Jurnal: Elektrika Borneo (JEB)
Vol. 6, No. 1, April 2020, hlm. 8-14 p-ISSN: 2443-0986
e-ISSN 2685-001X

PENERAPAN MODIFIKASI *VIGENERE CIPHER* PADA *LEAST SIGNIFICANT BIT STEGANOGRAPHY* MENGGUNAKAN PENDEKATAN *MIDPOINT CYRCLE*

Lipantri Mashur Gultom[1], Supria[2], Muhamad Nasir[3], Sarimuddin[4]

[1,2,3] Program Studi Teknik Informatika, Politeknik Negeri Bengkalis, Bengkalis, Riau, Indonesia
[4]Program Studi Sistem Informasi, Universitas Sembilanbelas November Kolaka, Kolaka, Sulawesi Tenggara, Indonesia

[1]lipantri@polbeng.ac.id
[2]phiya@polbeng.ac.id
[3]nasir@polbeng.ac.id
[4]sarimuddin@usn.ac.id

Abstract*— In the development of information technology is growing over time. With existing information technology has been widely used by people to exchange information, whether the information is confidential and non-confidential information. Such information requires strong security, particularly security in the delivery of information, because many hackers who always want to know the secrets of the information sent. Vigenere cipher is one of the methods of cryptography which is a method of encrypting a message from plain text into cipher text using a key that is intended that the message can't be read by unauthorized parties. Vigenere cipher has a weakness against cryptanalysis, one of which is a method kasiski. Least Significant Bit (LSB) is a method used to insert a message on low bit or bits of the far right, but the method is vulnerable to steganalysis. In this paper, the researchers used a modified process in cryptography to encrypt the message using the key (key) and then the encrypted message is inserted in a multimedia file with the method of least significant bits steganography. So that the proposed method will further enhance the security of the message, reduce vulnerability to cryptanalysis and steganalysis. The results of this study indicate that the hidden message can't be described well by steganalysis, due to modifications in vigenere cipher that uses the private key can only be described with the same private key.

***Keywords*— cryptography, the least significant bit, modification, private key, steganography.**

I**ntisari**— **Dalam perkembangan teknologi informasi yang semakin berkembang seiring dengan berjalannya waktu. Dengan teknologi informasi yang ada telah banyak digunakan orang untuk saling bertukar informasi, baik informasi yang bersifat rahasia dan informasi yang tidak bersifat rahasia. Informasi tersebut memerlukan keamanan yang kuat, khususnya keamanan dalam pengiriman informasi, karena banyak para *hacker* yang selalu ingin mengetahui rahasia pada informasi yang dikirim. *Vigenere cipher* salah satu dari metode *cryptography* yang merupakan metode enkripsi pesan dari *plain text* menjadi *cipher text* dengan menggunakan *key* yang bertujuan agar pesan tidak bisa dibaca oleh pihak yang tidak berwenang. *Vigenere cipher* memiliki kelemahan terhadap *cryptanalysis*, salah satunya adalah metode kasiski. *Least Significant Bit* (LSB) adalah sebuah metode yang digunakan untuk menyisipkan pesan pada bit rendah atau bit yang paling kanan, namun metode rentan terhadap *steganalysis*. Pada makalah ini, peneliti menggunakan proses modifikasi pada *criptography* untuk mengenkripsi pesan dengan menggunakan kunci (key) kemudian pesan yang dienkripsi disisipkan pada file multimedia dengan metode *least significant bit steganography*. Sehingga metode yang diusulkan ini akan lebih meningkatkan keamanan pesan, mengurangi kerentanan terhadap *cryptanalysis* dan *steganalysis*. Hasil dari penelitian ini menunjukkan bahwa pesan yang disembunyikan tidak akan bisa dideskripsi maupun dengan *steganalysis*, karena dengan modifikasi pada *vigenere cipher* yang menggunakan kunci pribadi hanya dapat dideskripsi dengan kunci pribadi yang sama.**

***Kata Kunci*— cryptography, the least significant bit, modification, key, Steganography, vigenere cipher.**

I. PENDAHULUAN

Teknologi informasi akan terus berkembang seiring dengan berjalannya waktu. Banyak orang yang menggunakan teknologi informasi tersebut untuk proses pertukaran informasi, seperti *email*, *chating* dan banyak lagi. Informasi yang dikirim merupakan informasi yang bersifat rahasia dan informasi yang bersifat tidak rahasia. Pada pengiriman informasi yang bersifat rahasia tentunya banyak hacker yang memiliki niat jahat, sehingga hacker melakukan berbagai cara untuk mengetahui isi pesan yang bersifat rahasia tersebut.

Vigenere cipher salah satu metode dari *cryptography* yang merupakan metode untuk mengenkripsi pesan dari *plain-text* menjadi *cipher-text*, yang bertujuan untuk mengamankan pesan agar tidak bisa dibaca oleh pihak yang tidak berwenang. *Vigenere cipher* menggunakan kunci (*key*) dalam mengenkripsi *plain-text* menjadi *cipher-text*, tetapi *vigenere cipher* memiliki kelemahan terhadap metode kasiski yang merupakan salah satu metode dari *criptanalysis*. Metode kasiski memanfaatkan kelemahan *Vigenere cipher* yang menggunakan kunci yang sama berulang kali dalam pengkodean karakternya. Walaupun begitu, masih ada teknik-teknik tertentu yang dapat dilakukan untuk memperkuat *Vigenere cipher* sekaligus menggagalkan metode Kasiski tersebut, yaitu dengan melakukan modifikasi pada *vigenere cipher*[1]. Modifikasi dilakukan dengan menerapkan enkripsi *Caesar Cipher* yang dibangkitkan dari kunci dan teknik pembangkitkan kunci berikutnya dengan menggunakan enkripsi *Vigenere* berlanjut sehingga kunci yang

digunakan untuk pengkodeannya akan berbeda dengan kunci yang digunakan sebelumnya. Dengan penggunaan metode ini, keterhubungan antara *plain text* dan *cipher text* akan akan menjadi semakin berkurang dan semakin sulit untuk dipecahkan kriptanalis [1].

Least significant bit steganography adalah metode yang sering dipakai untuk menyembunyikan pesan pada file multimedia seperti gambar, audio, video dan media lainnya [2][3]. Tetapi enkripsi pesan dengan menggunakan metode *least sinificant bit steganography* akan rentan terhadap *steganalysis* [4][5]. Sebuah metode seleksi fitur *steganalysis* berdasarkan kriteria *Fisher* digunakan dalam pengenalan pola sehingga dapat melakukan *steganalysis* terhadap *least significant bit* [6]. Pada penelitian makalah tahun 2014 oleh Vikas Verma, Poonam, Rishma Chawla [7], membuat penelitian tentang peningkatan metode *least significant bit steganography* dengan menggunakan pendekatan lingkaran *midpoint* sehingga dapat meningkatkan keamanan pesan. Metode ini akan mengurangi kerentanan terhadap *steganalysis* tetapi tidak pada *cryptanalysis* karena tidak diakukan enkripsi terlebih dahulu sebelum pesan disisipkan dengan metode *least significant bit steganography*.

Pada makalah ini, untuk lebih meningkatkan keamanan pesan tersebut diatas, peneliti akan menambahkan modifikasi *vigenere cipher* untuk mengenkripsi pesan atau *plain-text* menjadi *cipher-text*, kemudian hasil *cipher-text* disisipkan pada *image* menggunakan dengan metode *least significant bit steganography*. Hasil dari penelitian ini nantinya akan memperkuat penyembunyian pesan, sehingga pesan yang dikirimkan tidak akan bisa dibaca oleh pihak yang tidak berwenang.

II. LANDASAN TEORI

A. Teknik Modifikasi *Least Significant Bit*

Untuk meningkatkan keamanan pesan pada *steganography* sehingga dapat mengurangi kerentanan terhadap *steganalysis* maka solusinya adalah memodifikasi proses penyembunyian pesan pada *cover image* dengan menggunakan pendekatan *midpoint cyrcle*. *Least significant bit* digunakan untuk menyisipkan pesan pada bit yang bernilai rendah atau bit yang paling kanan, karena penggantian bit yang bernilai rendah tidak akan terlalu mempengaruhi tingkat warna. Pada sebuah gambar pada ruang warna RGB terdapat 3 warna *Red*, *Green* dan *Blue*, dan terdapat 24 bit setiap pixelnya yaitu 8 bit untuk warna merah, 8 bit untuk warna hijau dan 8 bit untuk warna biru. Jadi, pesan akan disisipkan disetiap bit ke 8 (bit paling kanan) pada setiap warna, sehingga 1 pixel gambar dapat disisipkan pesan sebesar 3 bit.

Contoh 1 :

a) Sebuah pesan "tes" jika dikonversi ke biner menjadi 1110100 1100101 1110011
b) Gambar dengan ukuran 2 x 5 pixel(px), jika dikonversi ke biner menjadi :

11001101	10010011	11100110	10001100	10000011	10001100
11001101	10010011	11100110	10001100	10000011	10101101
11001101	10010011	11100110	10001100	10000011	11001100
11001101	10010011	11100110	10001100	10000011	10011101
11001101	10010011	11100110	10001100	10000011	10101100

Gambar 1. Gambar 2x5 pixel dengan Nilai Biner

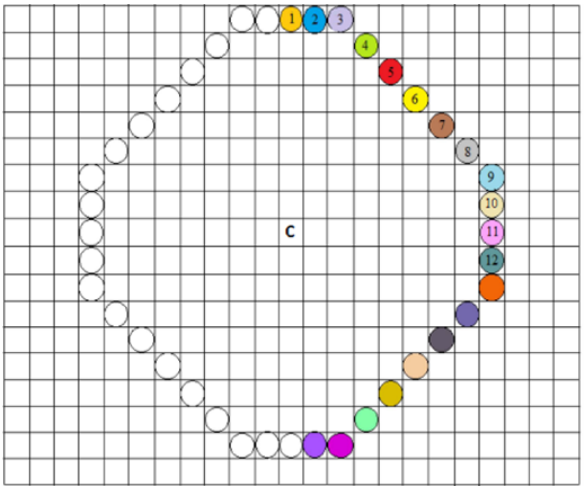
c) Dengan melakukan penyisipan pesan ke gambar sehingga menjadi :

1100110**1**	1001001**1**	1110011**1**	1000110**0**	1000001**1**	1001100
1100110**0**	1001001**1**	1110011**1**	1001100	1000001**0**	1010110**1**
1100110**0**	1001001**1**	1110011**1**	1001100**1**	1000001**1**	1100110**0**
1100110**0**	1001001**1**	1110011**1**	10001100	10000011	10011101
11001101	10010011	11100110	10001100	10000011	10101100

Ket : =t =e =s

Gambar 2. Pesan 'tes' Disisipkan Pada Gambar 2x5 pixel

Jadi, nilai yang ditandai 7 warna merah adalah 7 bit biner dari huruf "t", biru adalah 7 bit biner dari huruf "e" dan hijau adalah 7 bit biner dari huruf "s". Sehingga untuk menysisipkan kata "tes" memerlukan 7 pixel dari gambar. Pada penelitian makalah *international communication and signal processing*, tahun 2014 oleh Vikas Verma, Poonam, Rishma Chawla, India[7]. Membuat penelitian tentang peningkatan keamanan pada metode *least significant bit steganography* dengan menggunakan pendekatan lingkaran *midpoint* sehingga dapat meningkatkan keamanan dengan mengurangi kerentanan terhadap *steganalysis*.



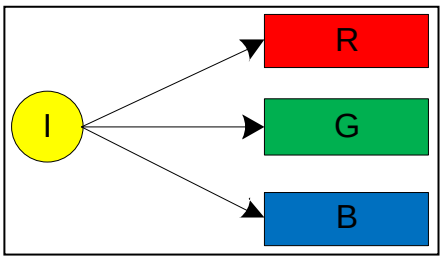
Gambar 3. Pemilihan Pixel Menggunakan Pendekatan *Mid-Point Cyrcle*[7]

Algoritma pendekatan pada *mid-point cyrcle* [7] adalah sebagai berikut :

a) Mengkonversi pesan atau gambar kedalam bentuk bilangan biner, kemudian disisipkan ke dalam setiap

bit paling kanan pada setiap bit warna *Red*, *Green* dan *Blue* seperti pada contoh 1 diatas.

b) Menggunakan dimensi (lebar dan tinggi) dari *cover* gambar dan temukan titik (pixel) tengah yang akan digunakan untuk menyembunyikan pesan.
c) Menghitung panjang jari-jari dengan dasar lebar atau tinggi dari cover gambar yang minimal. Kemudian ambil pilih salah satu radius (lebar - 1) atau (tinggi - 1).
d) Seperti ditunjukkan pada Gambar.1, terus cari dan menyimpan pixel dalam sebuah array dengan searah jarum jam yang terletak pada keliling lingkaran dari pusat dan jari-jari lingkaran dengan pendekatan lingkaran titik tengah.
e) Gambar. 2 menunjukkan penyisipan pesan kedalam tiga komponen warna R, G dan B. Dalam satu pixel dapat menyimpan 3 bit pesan. Jika kita memiliki n pixel pada lingkaran, maka banyaknya array 3 * n byte.



Gambar 4. Penyisipan Pesan Kedalam 3 Komponen Warna R, G dan B

f) Ganti 1-bit setiap *byte* pada komponen warna dengan pesan.
g) Untuk mendapatkan kembali pesan yang tersembunyi pada gambar, maka proses yang sama diulang dengan menemukan pixel pada lingkaran yang berisi informasi yang tersembunyi, ekstrak bit yang paling significant dari tiga byte pada setiap pixel. Mengambil secara urutan untuk menemukan kembali pesan yang tersembunyi.

Proses modifikasi pada *least significant bit* diatas adalah penyembunyian pesan pada pixel gambar dengan membentuk sebuah lingkaran. Modifikasi ini akan mempersulit untuk menemukan pesan yang tersembunyi pada pixel sehingga kurang rentan terhadap *steganalysis*. Kekurangan dari modifikasi ini adalah tidak semua pixel dipakai untuk menyembunyikan pesan karena pemilihan pixel membentuk sebuah lingkaran besar dan sampai lingkaran paling kecil, jadi pixel yang berada diluar lingkaran besar tidak akan dipakai untuk menyembunyikan pesan.

B. *Steganalysis* Dan *Cryptanalysis*

Steganografi adalah satu-satunya jawaban untuk komunikasi yang aman dan rahasia. Metode yang ada dalam gambar *steganography* fokus pada peningkatan kapasitas embedding data rahasia[8]. *Steganalysis* merupakan metode yang digunakan untuk mempelajari karakteristik penyembunyian suatu data pada media (*steganography*) dan bagaimana cara untuk mendeteksi bahkan sampai membongkar data tersembunyi tersebut. Metode steganalysis berdasarkan pada Pixel *Mesh Markov Transition Matrix* (PMMTM) [9] yang merupakan metode pengembangan baru yang digunakan untuk mendeteksi biner pada gambar dalam ruang domain *steganography*. Ada juga yang menggunakan statistik citra untuk mendeteksi dua kasus ketika gambar tersembunyi disimpan sebagai salah satu potongan besar (Simple Mode) atau tersebar (Shuffle Mode)[10].

Cryptanalysis merupakan salah satu teknik untuk mencoba memecahkan enkripsi data, biasanya dengan mencari kunci enkripsi. Metode Kasiski merupakan metode pemecahan algoritma *Vigenere cipher* yang dikemukakan pertama kali oleh Friedrich Kasiski ketika dia berhasil memecahkan kriptogram *Vigenere cipher* pada tahun 1863. Namun sebenarnya telah ditemukan sendiri oleh Charles Babbage pada tahun 1846. Metode Kasiski memanfaatkan kelemahan *Vigenere cipher* yang menggunakan kunci yang sama berulang-ulang sehinggan menghasilkan potongan *cipher text* yang sama untuk *plain text* yang sama [1].

C. Teknik Modifikasi *Vigenere Cipher*

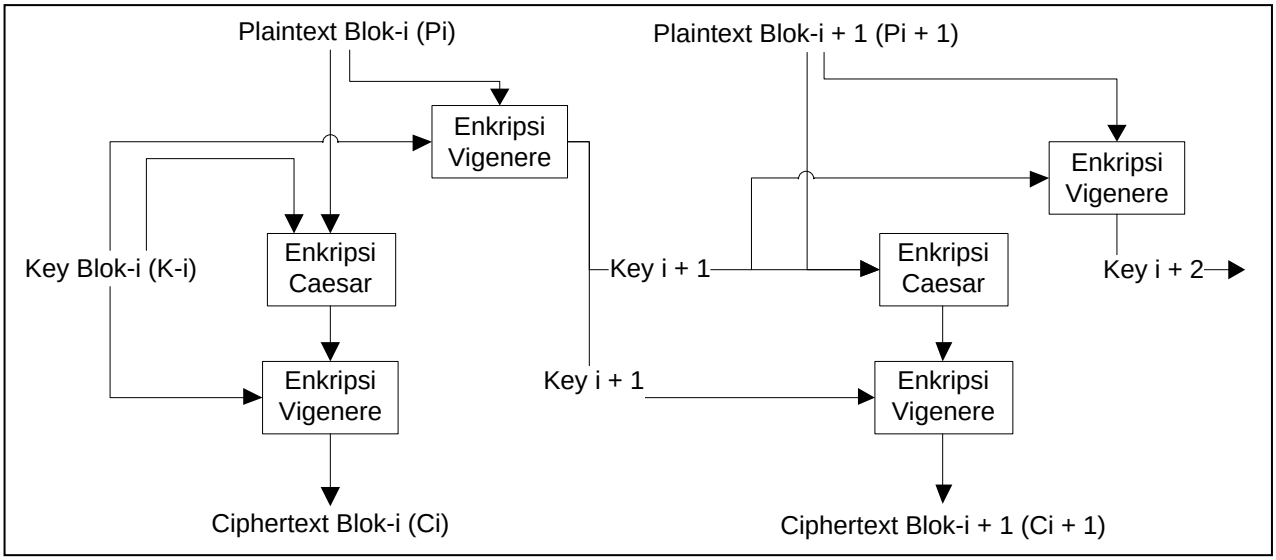
Vigenere cipher merupakan metode enkripsi data *plain text* menjadi *cipher text* dengan menggunakan *key*. Dengan metode kasiski yang sudah dijelaskan pada bagian sebelumnya telah dijelaskan bagaimana cara memecahkan *cipher* yang menggunakan *Vigenere cipher*. Namun, bukan berarti tidak ada hal yang bisa dilakukan untuk memperkuat *Vigenere Cipher* dari serangan *cryptanalysis*. Dapat dilakukan teknik-teknik modifikasi tertentu untuk menyamarkan keterhubungan antara *plain text* dan *ciphertext*-nya. Modifikasi yang dilakukan harus dapat mengurangi kemunculan key yang berulang atau bahkan menggunakan pendekatan *One-Pad* kriptografi yang mana panjang key adalah sama dengan panjang plaintext yang digunakan dimana key akan digenerate berbeda dengan key yang digunakan sebelumnya[1].

Pada penelitian oleh Fatardhi Rizky Andhika, STEI ITB [1], Modifikasi *Vigenere Cipher* dengan Menggunakan *Caesar Cipher* dan Enkripsi Berlanjut untuk Pembentukan *Key*-nya.

1) Modifikasi dilakukan dengan menerapkan enkripsi *Caesar Cipher* yang dibangkitkan dari kunci dan teknik pembangkitkan kunci berikutnya dengan menggunakan enkripsi *Vigenere* berlanjut sehingga kunci yang digunakan untuk pengkodeannya akan berbeda dengan kunci yang digunakan sebelumnya.
2) Dengan penggunaan metode ini, keterhubungan antara *plain text* dan *cipher text* akan akan menjadi semakin berkurang dan semakin sulit untuk dipecahkan kriptanalis.

Modifikasi *Vigenere Cipher* yang dilakukan disini adalah bukan modifikasi pada algoritma utamanya. Bentuk modifikasi yang dilakukan untuk proses enkripsi adalah[1]:

1) *Plain text* dibagi menjadi beberapa blok dengan panjang blok adalah panjang *key* yang digunakan;



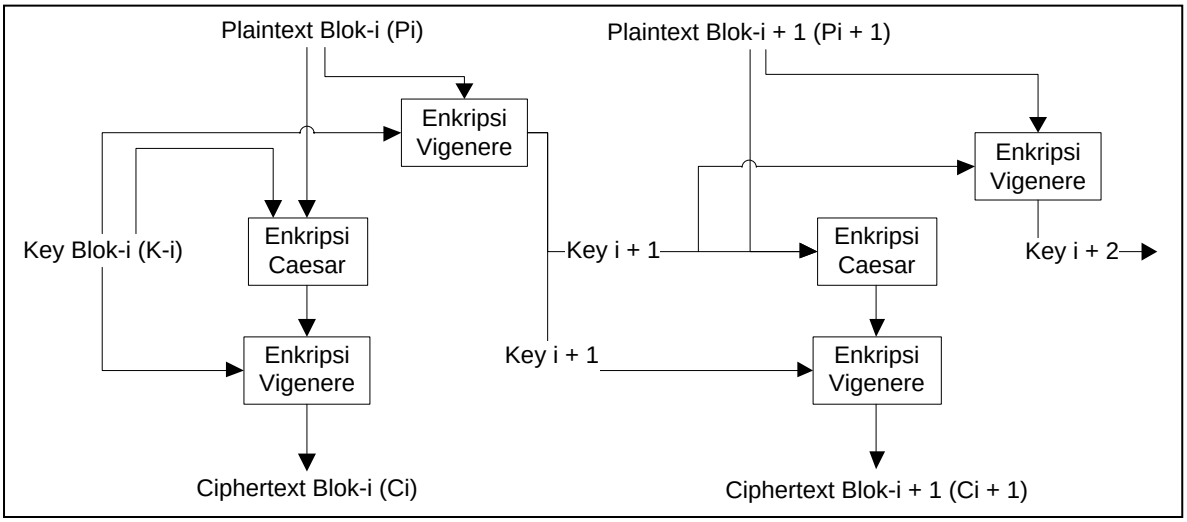
Gambar 5. Skema Enkripsi Modifikasi *Vigenere Cipher*

2) Setiap pemrosesan blok-i akan memiliki key Ki masing-masing yang dibangkitkan berdasarkan blok i-1 sebelumnya. Key Ki merupakan hasil *Vigenere cipher plain text* blok sebelumnya (*plain text* Pi-1) dengan menggunakan key Ki-1. Khusus untuk blok pertama, *key*-nya adalah *key* masukan pengguna;
3) Setiap blok plainteks-i (Pi) akan di-enkripsi terlebih dahulu dengan menggunakan algoritma *Caesar Cipher*. Besar pergeseran *caesar cipher*-nya ditentukan berdasarkan *key* masing-masing blok (Ki) dengan fungsi generatenya adalah : Nilai Caesar = (Ki karakter1 + Ki karakter2 +...+ Ki karakter-n) mod 26;
4) Hasil enkripsi Pi tadi akan dienkripsi menggunakan *vigenere cipher* untuk membentuk *Cipher text* blok-i (Ci) , key yang digunakan adalah Ki.

Dekripsi *vigenere cipher* yang merupakan cara untuk mengembalikan pesan yang dienkripsi menjadi pesan asli atau disebut juga dengan dekripsi *cipher text* menjadi *plain text*. Seperti dijelaskan sebelumnya bahwa dilakukan modifikasi pada enkripsi *vigenere cipher* maka dilakukan juga modifikasi pada proses dekripsi *vigenere cipher*.

Bentuk modifikasi yang dilakukan untuk proses dekripsi adalah sebagai berikut :

1) *Ciphertext* dibagi menjadi blok-blok dengan panjang blok adalah panjang *key* yang digunakan;
2) Setiap pemrosesan blok-i akan memiliki *key* Ki masing-masing yang dibangkitkan berdasarkan blok i-1 sebelumnya. *Key* Ki merupakan hasil *Vigenere cipher plain text* blok sebelumnya (*plain text* Pi-1) dengan menggunakan *key* Ki-1. Khusus untuk blok pertama, *key*-nya adalah *key* masukan pengguna;
3) Setiap *cipher text* blok-i (Ci) akan didekripsi menggunakan *vigenere cipher*, *key* yang digunakan adalah Ki;



Gambar 6. Skema Dekripsi Modifikasi *Vigenere Cipher*

4) Hasil dekripsi yang diperoleh di langkah-3 akan didekripsikan *Caesar Cipher*nya dengan nilai *Caesar Cipher*nya adalah sama dengan pada fungsi enkripsi yang pada akhir langkah ini akan terbentuk blok plainteks-i (Pi).

III. METODE PENELITIAN

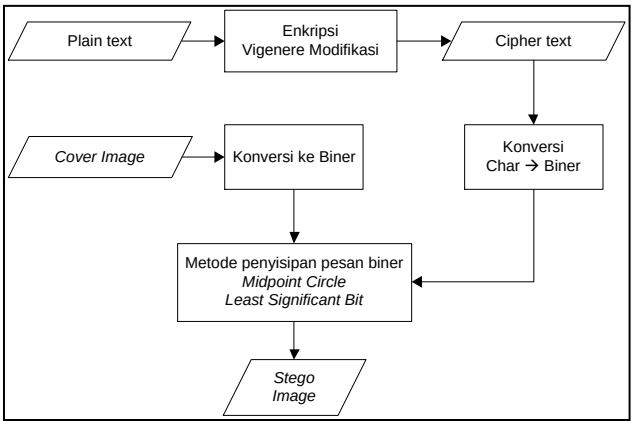
A. Proses Enkripsi Pesan Kedalam *Stego Image*

Proses penyisipan teks ke dalam gambar yang telah dipilih (*cover image*) untuk dikonversi ke dalam format biner, dari nilai pixel tersebut terdiri dari 3 layar RGB (24 bit). Kemudian menggunakan dimensi (panjang dan lebar) pada *cover image* untuk menentukan titik tengah pixel, setelah nilai tengah sudah ditemukan maka proses penyisipan *plaint text*.

Plain text yang akan disisipkan terlebih dahulu di lakukan proses enkripsi pesan dengan menggunakan modifikasi *vigenere chiper* seperti pada Gambar 5 untuk dijadikan sebagai chiper text. Dari hasil enkripsi, *chiper text* tersebut dikonversi ke dalam ASCII kemudian konversi kebiner. proses penyisipan teks dimulai dari tengah atas dan membentuk sebuah lingkaran. Apabila lingkaran tersebut sudah penuh maka lakukan pergeseran pixel dengan menggeser (lebar-1) dan (panjang-1) lihat gambar 3.

Algoritma proses penyembunyian (enkripsi) pesan kedalam *stego image* adalah sebagai berikut :

1) Pertama pesan dienkripsi dengan menggunakan modifikasi *vigenere cipher*, seperti ditunjukkan pada penjelasan sebelumnya atau dapat dilihat pada Gambar 5 Sehingga pesan akan menjadi *cipher text*;
2) Hasil *cipher text* pada no.1 dikonversi kedalam bentuk biner;
3) Sediakan *cover image*, kemudian *cover image* tersebut dikonversi kedalam bentuk biner;
4) Sisipkan setiap bit hasil biner dari pesan kesetiap bit *cover image* dengan menggunakan metode penyisipan pesan *embedding least significant bit*, penggunaan bit untuk penyisipan pesan membentuk sebuah lingkaran seperti dibahas sebelumnya atau dapat dilihat pada Gambar. 1;
5) Sampai hasilnya menjadi dalam bentuk *stego image*.

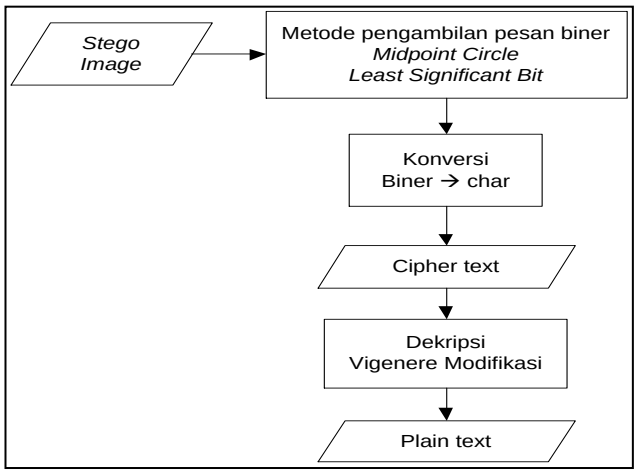


Gambar 7. Proses Enkripsi Pesan Ke *Stego Image*

B. Proses Dekripsi Pesan Dari *Stego Image*

Proses dekripsi pesan dilakukan dengan mengambil pesan yang disimpan *cover image* untuk dikembalikan menjadi pesan asli. Proses algoritma dekripsi pesan dari *stego image* adalah sebagai berikut :

1) *Image stego* dikonversi ke dalam format biner;
2) Dari nilai pixel tersebut ditentukan nilai tengahnya untuk mengambil kembali *chiper text* yang disembunyikan;
3) Setelah nilai tengah sudah ditemukan bit terakhir pada LSB diambil mulai dari posisi tengah atas yang membentuk sebuah lingkaran;
4) Bit yang telah diambil di konversi dalam bentuk *chiper text* yang masih dalam bentuk enkripsi;
5) Gambar. 6 untuk proses deskripsi teks untuk menemukan *plaint text* yang yang sesungguhnya.



Gambar 8. Proses Deskripsi Pesan Dari *Image Stego*

IV. HASIL DAN PEMBAHASAN

Pada penelitian ini, implementasi dilakukan dengan membuat program enkripsi menggunakan bahasa pemrograman VB 2019. Dalam uji coba kasus ini akan dengan dicoba dengan data sebagai berikut :

Plainteks : BILA SAYA BILANG SUKA
Key : MANA

Key digunakan tersebut akan terus *looping* sejumlah teks yang digunakan Pada plainteks. Blok-i huruf tersebut dienkripsi dengan menggunakan enkripsi *caesar chiper* + *key* kemudian dari hasil dilakukan kembali proses enkripsi dengan *enkripsi vigenere* + *key* untuk dijadikan *cipherteks*. Kemudian berlanjut pada blok i+1 berikutnya sampai i = jumlah panjang karakter dari *plain text*. dari *key* diatas akan membentuk kata sepeti :

Plaintext : BILA SAYA BILANG SUKA
Key : MANA MANA MANA MANA MA
Ciphertext : MHXZ YBPT PZQJ WZCX LE

Gambar 9. Implementasi Enkripsi Menggunakan VB.

Dari hasil implementasi *cover image* dimasukan terlebih dahulu kemudian memasukan pesan "BILA SAYA BILANG SUKA" dan *key* "MANA". Sebelum pesan tersebut disembuyikan kedalam *cover image* dilakukan enkripsi menggunakan modifikasi *vigere chiper*. Dari hasil enkripsi data tersebut dikonversi ke dalam biner kemudian disisipkan pada bit terendah yang ada pada *cover image* dengan metode *least significant bit steganography* dengan menggunakan pendekatan lingkaran *midpoint* sehingga dapat meningkatkan keamanan dengan mengurangi kerentanan terhadap *steganalysis*.

Jumlah karakter yang ada pada *key* akan mengikuti jumlah panjang karakter pesan. Apabila jumlah karakter yang ada pada *key* lebih kecil maka *key* akan terus berulang sejumlah teks yang ada pada pesan. Hal ini meningkatkan keamanan data yang akan dienkripsi pada karakter selanjutnya. Pada proses deskripsi *key* yang dimasukan harus sesuai kata pada proses enkripsi. Apabila kata yang dimasukan tidak sesuai akan menghasilkan data acak karena proses deskripsi tidak sesuai dengan *key* sebulumnya.

Hasil pengujian pada penelitian ini dilakukan dengan menggunakan :

1) Laptop lenovo AMD A8
2) Bahasa pemrograman VB 2019

Pada pengujian ini dilakukan dengan menggunakan beberapa *cover image* dengan format BMP dan JPG. hasil ditunjukkan pada Tabel 1. Dari hasil eksperimen yang kami lakukan terlihat bahwa penggunaan *least significant bit* dengan menggunakan pendekatan *midpoint cyrle* lebih mendukung pada format "BMP", karena bitmap terdiri dari susunan titik (pixel) yang pada setiap titiknya diawali satu bit data dan memiliki resolusi yang tinggi sedangkan JPG memiliki media penyimpanan yang terbatas. Perbandingan dari ukuran ke BMP dapat turun menjadi seper sepuluh setelah dikonversi ke JPG. Dari rendahnya pixel tersebut *midpoint cyrcle* mengakibatkan JPG yang akan disisipkan pesan akan mengalami peningkatan kapasitas gambar.

TABEL I
PENGUJIAN DENGAN FORMAT FILE BMP DAN JPG

Cover Image Size (Kb)	Plain text (Karakter)	Stego Image Size (Kb)	Format
558	22	558	BMP
665	60	664	BMP
331	100	334	BMP
8.31	22	148	JPG
11	22	147	JPG
17.1	22	147	JPG

V. KESIMPULAN

Metode *least significant bit steganography* yaitu teknik penyembunyian pesan pada gambar dimana pada penelitian ini menggunakan dua modifikasi yaitu dengan metode *midpoint circle approach* adalah teknik menyembunyikan pesan dalam bentuk lingkaran dan modifikasi enkripsi *vigenere cipher* adalah teknik menyembunyikan pesan sebelum dimasukan pada *cover image*. Hasil dari penggabungan dua metode tersebut dapat diimplementasikan dengan baik namun terdapat kekurangan yaitu pada *midpoint circle approach*, tidak semua pixel pada *cover image* terpakai secara keseluruhan karena metode tersebut membentuk sebuah lingkaran yang mana pixel pada luar lingkaran tersebut tidak digunakan dan terjadi peningkatan ukuran gambar walau tidak signifikan.

REFERENSI

[1] F. R. Andhika, "Modifikasi Vigenere Cipher Dengan Menggunakan Caesar Cipher Dan Enkripsi Berlanjut Untuk Pembentukan Key-Nya" Diakses Pada Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011.

[2] Azlansyah. M dan Setiyono, B, "Penyisipan Pesan Pada Citra Digital Menggunakan Metode Least Significant Bit", Jurnal Sains Dan Seni ITS Vol. 8, No. 1 (2019).

[3] Hafiz, A, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)", Jurnal Cendikia Vol. XVII Cendikia. 2019.

[4] Rachael, O et al, "Image Steganography and Steganalysis Based On Least Significant Bit (LSB)", Proceedings of ICETIT 2019. Lecture Notes in Electrical Engineering, vol 605. Springer, Cham, 2019.

[5] Sharma, P.K and Rajni, "Information Security Through Image Watermarking Using Least Significant Bit Algorithm", Computer Science & Information Technology (CS & IT) pp. 61–67, 2012.

[6] J. Lu, F. Liu, and X. Luo, "Selection Of Image Features For Steganalysis Based On The Fisher Criterion", Digit. Investig., vol. 11, no. 1, pp. 57–66, Mar. 2014.

[7] Verma and R. Chawla, "An Enhanced Least Significant Bit Steganography Method Using Midpoint Circle Approach", International Conference on Communication and Signal Processing, pp. 105–108, 2014.

[8] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color Image Steganography Based On Pixel Value Modification

Method Using Modulus Function", IERI Procedia, vol. 4, pp. 17–24, 2013.

[9] B. Feng, W. Lu, and W. Sun, "Binary Image Steganalysis Based On Pixel Mesh Markov Transition Matrix", J. Vis. Commun. Image Represent., Oct. 2014.

[10] A. Gupta and R. Garg, "Detecting LSB Steganography In Images", Diakses Pada http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.226.2123