBAHASAN

A. Hasil

Kerahasiaan Pesan Menggunakan Algoritma FEAL dan Caesar Chiper yang Disisipkan ke Dalam Gambar Menggunakan Metode *Least Significan Bit* (LSB) dibuat menggunakan *Visual Basic* 2010, dimulai dengan merancang sistem, menerapkan perhitungan metode dan menerapkan komponen sebenarnya ke dalam *Visual Basic* 2010 sehingga aplikasi dapat diselesaikan sesuai dengan perancangan. Berikut adalah beberapa tampilan yang dihasilkan dari pembuatan aplikasi yang telah dilakukan:



Gambar 2. Tampilan *Form* Enkrip Dan Sisip

Gambar IV.1 merupakan *form* enkrip dan sisip, untuk merahasiakan pesan yang akan dienkrip kemudian disisipkan ke dalam gambar maka pengguna terlebih dahulu harus mengupload gambar yang akan digunakan dengan menekan tombol browse, setelah gambar berhasil diupload kemudian pengguna harus memasukkan kunci enkrip. Setelah semua kunci dimasukkan kemudian pengguna harus menulis sebuah pesan di dalam kotak isi pesan dan mengklik tombol enkrip maka aplikasi akan menampilkan jendela untuk pencarian lokasi penyimpanan gambar yang telah disisipkan pesan yang telah dienkripsi.

Jika pengguna ingin mengosongkan pesan maka pengguna harus mengklik tombol kosongkan pesan dan jika pengguna ingin mengekstrak kembali pesan yang ada di dalam gambar maka pengguna harus mengklik tombol ekstrak dan dekrip kemudian sistem akan menampilkan *form* ekstrak dan dekrip seperti pada Gambar IV.2.



Gambar 3. Tampilan *Form* Ekstrak Dan Dekrip

Gambar IV.2 merupakan *form* ekstrak dan dekrip, penggunaan aplikasi dimulai dari pengambilan gambar pada tombol browse, kemudian pengguna harus memasukkan kunci dan tekan tombol dekrip. Untuk membuka kembali dan menyisipkan pesan ke dalam gambar maka pengguna harus mengklik tombol Enkrip Dan Sisip.

B. Pembahasan

a) Metode FEAL

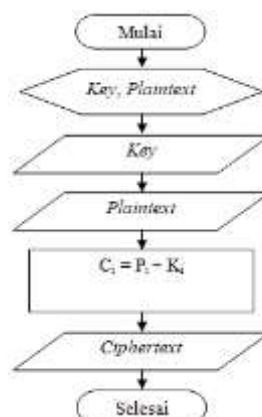
Langkah-langkah metode FEAL untuk enkrip dapat dilihat sebagai berikut:

1. Buat pesan untuk di enkrip.
2. Buat kunci untuk proses enkrip.
3. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
4. Lakukan proses xor *ascii* kunci terhadap *ascii* pesan pada tiap karakter.

Berikut ini adalah rumus enkrip dari metode FEAL:

$$C_i = (P_i \text{ xor } K_i) \text{ mod } 256$$

Flowchart metode enkrip FEAL dapat dilihat sebagai berikut:



Gambar 4. *Flowchart* Enkrip Metode FEAL

Langkah-langkah metode FEAL untuk dekrip dapat dilihat sebagai berikut:

1. Masukkan *ciphertext* untuk di dekrip.
2. Masukkan kunci dekrip *ciphertext*.

3. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
4. Lakukan proses xor *ascii* pesan terhadap *ascii* kunci pada tiap karakter.

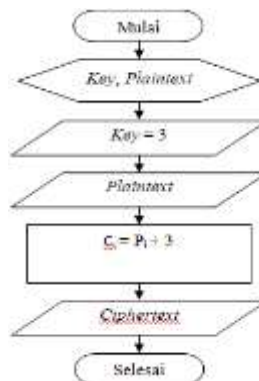
Kemudian di enkrip menggunakan metode *Caesar cipher*:

Langkah-langkah metode *Caesar Cipher* untuk enkrip dapat dilihat sebagai berikut:

1. Buat pesan untuk di enkrip.
2. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
3. Lakukan proses penjumlahan 13 terhadap *ascii* pesan pada tiap karakter.

Berikut ini adalah rumus enkrip dari metode *Caesar Cipher*: $C_i = P_i + 3$

Flowchart metode enkrip *Caesar Cipher* dapat dilihat sebagai berikut:



Gambar 5. Flowchart Enkrip Metode Caesar Cipher

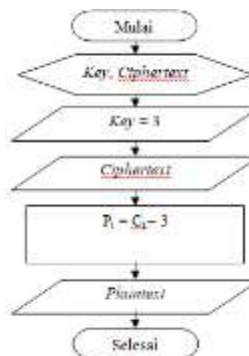
b) Metode Caesar Cipher

Langkah-langkah metode *Caesar Cipher* untuk dekrip dapat dilihat sebagai berikut:

1. Masukkan *ciphertext* untuk di dekrip.
2. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
3. Lakukan proses pengurangan 3 terhadap *ascii* pesan pada tiap karakter.

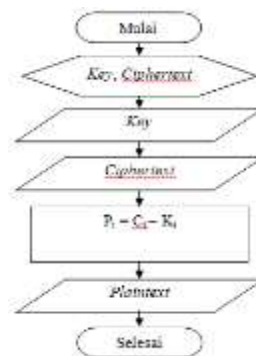
Berikut ini adalah rumus dekrip dari metode *Caesar Cipher*: $P_i = C_i - 3$

Flowchart metode dekrip *Caesar Cipher* dapat dilihat sebagai berikut:



Gambar 6. Flowchart Dekrip Metode Caesar Cipher

Berikut ini adalah rumus dekrip dari metode FEAL: $P_i = (C_i - K_i) \bmod 256$
Flowchart metode dekrip FEAL dapat dilihat sebagai berikut:



Gambar 7. Flowchart Dekrip Metode FEAL

4. Enkrip

Pada tahapan ini dilakukan proses enkrip yang dimulai dari metode FEAL, kemudian hasil metode FEAL di enkrip menggunakan metode Caesar cipher.

Contoh Proses Enkrip:

Plaintext : 954608

Kunci: 123456

Solusi:

Ascii Plaintext:

9 = 57

5 = 53

4 = 52

6 = 54

0 = 48

8 = 56

Key:

1 = 49

2 = 50

3 = 51

4 = 52

5 = 53

6 = 54

$C_1 = (9 + k_1) \bmod 256$
 $= (57 + 49) \bmod 256$
 $= 106 \bmod 256$
 $= 106 = j$

$C_2 = (5 + k_2) \bmod 256$

$$\begin{aligned} &= (53 + 50) \bmod 256 \\ &= 103 \bmod 256 \\ &= 103 = g \\ \text{C3} &= (4 + k3) \bmod 256 \\ &= (52 + 51) \bmod 256 \\ &= 103 \bmod 256 \\ &= 103 = g \\ \text{C4} &= (6 + k4) \bmod 256 \\ &= (54 + 52) \bmod 256 \\ &= 106 \bmod 256 \\ &= 106 = j \\ \text{C5} &= (0 + k5) \bmod 256 \\ &= (48 + 53) \bmod 256 \\ &= 101 \bmod 256 \\ &= 101 = e \\ \text{C6} &= (8 + k6) \bmod 256 \\ &= (56 + 54) \bmod 256 \\ &= 110 \bmod 256 \\ &= 110 = n \end{aligned}$$

Chipertext: jggjen

Kemudian di enkrip menggunakan *Caesar cipher*:

Ubah plaintext menjadi ASCII:

j = 106
g = 103
g = 103
j = 106
e = 101
n = 120

Proses enkripsi:

$$\begin{aligned} C_i &= P_i + K_i \\ j &= 106 + 3 = 109 = m \\ g &= 103 + 3 = 106 = j \\ g &= 103 + 3 = 106 = j \\ j &= 106 + 3 = 109 = m \\ e &= 101 + 3 = 104 = h \\ n &= 120 + 3 = 123 = q \end{aligned}$$

Ciphertext: mjjmhq

5. Dekrip

Tahap selanjutnya adalah dengan melakukan dekrip. Pertama-tama di dekrip menggunakan metode Caesar cipher kemudian metode FEAL.

Proses dekripsi metode caesar cipher:

$$\begin{aligned} P_i &= C_i - K_i \\ m &= 109 - 3 = 106 = j \\ j &= 106 - 3 = 103 = g \end{aligned}$$

$$j = 106 - 3 = 103 = g$$

$$m = 109 - 3 = 106 = j$$

$$h = 104 - 3 = 101 = e$$

$$q = 123 - 3 = 120 = n$$

Plaintext: jggen

Contoh proses dekrip FEAL:

Chipertext: jggjen

Kunci: 123456

Ascii Plaintext:

$$j = 106$$

$$g = 103$$

$$g = 103$$

$$j = 106$$

$$e = 101$$

$$n = 110$$

Key:

$$1 = 49$$

$$2 = 50$$

$$3 = 51$$

$$4 = 52$$

$$5 = 53$$

$$6 = 54$$

$$\begin{aligned} P1 &= (j - k1) \bmod 256 \\ &= (106 - 49) \bmod 256 \\ &= 57 \bmod 256 \\ &= 57 = 9 \end{aligned}$$

$$\begin{aligned} P2 &= (g - k2) \bmod 256 \\ &= (103 - 50) \bmod 256 \\ &= 53 \bmod 256 \\ &= 53 = 5 \end{aligned}$$

$$\begin{aligned} P3 &= (g - k3) \bmod 256 \\ &= (103 - 51) \bmod 256 \\ &= 52 \bmod 256 \\ &= 52 = 4 \end{aligned}$$

$$\begin{aligned} P4 &= (j - k4) \bmod 256 \\ &= (106 - 52) \bmod 256 \\ &= 54 \bmod 256 \\ &= 54 = 6 \end{aligned}$$

$$\begin{aligned} P5 &= (e - k5) \bmod 256 \\ &= (101 - 53) \bmod 256 \\ &= 48 \bmod 256 \\ &= 48 = 0 \end{aligned}$$

$$\begin{aligned} P6 &= (n - k6) \bmod 256 \\ &= (110 - 54) \bmod 256 \\ &= 56 \bmod 256 \\ &= 56 = 8 \end{aligned}$$

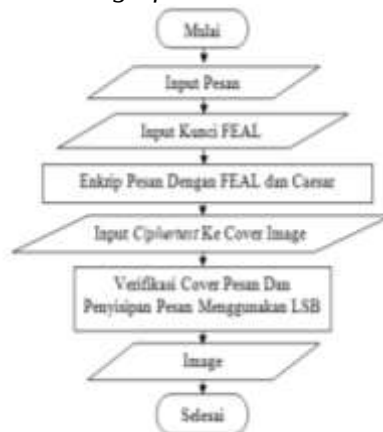
Plaintext: 954608

c) Metode Least Significant Bit (LSB)

Langkah-langkah metode LSB untuk penyisipan dan pengembalian pesan dapat dilihat sebagai berikut:

1. Tahapan dalam proses penyisipan pesan yakni:
 - a. Input pesan rahasia.
 - b. Verifikasi pesan, harus diinputkan.
 - c. *Input cover image*.
 - d. Verifikasi *cover image*.
 - e. Penyisipan pesan dengan metode *Least Significant Bit* yaitu dengan cara data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenalan start dari data tersebut dan pengenalan akhir dari data tersebut.
2. Tahapan dalam proses pengembalian pesan yakni:
 - a. *Input stego image*.
 - b. Verifikasi *stego image*.
 - c. Verifikasi *stego image*, harus terdapat pesan.
 - d. Pengambilan pesan dengan metode *Least Significant Bit* yaitu dengan cara data yang telah diisipkan pesan pada akhir file dibuka dari tanda khusus sebagai pengenalan start dari data tersebut dan pengenalan akhir dari data tersebut.

Flowchart penyisipan metode *Least Significant Bit*:



Gambar 8. Penyisipan Ciphertext FEAL, Caesar Cipher Dengan LSB

Flowchart pengembalian pesan metode *Least Significant Bit*:



Gambar 9. Pengembalian *Plaintext Caesar Cipher*, FEAL Dengan LSB

1. Proses Penyisipan Pesan

Untuk menyisipkan pesan ke dalam sebuah gambar, maka terlebih dahulu pesan diubah ke dalam kode *ascii* kemudian diubah lagi ke dalam bilangan biner sebagai berikut:

ASCII *Plaintext* (hasil enkrip): <8793:

Ascii *Plaintext*: < = 60 = 0011 1100

Misalkan matriks tingkat derajat keabuan citra dengan ukuran 3x3 pixel sebagai berikut:



Gambar 10. File Gambar Asli Format .BMP

Tabel 1. RGB Matriks Gambar Awal

Red (R)	Green (G)	Blue (B)
1111 1111	0000 0000	0000 0000
1111 1111	0000 0000	0000 0000
1111 1111	0000 0000	0000 0000
0000 0000	1111 1111	0000 0000
0000 0000	1111 1111	0000 0000
0000 0000	1111 1111	0000 0000
0000 0000	0000 0000	1111 1111
0000 0000	0000 0000	1111 1111
0000 0000	0000 0000	1111 1111

Kemudian pesan 13 = 00001101 disisipkan sehingga menjadi:

Tabel 2. RGB Matriks Gambar Akhir

Red (R)	Green (G)	Blue (B)
1111 1111	0000 0000	0000 000 <u>0</u>
1111 1111	0000 0000	0000 000 <u>0</u>
1111 1111	0000 0000	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	0000 0000	1111 111 <u>0</u>
0000 0000	0000 0000	1111 111 <u>0</u>
0000 0000	0000 0000	1111 1111

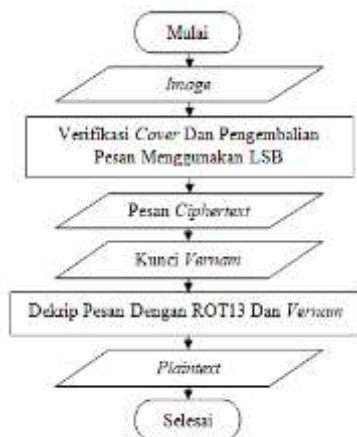
Keterangan:

Lakukan sampai seluruh pesan tersisip. Angka yang digaris bawah adalah pesan yang disisipkan menggunakan metode LSB. Nilai-nilai tersebut disimpan kembali ke dalam gambar sehingga menghasilkan gambar sebagai berikut:



Gambar 11. File Gambar Format .BMP Tersisip Pesan

Flowchart pengembalian pesan algoritma *Least Significant Bit*:



Gambar 12. Pengembalian Plaintext ROT13, Vernam Dengan LSB

Untuk mengekstrak pesan dari sebuah citra gambar yang disisipkan sebuah pesan, maka terlebih dahulu sebuah gambar diubah dalam bentuk nilai warna ke dalam kode *ascii* kemudian diubah lagi menggunakan bilangan biner. Gambar tersisip pesan adalah sebagai berikut:



Gambar 13. File Gambar Format .BMP Tersisip Pesan

Kemudian ekstrak pesan tersebut dari nilai biner gambar RGB:

Tabel 3. Citra Gambar Tersisip Pesan

Red (R)	Green (G)	Blue (B)
1111 1111	0000 0000	0000 000 <u>0</u>
1111 1111	0000 0000	0000 000 <u>0</u>
1111 1111	0000 0000	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	1111 1111	0000 000 <u>1</u>
0000 0000	0000 0000	1111 111 <u>0</u>
0000 0000	0000 0000	1111 111 <u>0</u>
0000 0000	0000 0000	1111 1111

Pada tabel III.3 merupakan citra gambar yang tersisip sebuah pesan, untuk mengekstrak sebuah pesan menggunakan metode LSB maka dapat diambil bit dari bilangan biner paling kanan dan kemudian disusun menjadi 8 bit bilangan biner sebagai berikut: 00111100.

Setelah bit tersusun menjadi 8 blok, kemudian 8 bit tersebut diubah ke dalam bentuk bilangan desimal yang menjadi kode *ascii* sebagai berikut: 00111100 = 60

Kode *ascii* tersebut diubah ke dalam karakter, sehingga pesan yang tadinya tersisip sudah dapat diketahui: 00111101 = 60

Lakukan seterusnya hingga menghasilkan seluruh pesan yang tersisip menjadi sebuah pesan.

2. Uji Coba

Uji coba pada Kerahasiaan Pesan Menggunakan Algoritma FEAL dan Caesar Chiper yang Disisipkan ke Dalam Gambar Menggunakan Metode *Least Significan Bit* (LSB) yaitu dengan menggunakan *blackbox testing* sebagai berikut:

Tabel 4. Blackbox Testing Enkrip Dan Sisip

No	Form Enkrip Dan Sisip	Keterangan	Hasil
1	Klik tombol browse	Aplikasi membuka jendela sistem	Benar
2	Klik tombol enkrip	Aplikasi mengubah pesan asli menjadi pesan rahasia	Benar
3	Klik tombol kosongkan pesan	Aplikasi menghapus pesan di dalam kotak pesan	Benar
4	Klik tombol buka dan dekrip	Aplikasi membuka <i>form</i> ekstrak dan dekrip	Benar

Tabel 5. Blackbox Testing Ekstrak Dan Dekrip

No	Form Buka Dan Dekrip	Keterangan	Hasil
1	Klik tombol browse	Aplikasi membuka jendela sistem	Benar
2	Klik tombol dekrip	Aplikasi akan mengubah pesan rahasia menjadi pesan asli	Benar
3	Klik tombol enkrip dan sisip	Aplikasi akan membuka <i>form</i> enkrip dan sisip	Benar
4	Klik tombol kosongkan pesan	Aplikasi membuka <i>form</i> ekstrak dan dekrip	Benar

3. Hasil Uji Coba

Berikut ini adalah kesimpulan dari hasil uji coba terhadap sistem yang telah dibuat:

Seluruh tools pada aplikasi telah berfungsi dengan baik.

1. Upload gambar ke dalam aplikasi berfungsi dengan baik.
2. Proses enkripsi dan dekripsi pesan berfungsi dengan baik.
3. Proses penyisipan pesan ke dalam gambar telah berjalan dengan baik.
4. Proses ekstraksi pesan dari dalam gambar telah berjalan dengan baik.
5. Perhitungan metode pada aplikasi telah sesuai dengan perhitungan teori.
6. Proses aplikasi tidak memiliki keterlambatan (*bug*).

4. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Dengan teknik kriptografi maka sebuah pesan dapat dirahasiakan dengan mengubah pesan yang dapat dipahami menjadi pesan yang tidak dapat dipahami oleh pencuri informasi.
2. Dengan menggunakan pesan dan kunci yang akan diinputkan, kemudian pesan dan kunci diubah menjadi *ascii* sehingga dapat diproses menggunakan Algoritma FEAL dan Caesar Chiper menjadi

pesan rahasia (*ciphertext*). *Ciphertext* tersebut disisipkan ke dalam gambar menggunakan metode LSB dengan menggunakan nilai biner dari *ciphertext* dan disisipkan diujung bit biner gambar.

3. Dengan menggunakan pemrograman *visual basic* 2010 kemudian menerapkan metode FEAL, Caesar Cipher dan LSB ke dalam pemrograman *visual basic* maka dapat menghasilkan Kerahasiaan Pesan Menggunakan Algoritma FEAL dan Caesar Cipher yang Disisipkan ke Dalam Gambar Menggunakan Metode *Least Significant Bit* (LSB).

UCAPAN TERIMA KASIH

Menulis karya ilmiah adalah proses yang menuntut keterampilan yang luas dan komitmen yang tinggi. Setelah melewati beberapa tahap penulisan yang panjang, akhirnya artikel ilmiah saya siap untuk diterbitkan. Sebelum itu, saya ucapkan terima kasih kepada semua orang yang telah membantu saya. Pertama-tama, saya ucapkan terima kasih kepada pembimbing saya. Tanpa bimbingan dan dukungan pembimbing, saya tidak akan dapat menyelesaikan proyek ini dengan sukses. Terima kasih untuk dedikasi dan pengorbanan pembimbing dalam membantu saya menyelesaikan proyek ini. Kedua, kepada diri sendiri begitu banyak hal yang terjadi, dan saya tetap bisa kuat dalam mengerjakan karya ilmiah ini, dalam proses penulisan ini saya telah bertemu versi diri saya yang paling lelah, paling capek, dan paling sok kuat, terima kasih sudah kuat sampai detik ini.

REFERENSI

- [1] Djawad, A. A. (2016). Pesan, Tanda, dan Makna dalam Studi Komunikasi. *STILISTIKA: Jurnal Bahasa, Sastra, Dan Pengajarannya*, 1(1).
- [2] Irawan, C. (2020). Kombinasi Metode Elgamal Dan Caesar Untuk Keamanan Pesan Yang Disisipkan Kedalam Gambar Menggunakan Lsb.
- [3] Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 1(1), 61-64.
- [4] Siregar, S. N. (2020). Pengamanan Pesan Teks Menggunakan Algoritma FEAL dan RSA Pada Aplikasi Android. *Journal of Computer System and Informatics (JoSYC)*, 1(4), 328-336.
- [5] Oper, N., Balafif, S., & To'o Fathonah Al-Khaliq, Z. (2022). MODIFIKASI ALGORITMA KRIPTOGRAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, 4(3), 179-184.
- [6] Ardiansyah, A., & Kumiasih, M. (2018). Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit. *Respati*, 13(3).
- [7] Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN. *Computer and Science Industrial Engineering (COMASIE)*, 7(2), 117-126.
- [8] Zuli, F., & Irawan, A. (2014). Penerapan Kombinasi Sandi Caesar Dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik. *STUDIA INFORMATIKA: JURNAL SISTEM INFORMASI*, 7(2).

- [9] Darmayanti, I., Astrida, D. N., & Ariyus, D. (2018). Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caesar Cipher Kedalam Bentuk Sandi Morse. Jurnal Ilmiah IT CIDA, 4(1).
- [10] Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN. Computer and Science Industrial Engineering (COMASIE), 7(2), 117-126.