JURNAL INFORMATIKA, Vol.7 No.1 April 2020, Halaman 37~45
ISSN: 2355-6579 | E-ISSN**:** 2528-2247

Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi *Least Significant Bit*

Tuti Alawiyah[1], Rian Ardianto[2], Dini Silvi Purnia[3]

[1,2]Universitas Bina Sarana Informatika
e-mail: [1] tuti.tah@bsi.ac.id, [2] ra2321998@gmail.com

[3]STMIK Nusa Mandiri
e-mail: dini.dlv@bsi.ac.id

Abstrak

Kemajuan teknologi diiringi dengan meningkatnya ancaman terhadap keamanan serta kerahasiaan pesan/informasi. Salah satu cara untuk menjaga keamanan dan kerahasiaan pesan/informasi dapat menggunakan teknik steganografi. Steganografi adalah teknik untuk menyembunyikan pesan/informasi pada sebuah media, bisa berupa media gambar, suara ataupun video, sehingga pesan yang disembunyikan sulit dikenali oleh indera manusia. Penelitian ini bertujuan untuk membuat aplikasi steganografi dengan metode least significant bit serta implementasi vigenere cipher untuk meningkatkan keamanan pesan/informasi. Informasi/pesan akan disisipkan pada satu bit paling kanan ke pixel file objek tanpa merubah medianya. Penelitian ini menghasilkan aplikasi yang dapat menyembunyikan informasi/pesan pada media gambar. Untuk meningkatkan sistem pengamanannya, proses deskripsi disertai dengan metode vigenere cipher jika pesan/informasi diakses oleh orang yang tidak berhak atas informasi/pesan tersebut.

Kata kunci: least significant bit, steganografi, vigenere cipher

Abstract

Technological advances are accompanied by increasing threats to the security and confidentiality of message/information. One way to maintain the security and confidentiality of message/information can be using steganography techniques. Steganography is a technique for hiding message/information in a media, it can be in the form of image, sound or video media, so the hidden message is difficult to recognize by the human senses. This study aims to make the application of steganography with the least significant bit method and the implementation of the vigenere cipher to improve message / information security. Information/message will be inserted in the rightmost bit into the pixel file object without changing the media. This research produces an application that can hide information/message on image media. To improve the security system, the description process is accompanied by the vigenere cipher method if the message/information is accessed by people who are not entitled to the information/message.

Keywords*: least significant bit, steganography, vigenere cipher*

Pendahuluan

Dukungan teknologi yang maju saat ini meningkatkan keamanan dalam penyimpanan juga pada proses pertukaran data. Namun, perkembangan teknologi juga membawa ancaman pada kemanan data semakin meningkat. Kebutuhan akan kerahasiaan data dan informasi yang dipertukarkan/disimpan akan semakin meningkat pada setiap aplikasi sistem informasi. Hal-hal yang berkaitan dengan pengamanan data penting harus benar-benar diperhatikan, agar data yang tersimpan dalam komputer tetap aman dari orang-orang yang tidak bertanggungjawab dan orang yang tidak mempunyai wewenang untuk mengakses data tersebut.

Salah satu cara untuk mengamankan data adalah dengan menyembunyikan data tersebut paa sebuah media, sehingga data yang disembunyikan sulit dikenali oleh indra manusia. Pengamanan seperti ini disebut dengan steganografi. Penyisipan informasi

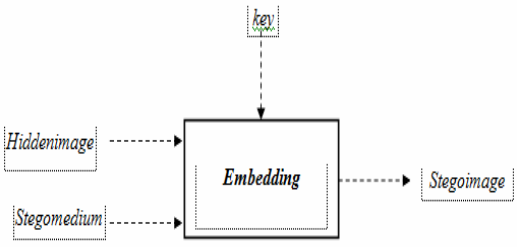
menggunakan teknik steganografi dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai bahan medianya seperti format teks, format gambar, bahkan untuk format audio dan sebagainya, asalkan file-file tersebut mempunyai bit-bit data redundansi yang dapat dimodifikasi.

Menurut (Monalisa, 2014) menyatakan bahwa: Steganografi adalah jenis komunikasi yang tersembunyi yang secara harfiah berarti "tulisan tertutup". Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang populer untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal.

Steganografi memiliki dua proses yaitu proses penyisipan pesan dan proses pengembalian pesan. Proses penyisipan pesan membutuhkan masukan media penyisipan pesan yang akan disisipkan beserta kunci. Keluaran dari proses penyisipan ini adalah media yang telah berisi pesan. Sedangkan proses pengembalian pesan membutuhkan masukan media yang telah berisi pesan. Keluaran dari proses pengembalian pesan adalah pesan yang telah disisipkan.

Menurut (Adiputra Sejati, 2010) dalam jurnal (Lilyani, 2014) Proses Steganografi tersebut dapat diilustrasikan pada gambar berikut:

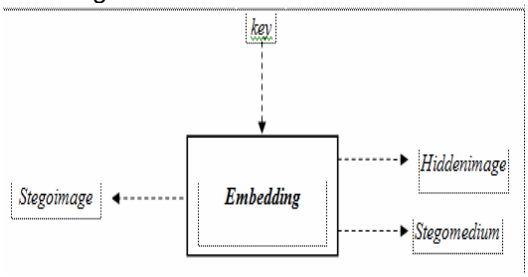
1) Proses *embedding*, yakni proses penyembunyian pesan dimana pada bagian pertama dilakukan proses *embedding hidden image* yang hendak disembunyikan ke dalam *stegomedium* sebagai media penyimpanan, dengan memasukkan kunci (*key*), sehingga dihasilkan media dengan data tersembunyi di dalamnya (*stegoimage*).



Sumber: (Lilyani, 2014)

Gambar 1. *Embedding* Citra

2) Proses ekstraksi pada *stegoimage* dengan memasukkan *key* yang sama sehingga didapatkan kembali *hidden image.*



Sumber: (Lilyani, 2014)

Gambar 2. Ekstraksi Citra

Menurut Munir, Rinaldi (2006) dalam jurnal (Rahimah, 2014) “Metode LSB (Least Significant Bit), merupakan metode yang bekerja pada bit yang terendah dari suatu deretan bit bit data. Penggunaan LSB ini dengan menyisipkannya pada bit rendah atau bit yang paling kanan (lsb) pada data pixel yang menyusun gambar tersebut. Seperti di ketahui untuk file bitmap 24 bit di setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing–masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111”.

Menurut (Sulistyanto, 2015) mengemukakan bahwa: “bit atau *binary digit* adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 (nol) atau 1 (satu). Semua data di dalam komputer di simpan kedalam satuan bit, termasuk gambar, suara maupun video. Format pewarnaan di dalam citra gambar seperti *monochrome*, *grayscale*, RGB, CMYK juga menggunakan satuan bit dalam penyimpanannya. Sebagai contoh pewarnaan *monochrome* bitmap (menggunakan 1 bit untuk setiap pikselnya), RGB – 24 bit (8 bit red, 8 bit green, 8 bit blue), *grayscale* menggunakan 8 bit untuk menentukan tingkat kehitaman suatu piksel”.

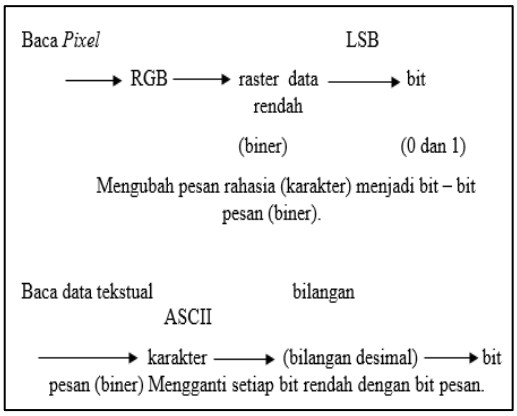
Menurut (Rakhmat & Fairuzabadi, 2010) dalam jurnal (Sa’id & Wijanarto, 2015) menjelaskan bahwa “Least Significant Bit terletak paling kanan dari barisan bit. Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai

byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya".

Menurut (Cahyadi, 2012) menyimpulkan bahwa "untuk menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam cover dengan bit-bit data rahasia. Untuk menyembunyikan suatu gambar dalam LSB pada setiap byte dari gambar 24-bit, dapat disimpan 3 byte dalam setiap pixel".

langkah-langkah penyelesaian metode steganografi least significant bit menurut (Setiani, 2008) adalah sebagai berikut:

a. Algoritma metode penyisipan data tekstual ke dalam data citra.
   Mengubah setiap pixel (satu dot atau elemen dari raster) gambar asli menjadi raster (bentuk Array yang mengandung dot / titik) data dengan cara seperti yang tampak pada Gambar 1.



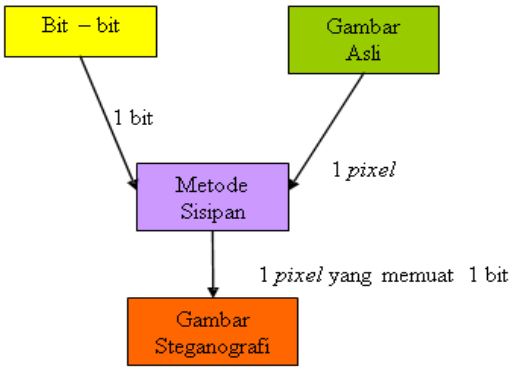
Sumber (Setiani, 2008)

Gambar 3. Algoritma Penyisipan Data

   Jika bit rendah = bit pesan, maka raster data tidak berubah
   Jika bit rendah < bit pesan, maka data ditambah 1
   Jika bit rendah > bit pesan, maka raster data dikurangi 1
   Lalu menulis pixel yang baru sesuai dengan raster data:
   Raster data ➔ RGB ➔ Pixe

b. Algoritma metode ekstraksi data tekstual dari media penyimpanan data citra.
   Setiap pixel citra steganografi diubah menjadi raster data agar memperoleh bit rendah. Prosesnya sama dengan tahap pertama metode penyisipan. Bit rendah setiap pixel dikumpulkan hingga terbentuk bit stream. Arah bacanya adalah atas ke bawah dan kiri ke kanan. Setiap 8 bit stream merepresentasikan sebuah karakter. Setelah semua bit stream diubah menjadi karakter, akan diperoleh data teks yang tersembunyi di antara kumpulan karakter.

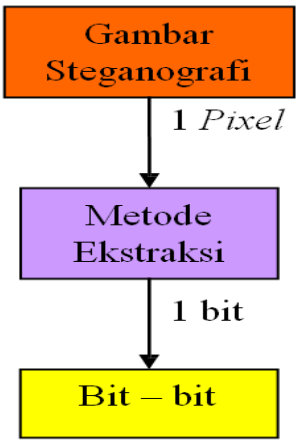
c. Metode penyisipan teks ke dalam data citra



Sumber (Setiani, 2008)

Gambar 4. Diagram Penyisipan Data

d. Metode ekstraksi data tekstual dalam citra.



Sumber (Setiani, 2008)

Gambar 5. Diagram Ekstraksi Pada Data Citra

Vigenere cipher adalah pengembangan dari metode algoritma kriptorafi caesar cipher, yang berfungsi menyandikan teks alfabet berdasarkan huruf-huruf pada kata kunci dengan menggunakan deretan sandi caesar.

Menurut (Arjana, Rahayu, Yakub, & Hariyanto, 2012) teknik dari substitusi *vigenere cipher* bisa dilakukan dengan dua cara: yaitu *Vigenere Cipher* dengan angka dan *Vigenere Cipher* dengan huruf

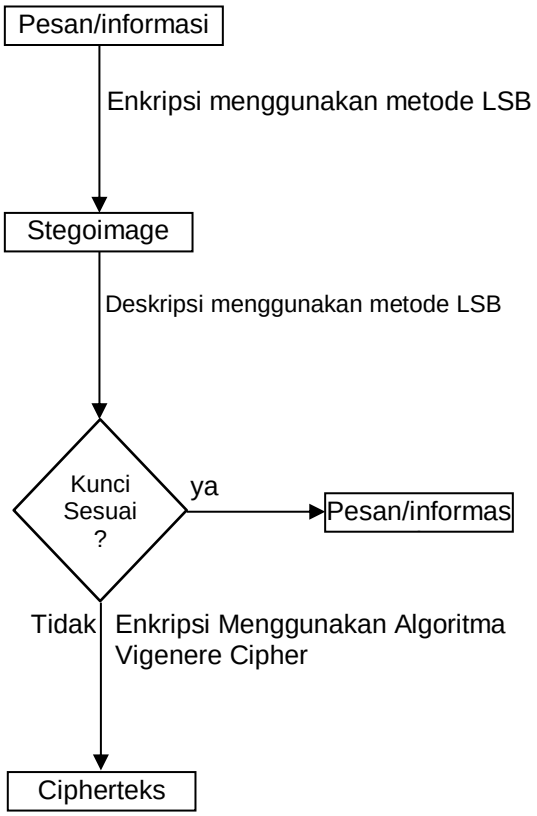
Tujuan dari penelitian ini, adalah:

a. Menjaga kerahasiaan pesan, sehingga hanya orang yang memiliki otoritas terhadap data yang disandikan yang dapat membaca pesan.

b. Implementasi teknik steganografi untuk pengamanan data dengan metode algoritma *Least Significant Bit* (LSB).
c. Dapat menerapkan teknik steganografi least significant bit pada setiap proses enkripsi dan deskripsi untuk menjaga agar informasi yang disampaikan tetap terjaga keamanan dan kerahasiaannya.
d. Merancang sebuah aplikasi desktop penyisipan pesan berupa teks kedalam citra digital.

1. Metode Penelitian

Penelitian ini menerapkan metode Steganografi *least significant bit* (LSB) untuk mengamankan data, serta penggunaan algoritma vigenere cipher dalam proses deskripsi jika yang melakukan deskripsi bukan orang yang berhak atas data tersebut (kunci yang dimiliki tidak sesuai).



Gambar 6. Tahapan Pengamanan Data

Hasil dan Pembahasan

1. Kebutuhan Pengguna

a. Pengguna dapat membuat akun untuk bisa masuk ke menu utama dan mendapatkan kunci.
b. Pengguna dapat mengubah kata sandi akun.
c. Pengguna dapat menghapus akun yang tidak digunakan.
d. Pengguna dapat melakukan proses enkripsi.
e. Pengguna dapat melakukan proses deskripsi.
f. Pengguna dapat mengelola riwayat direktori setelah proses enkripsi.

2. Kebutuhan Sistem

a. Sistem dapat melakukan proses enkripsi pada media gambar dengan sedikitnya perubahan yang timbul terhadap media (Hide Host) tersebut menggunakan metode Least Significant Bit (LSB) yang memodifikasi pada pasangan piksel tertentu dan menerapkan 4 aturan penyisipan. Aturan dalam penyisipan pesan menggunakan algoritma LSB memiliki persamaan sebagai berikut:
   1) Jika mi sama dengan xi dan jika m(i+1) tidak sama dengan f([xi/2]+xi+1) maka nilai dari piksel y(i+1) sama dengan xi+1 ditambah 1 atau dikurang 1 secara acak dengan ketentuan jika 255 tidak bisa ditambah 1 dan jika 0 tidak dapat dikurangi 1, dan nilai piksel yi sama dengan nilai xi.
   2) Jika mi sama dengan xi dan jika mi+1 sama dengan f([xi /2]+xi+1 maka nilai dari piksel yi+1 sama dengan xi+1, dan nilai piksel yi sama dengan nilai xi.
   3) Jika mi tidak sama dengan xi dan mi+1 sama dengan xi+1 maka nilai dari piksel yi sama dengan nilai piksel xi dikurangi 1 dan nilai piksel yi+1 sama dengan nilai dari xi+1.
   4) Jika mi sama dengan xi dan mi+1 tidak sama dengan xi+1 maka nilai dari piksel yi sama dengan nilai piksel xi ditambah 1 dan nilai piksel yi+1 sama dengan nilai dari xi+1.

x_i	x_{i+1}	x_i	x_{i+1}	m_i	m_{i+1}
162	150	10100010	10010110	0	0

y_i	y_{i+1}	y_i	y_{i+1}
162	151	10100010	10010111

x_i	x_{i+1}	x_i	x_{i+1}	m_i	m_{i+1}
162	150	10100010	10010110	0	1

y_i	y_{i+1}	y_i	y_{i+1}
162	150	10100010	10010110

x_i	x_{i+1}	x_i	x_{i+1}	m_i	m_{i+1}
162	150	10100010	10010110	1	0

y_i	y_{i+1}	y_i	y_{i+1}
161	150	10100001	10010110

x_i	x_{i+1}	x_i	x_{i+1}	m_i	m_{i+1}
162	150	10100010	10010110	1	1

y_i	y_{i+1}	y_i	y_{i+1}
163	150	10100011	10010110

Gambar 7. Proses Penyisipan

b. Sistem dapat melakukan proses deskripsi pada menu deskripsi.
Pengambilan pesan (Unhide) dengan metode LSB Setelah melakukan proses merahasiakan pesan, maka akan diuji apakah pesan dapat diambil kembali. Untuk lebih memahami proses pengambilan pesan pada metode yang diusulkan ini, maka akan diberikan potongan dari piksel citra sebagai ilustrasi dari proses pengambilan pesan dengan menggunakan steganografi LSB. Aturan dalam pengambilan pesan menggunakan steganografi LSB memilki persamaan sebagai berikut :
   1) mi sama dengan yi.
   2) mi+1 sama dengan f([0,5.yi] + yi+1).

162	150
x_i	x_{i+1}

y_i	y_{i+1}	LSB(y_i)	f (y_i, y_{i+1})
162	151	0	0
162	150	0	1
161	150	1	0
163	150	1	1

Gambar 8. Proses Pengambilan

c. Jika seorang pengguna melakukan deskripsi pada file hasil enkripsi pengguna lain, maka teks yang sudah dideskripsi oleh metode LSB akan dienkripsi menggunakan Vigenere Cipher sehingga menghasilkan Chypertext. Dalam proses enkripsi menggunakan algoritma vigenere cipher dengan persamaan ci= (pi + ki) mod 128.

Input	Data *.txt yang akan dienkripsi
Output	Data *.txt yang telah dienkripsi
Proses	Panjangtekslength(p)// memeriksa panjang plainteks For 1 to panjangText // menyamakan panjang k dengan panjang p Huruf[i] M[i] nilaiASCII[i] For 1 to panjangText // menyamakan panjang k dengan panjang p i mod 128 =1? c = (p + k) mod128 Cetak char (c) c = Cipherteks

Gambar 9. Algoritma Enkripsi

Berikut adalah proses enkripsi vigenere cipher:
1) Pesan yang dijadikan p di baca panjang elementnya.
2) Kemudian kunci dibaca panjang elementnya k dan di looping sesuai panjang element p.
3) Setelah panjang element k sama dengan p, maka k di ubah ke bilangan ascii lalu di susun menjadi seperti p.
4) Lalu p dan k di oprasikan dengan persamaan enkripsi vigenere cipher. Pada tabel 4 dan tabel 5 dibawah ini adalah p dan k pada f(1,1) sampai f(1,8).

	f(1,1)	f(1,2)	f(1,3)	f(1,4)	f(1,5)	f(1,6)	f(1,7)	f(1,8)
p	v	i	g	e	n	e	r	e
k	f	a	s	a	f	a	s	a

Gambar 10. Karakter p, k, dan c pada f(1,1) sampai f(1,8)

	f(1,1)	f(1,2)	f(1,3)	f(1,4)	f(1,5)	f(1,6)	f(1,7)	f(1,8)
p	118	105	103	101	110	101	104	101
k	102	97	115	97	102	97	115	97

Gambar 11. Nilai ASCII p, k, dan c pada f(1,1) sampai f(1,8)

Dari *p* dan *k* diatas maka *c* dapat diketahui dengan pengoprasian sebagai berikut:

c (1,1) = (118 + 102) mod 128 = 92
c (1,2) = (105 + 97) mod 128 = 74
c (1,3) = (103 + 115) mod 128 = 90
c (1,4) = (101 + 97) mod 128 = 70
c (1,5) = (110 + 102) mod 128 = 84
c (1,6) = (101 + 97) mod 128 = 70
c (1,7) = (104 + 115) mod 128 = 101
c (1,8) = (101 + 97) mod 128 = 70

Hasil dari operasi dengan persamaan vigenere cipher dalam bentuk kode ascii akan dikembalikan lagi dalam bentuk karakter adalah sebagai berikut:

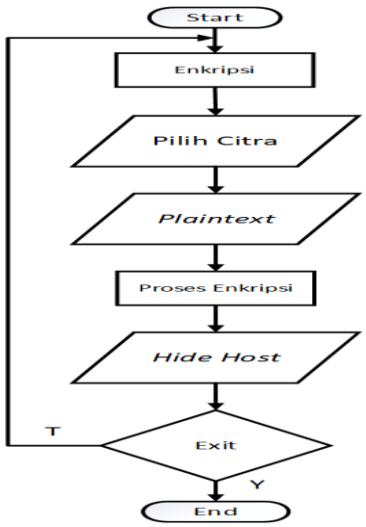
	f(1,1)	f(1,2)	f(1,3)	f(1,4)	f(1,5)	f(1,6)	f(1,7)	f(1,8)
c	92	74	90	70	84	70	101	70
	\	J	Z	F	T	F	e	F

Gambar 12. Hasil Operasi dengan Persamaan *Vigenere Cipher.*

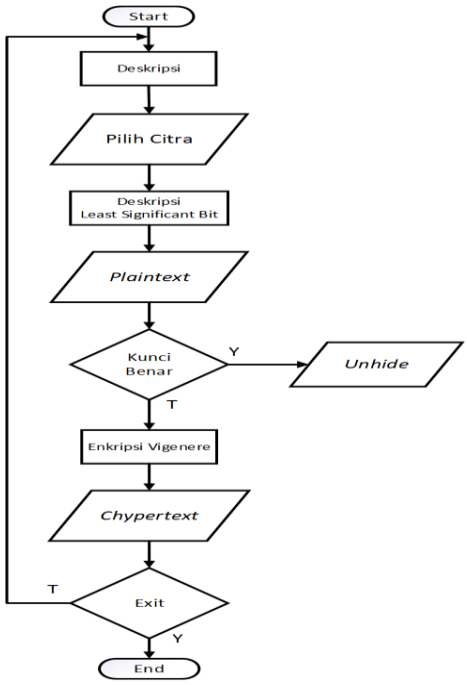
File yang sudah dienkripsi dengan vigenere cipher tidak bisa dideskripsi menjadi pesan asli.

d. Sistem memiliki kunci untuk setiap pengguna berdasarkan nama pengguna tersebut saat ketika masuk menu utama yang berfungsi untuk meminimalisir pengembalian data yang tidak memiliki wewenang terhadap pesan yang diamankan.
e. Sistem mampu menampilkan hasil proses enkripsi berupa informasi penyimpanan data dari menu riwayat direktori setiap pengguna.

3. Flowchart



Gambar 13. *Flowchart* Enkripsi

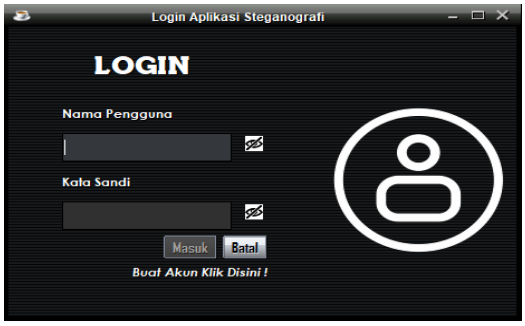


Gambar 14. *Flowchart* Deskripsi

4. Implementasi

a. Form Login

Form login ini berfungsi sebagai fasilitas seorang pengguna untuk dapat masuk ke dalam menu utama aplikasi steganografi. Jika pengguna akan masuk, maka harus memasukan nama pengguna dan kata sandi ditempat yang telah disediakan. Setelah nama pengguna dan kata sandi telah dimasukan, pengguna harus menekan tombol masuk jika sesuai maka akan menuju tampilan menu utama.



Gambar 15. Implementasi Form Login

b. Form Buat Akun

Form buat akun ini berfungsi sebagai fasilitas seorang pengguna untuk dapat masuk ke dalam menu utama setelah melalui form login aplikasi steganografi. Jika pengguna akan masuk, dan belum memiliki akun maka harus membuat akun terlebih dahulu. Masukan nama pengguna, kata sandi, dan nama ditempat yang telah disediakan. Setelah data terisi dengan lengkap, pengguna harus menekan tombol simpan jika sesuai maka akan ada pemberitahuan, selanjutnya menekan tombol kembali untuk menuju form login supaya bisa masuk ke form menu utama.

Gambar 16. Implementasi Form Buat Akun

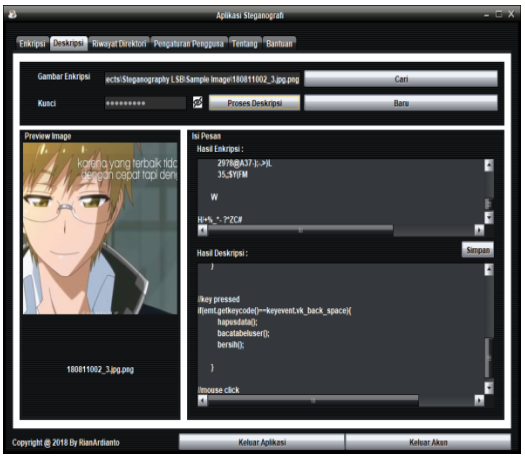
c. Form Enkripsi

Pada tampilan form enkripsi berfungsi untuk menyisipkan pesan ke dalam media gambar. Terdapat tombol cari untuk memilih media gambar dan pesan yang akan dipilih pada penyimpanan data, kunci sudah otomatis ada berdasarkan nama pengguna, sedangkan nama gambar diisi untuk menduplikasi gambar asli sehingga gambar yang telah tersisipi pesan terlihat berbeda dengan gambar asli. Bila sudah maka tinggal menekan tombol proses enkripsi. Jika ingin melakukan proses data enkripsi lagi maka tekan tombol baru.

Gambar 17. Implementasi Form Enkripsi

d. Form Deskripsi

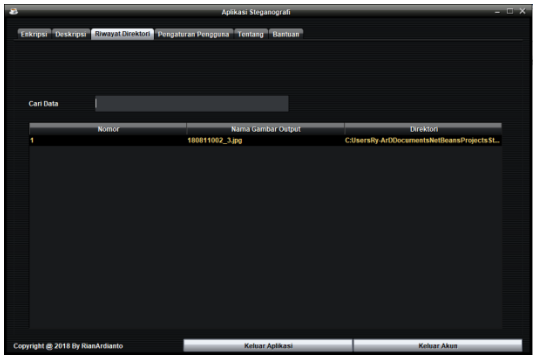
Pada tampilan form deskripsi berfungsi untuk mengembalikan pesan yang telah disisipkan ke dalam media gambar. Terdapat tombol cari untuk memilih media gambar yang telah disisipkan pesan, kunci sudah otomatis ada berdasarkan nama pengguna, selanjutnya tekan tombol proses deskripsi. Jika ingin melakukan proses dekripsi lagi tekan tombol baru, lalu melakukan pada langkah yang sama sebelumnya. Sedangkan tombol simpan untuk menyimpan pesan deskripsi yang telah terpisahkan dengan media gambar.



Gambar 18. Implementasi Form Deskripsi

e. Form Riwayat Direktori

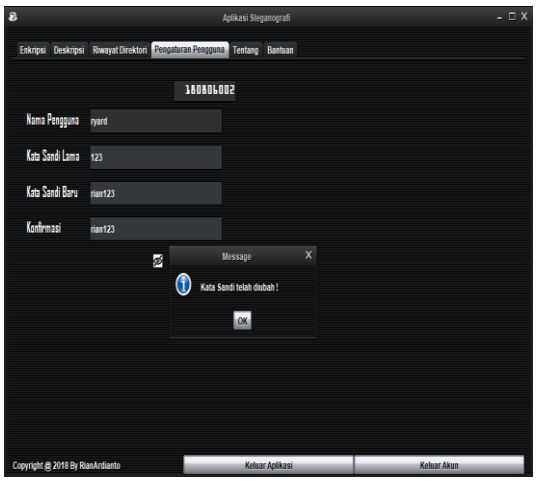
Pada riwayat direktori terdapat tampilan berupa informasi data nama gambar yang telah disisipkan beserta alamat penyimpanan data penting, yang setiap pengguna berbeda riwayat berdasarkan nama pengguna saat login.



Gambar 19. Implementasi Riwayat Direktori

f. Form Pengaturan Pengguna

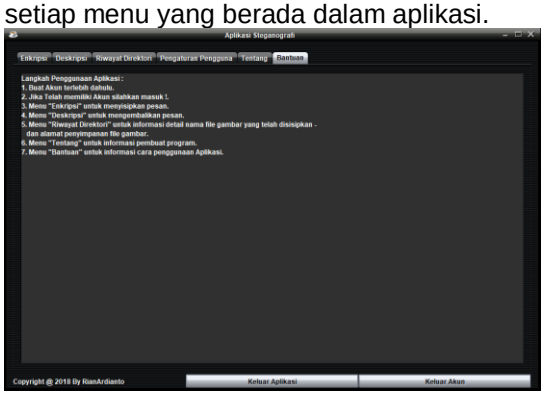
Pada tampilan pengaturan pengguna terdapat fungsi berupa data pengguna saat akan diubah kata sandi beserta konfirmasi kata sandi dan terdapat tombol yang berfungsi untuk membuang akun jika sudah tidak diperlukan.



Gambar 20. Implementasi Pengaturan Pengguna

g. Form Bantuan

Pada tampilan Form Bantuan menampilkan informasi cara penggunaan aplikasi berupa detail kegunaan isi dari setiap menu yang berada dalam aplikasi.



Gambar 21. Implementasi Form Bantuan

Kesimpulan

Berdasarkan pembahasan yang telah diuraikan, maka Peneliti mendapat kesimpulan sebagai berikut: (1). Hasil dari penerapan untuk penyisipan pesan rahasia pada gambar berjalan dengan baik. Pesan atau dokumen yang disisipkan pada file gambar dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses enkripsi dan setelah proses dekripsi mempunyai hasil yang sama tanpa ada perubahan pesan atau gangguan, (2). Proses perbaikan citra yang disisipi dengan gambar awal sebelum disisipkan pesan teks tidak mengalami perubahan bentuk, sehingga secara kasat mata tidak dapat diketahui apakah ada pesan didalam gambar tersebut dan output gambar hasil enkripsi mengalami perubahan ukuran file gambar, (3). Penggabungan teknik algoritma vigenere cipher dan steganografi menggunakan least significant bit (LSB) memiliki hasil citra dengan baik dapat membantu menjaga kerahasiaan pesan karena orang yang tidak mengetahui kunci rahasia yang digunakan akan kesulitan untuk mendapatkan pesan yang terdapat pada stego-image. Walaupun orang tersebut dapat mengambil pesan pada stego-image, namun pesan tersebut masih berupa ciphertext sehingga perlu mencari kunci untuk mendekripsikannya.

Referensi

Arjana, P. H., Rahayu, T. P., Yakub, & Hariyanto. (2012). *Implementasi enkripsi data dengan algoritma*. *2012*(Sentika), 164–169.

Cahyadi, T. (2012). Implementasi steganografi lsb dengan enkripsi vigenere cipher pada citra jpeg. *Universitas Diponegoro Semarang*, *1*.

Lilyani, D. (2014). *IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE DYNAMIC CELL SPREADING*. (0911074), 1–8.

Monalisa, S. H. (2014). *STEGANOGRAFI PADA FILE CITRA UNTUK PENGAMANAN DATA*. (1011690), 75–79.

Rahimah. (2014). Implementasi Penyembunyian Dan Penyandian Pesan Pada Citra Menggunakan Algoritma Affine. *Pelita Informatika Budi Darma*, *VI*(1), 144–148.

Rakhmat, B., & Fairuzabadi, M. (2010).

Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4. *5*(September), 1–17.

Sa'id, F., & Wijanarto. (2015). *Implementasi algoritma vigenere dan metode lsbmr pada citra diam 1,2*. *14*(3), 189–197.

Setiani, Y. (2008). *Pembuatan aplikasi steganografi menggunakan matlab 7.0*.

Sulistyanto, A. (2015). *Aplikasi Steganografi dengan Metode LSB dan Enkripsi Pesan dengan Pembangkitan Bilangan Acak*.