JOURNAL OF INFORMATICS, BUSSINES, EDUCATION, AND INNOVATION TECHNOLOGY

Implemetasi Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit Dengan Kriptografi Super Enskripsi

Implementation of Steganography in Digital Images Using the Least Significant Bit Method with Super Encryption

Virgienia V.R Kaunang[1], Arje C. Djamen[2], Quido C. Kainde[3]

[1,2,3] Fakultas Teknik, Universitas Negeri Manado, Sulawesi Utara, Indonesia

Article Info

Article history:
Received: Feb 09, 2024
Revised: March 20, 2024
Accepted: Apr 28, 2024

Kata kunci
Super Enkripsi, Steganografi, Citra Digital, *Cipher text*, *Plain text*, *key*, *Stego Image*, *Vigenere Cipher*, *Advanced Encryption Standard*, *Least Significant Bit*.

ABSTRAK

Super Enkripsi merupakan salah satuh satu teknik kriptografi dengan menggabungkan dua atau lebih dari satu algoritma *cipher* dengan tujuan untuk menciptakan *cipher text* yang lebih kuat. Kriptografi sendiri umumnya merupakan suatu teknik untuk mengubah pesan menjadi kode - kode acak agar tidak diketahui pihak lain yang tidak diinginkan. kriptografi memiliki berbagai macam bentuk metode dan algoritma, dua diantaranya adalah Algoritma *vigenere cipher* dan *Advanced Encryption Standard* (AES). Pesan yang berupa teks dapat di enkripsi menggunakan *key* atau kunci dengan menggunakan teknik super enkripsi dari gabungan *vigenere cipher* dan algoritma *Advanced Encryption Standard* (AES). Steganografi merupakan suatu teknik untuk menyembunyikan informasi atau data pada suatu media atau berkas. Steganografi juga memiliki beberapa metode algoritma yang dapat diimplementasikan dalam prosesnya, salah satunnya yaitu metode *Least Significant Bit* (LSB). Penelitian ini bertujuan untuk membuat suatu program atau aplikasi yang dapat menyisipkan teks yang sudah terenkripsi menggunakan teknik Super Enkripsi ke dalam suatu berkas media gambar atau citra digital menggunakan teknik Steganografi dengan algoritma Least Significant Bit (LSB). Program yang dibuat dengan Super Enkripsi dan Steganografi ini berhasil menghasilkan Gambar *Stego* atau Berkas Gambar yang sudah dimodifikasi dan disisipkan pesan tersandi ke dalamnya. Gambar *Stego* tersebut dapat di muat kembali dalam program lalu mengekstrak teks tersandi yang kemudian dilakukan proses dekripsi teks sandi tersebut agar mendapatkan teks asli yang di inginkan berdasarkan *key* yang dimasukkan pengguna.

Keywords
Super Encryption, Steganography, Digital Image, Cipher text, Plain text, key, Stego Image, Vigenere Cipher, Advanced Encryption Standard, Least Significant Bit.

ABSTRACT

Super Encryption is one of the cryptographic techniques that combines two or more cipher algorithms with the aim of creating a stronger ciphertext. Cryptography itself is generally a technique to transform messages into random codes to prevent unauthorized parties from understanding them. Cryptography has various forms of methods and algorithms, two of which are the Vigenere cipher algorithm and the Advanced Encryption Standard (AES). Text messages can be

encrypted using a key or passphrase using the super encryption technique, which combines the Vigenere cipher and the Advanced Encryption Standard (AES) algorithm. Steganography is a technique used to hide information or data within a medium or file. Steganography also has several algorithmic methods that can be implemented in its process, one of which is the Least Significant Bit (LSB) method. This research aims to create a program or application that can embed encrypted text using the Super Encryption technique into an image or digital image file using the Steganography technique with the Least Significant Bit (LSB) algorithm. The program developed with Super Encryption and Steganography successfully generates a modified image or stego image with the encrypted message embedded in it. The stego image can be loaded back into the program to extract the embedded encrypted text, which can then undergo a decryption process to obtain the desired original text based on the user-entered key.

Corresponding Author:
Arje C. Djamen ST.,MT,
Informatics Engineering Study Program and Faculty of Engineering
Manado State University
Tataaran Satu, South Tondano, Minahasa, North Sulawesi, Indonesia
Email: arjedjamen@unima.ac.id

PENDAHULUAN

Seiring dengan berkembangnya teknologi yang begitu pesat memudahkan seseorang untuk menyampaikan pesan kepada orang lain secara instan. Berbagai cara untuk menyampaikan pesan pun semakin beragam contohnnya menggunakan Surat elektronik atau aplikasi pesan instan. Dalam kegiatan saling berkirim pesan, penyadapan bisa saja terjadi, terlebih ketika informasi yang hendak disampaikan bersifat rahasia dan penting sehingga aspek penting dalam pengiriman data dan informasi digital adalah masalah keamanan.

Pesan berbentuk digital dapat berupa berkas text, gambar, suara maupun video atau pun gambar bergerak. Penerapan keamanan suatu pesan digital menjadi hal yang penting untuk di lakukan. Pesan dapat disisipkan dalam suatu media digital. Hal ini bertujuan supaya orang lain tidak dapat mengetahui isi informasi rahasia yang tersimpan di dalam pesan digital yang ditujukan untuk penerima.

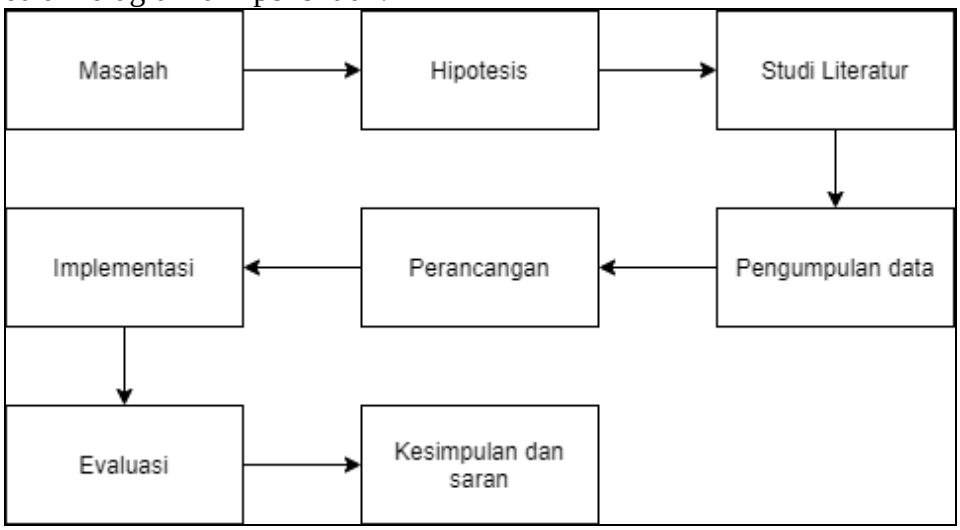
Salah satu cara yang dapat digunakan untuk mengamankan data digital ini adalah dengan memanfaatkan Steganografi dan Kriptografi. Steganografi merupakan seni untuk menyelundupkan atau menyembunyikan suatu infromasi, dimana informasi tersebut disisipkan dalam suatu media atau bisa juga citra digital yang tampak seperti biasa saja. Teknik dalam Steganografi memiliki beberapa metode untuk menyisipkan suatu pesan tersembunyi, salah satunya menggunakan metode LSB (Least Significant Bit). Metode ini merupakan metode steganografi yang sederhana dan mudah dimplementasikan. Metode ini menyembunyikan pesan dalam bit terendah pada citra digital yang digunakan sebagai wadah penampung pesan.

Kriptografi sendiri merupakan teknik untuk mengubah pesan menjadi kode-kode yang tidak diketahui maksudnya, sehingga pihak lain yang tidak diinginkan akan kesulitan untuk menerjemahkan isi pesan.

Berdasarkan latar belakang tersebut maka dilakukan penelitian dengan menggabungkan algoritma kriptografi Super Enkripsi dan steganografi LSB. Penelitian ini akan diberi judul Implementasi Steganografi pada Citra Digital menggunakan Metode Least Significant Bit dengan Kriptografi Super Enkripsi.

METODE PENELITIAN

Saat menjelaskan suatu masalah, kerangka pemikiran atau alur penelitian disajikan untuk memudahkan pemahaman dalam penelitian. Metode tersebut disajikan dalam diagram alir penelitian.



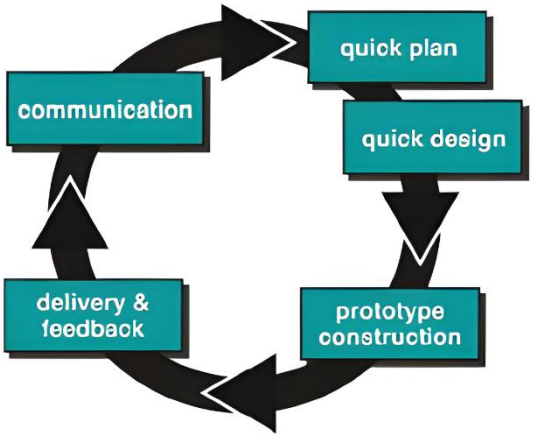
Gambar 1.Kerangka pikir penelitian

Penelitian ini diawali dengan sebuah permasalahan yang muncul dan sebuah hipotesis atau jawaban sementara terhadap masalah yang hendak diteliti. Masalah yang diteliti, yaitu Bagaimana cara mengimplementasikan metode super enkripsi pada pesan atau berkas teks serta Bagaimana cara menyisipkan pesan teks yang sudah ter-enkripsi pada citra digital dengan implementasi metode *Least Significant Bit* (LSB) dalam teknik Steganografi. Untuk menyelesaikan masalah tersebut terdapat sebuah hipotesis, yakni dengan Membuat program steganografi yang mengimplementasikan metode *Least Significant Bit* (LSB) dan dan menggabungkan dua metode enkripsi (Super Enkripsi) pada citra digital. Setelah mengetahui hipotesis dari masalah yang hendak diteliti, maka tahap selanjutnya adalah melakukan studi literatur yang didasarkan pada masalah dan hipotesis yang ada, di mana pada tahap ini akan ditelusuri berbagai macam literatur yang berkaitan dengan Steganografi, metode LSB, metode enkripsi dan penelitian yang hendak dilakukan. Tahap selanjutnya adalah tahap pengumpulan data. Pada tahap ini, data yang digunakan merupakan berkas citra digital yang diambil dari *google images*. Selanjutnya, tahap perancangan merupakan tahap di mana akan dirancang aliran proses dari sistem yang akan dibangun. Setelah tahap perancangan, maka terdapat tahap implementasi atau tahap pengkodean untuk melaksanakan segala rancangan yang telah dibuat pada program yang akan dibangun dan pada akhirnya terdapat tahap evaluasi untuk menguji sistem yang telah berhasil dibangun. Tahap terakhir dari penelitian adalah tahap kesimpulan dan saran, di mana pada tahap ini akan ditarik kesimpulan dari penelitian yang telah dilakukan apakah sistem yang dibangun dapat memecahkan

permasalahan yang ada atau tidak dan apakah tujuan dari penelitian yang dilakukan tercapai atau tidak, serta saran untuk mengembangkan penelitian ini kedepannya.

Metode Pengembangan

Dalam mengembangkan system ini, penulis menggunakan metode pengembangan *Prototyping*, Prototyping adalah teknik untuk mengumpulkan informasi tertentu secara cepat tentang kebutuhan informasi pengguna. Fokus pada penyajian aspek perangkat lunak yang akan terlihat oleh pelanggan atau pengguna. Prototipe akan dievaluasi oleh pelanggan/pengguna dan digunakan untuk menyaring kebutuhan pengembangan perangkat lunak.



Gambar 2. Model *Prototyping*

Gambar 2 menunjukkan langkah-langkah dari model prototyping. Langkah pertama dalam model ini adalah perencanaan cepat dan kemudian desain. Setelah tahap desain selesai, dilanjutkan ke realisasi prototipe aplikasi. Setelah itu, sampel uji akan diserahkan kepada pelanggan untuk ditinjau dan dikomentari. Model prototyping memiliki keuntungan dari komunikasi yang kuat antara pengguna dan pengembang, membantu analis untuk mengidentifikasi kebutuhan nyata pengguna, dan meminimalkan kesalahan persepsi.

Kelebihan Metode *Prototype*:

1. Pelanggan terlibat aktif dalam pengembangan sistem, sehingga hasil pengembangan produk akan mudah sesuai dengan keinginan dan kebutuhan pelanggan.
2. Identifikasi kebutuhan menjadi lebih mudah.
3. Mempersingkat waktu pengembangan produk perangkat lunak.
4. Ada komunikasi yang baik antara pengembang dan pelanggan.
5. Pengembang dapat mendefinisikan kebutuhan pelanggan dengan lebih baik.
6. Menghemat waktu pengembangan sistem.
7. Penerapan menjadi lebih mudah karena pelanggan tahu apa yang diharapkan.

Kekurangan Metode *Prototype*:

1. Proses analisis dan desain terlalu pendek.
2. Umumnya kurang fleksibel untuk berubah.
3. Sementara pengguna melihat berbagai peningkatan di setiap rilis prototipe, mereka mungkin tidak menyadari bahwa rilis itu dibuat tanpa mempertimbangkan kualitas dan pemeliharaan jangka panjang.

Pengembang terkadang membuat kompromi implementasi dengan menggunakan sistem operasi yang tidak terkait dan algoritma yang tidak efisien.

HASIL DAN PEMBAHASAN

Pengumpulan Data

Dalam penelitian ini, data yang digunakan merupakan berkas gambar atau citra digital berformat PNG dan teks.

Input *Teks*

Untuk data input, teks yang digunakan berupa *Lorem Ipsum text generated* dari internet sebagai teks yang akan digunakan untuk bahan uji coba.

Input Gambar

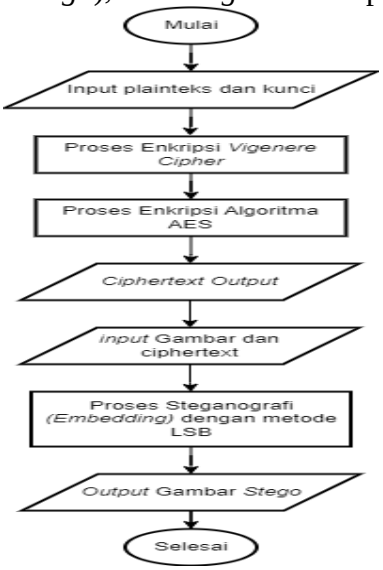
Dalam penelitian ini, berkas penampung yang digunakan merupakan berkas citra atau gambar dalam format *Portable Network Graphics* (PNG) dengan beragam ukuran dan dimensi atau resolusi yang akan digunakan sebagai bahan uji coba.

Tabel 1. Berkas Gambar untuk uji coba

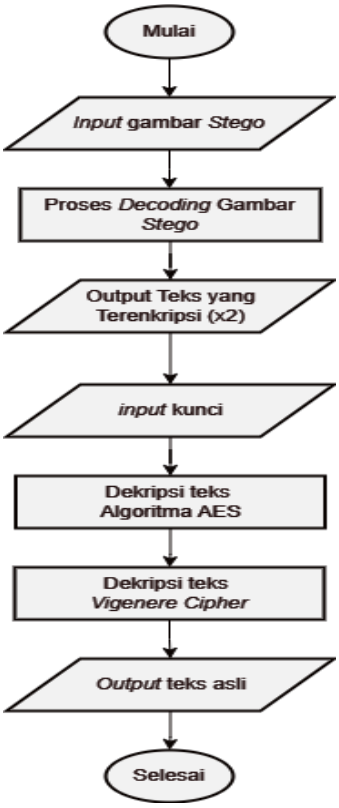
No	Nama Berkas	Ukuran Berkas	Dimensi
1	black_white.png	0,22 MB	1366 × 768
2	blue_concept.png	2,86 MB	3000 × 2000
3	fatek.png	1,78 MB	2100 × 1500
4	tech.png	0,42 MB	680 × 383
5	unima.png	1.47 MB	1920 00

Prinsip Kerja Sistem

Pada perancangan ini akan diperlihatkan diagram blok mulai dari proses enkripsi teks dan *encoding* gambar, sampai proses *decoding* gambar kemudian dekripsi teks sehingga menghasilkan teks asli yang di input pengguna. Secara garis besar, aplikasi yang akan dirancang memiliki fitur input teks, input gambar, enkripsi dan *encoding*, simpan gambar, muat gambar (gambar *stego*), *decoding* dan dekripsi pesan.



Gambar 3. *Flowchart* proses enkripsi dan *encoding*

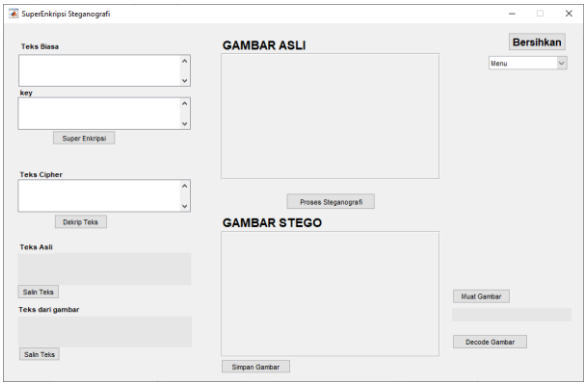


Gambar 4 *Flowchart* proses *decoding* dan dekripsi

Cara kerja pertama sistem ini dapat dilihat pada gambar 3 yaitu dimulai dengan input teks yang di enkripsi dengan dua algoritma yaitu *vigenere cipher* kemudian Algoritma AES. Kunci dari masing-masing algoritma enkripsi akan dimasukkan atau akan dilakukan proses *encoding* pada berkas gambar bersamaan dengan proses input gambar yang akan di jadikan tampungan dengan proses steganografi LSB. Kemudian akan menghasilkan keluaran atau output gambar *stego* atau *stego image*, yaitu gambar yang sudah dimodifikasi atau sudah disisipi pesan teks terenkripsi.
Pada gambar 4, gambar *stego* yang sudah dimodifikasi di *input* kembali dan akan dilakukan proses dekode gambar untuk mengeluarkan teks terenkripsi dari gambar *stego*. Dari teks terkenripsi yang di dapat akan dilakukan proses dekripsi teks dari masing – masing kedua algoritma enkripsi menggunakan *input* kunci. Kemudian akan ditampilkan teks yang tersembunyi atau teks asli.

Tampilan Antarmuka

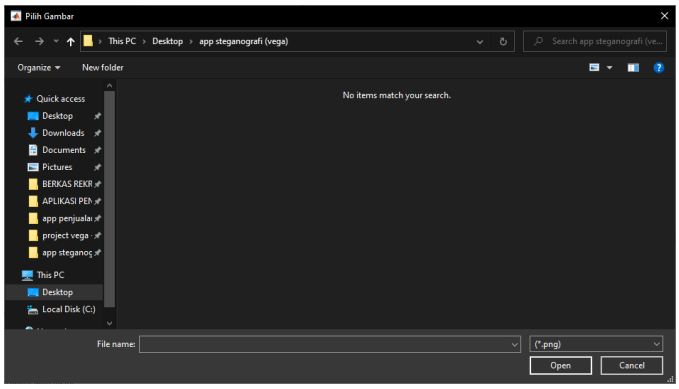
Pada penelitian ini, tampilan antarmuka dibuat untuk memudahkan penggunaan program. Tampilan antarmuka yang akan dibuat berbasis Matlab *Graphical User Interface Development Environtmen* (GUIDE) dimana fitur ini sudah ada dalam aplikasi pemrograman Matlab. Rancangan antarmuka untuk penelitian ini terdapat jendela utama dan beberapa pop up jendela.



Gambar 5. Tampilan utama program

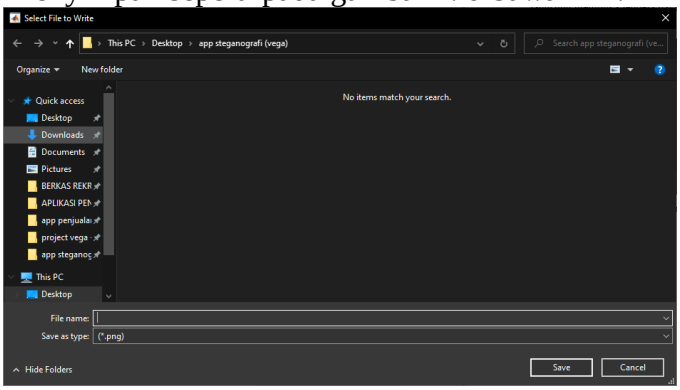
Pada Gambar 5. merupakan tampilan utama aplikasi dimana terdapat berbagai macam *callback* yang merujuk pada fungsi kode *script* untuk memproses perintah. Fungsi-fungsi dari panel jendela utama akan dijelaskan sebagai berikut:

a. Panel untuk masukkan teks dengan keterangan "Teks biasa", merupakan tempat untuk memasukkan *input plain text* atau teks biasa sebagai pesan yang nantinya akan dilakukan proses super enkripsi.
b. Panel "key" untuk masukkan *key*, merupakan tempat unruk memasukkan *input key* atau kunci yang nantinya akan dilakukan proses super enkripsi bersama *input* teks pesan.
c. Panel "teks cipher" merupakan jendela teks hasil keluaran dari proses super enkripsi dan sekaligus input panel untuk memasukkan teks cipher.
d. Panel statis "teks asli", merupakan jendela teks hasil keluaran dari proses dekripsi dimana disini menampilkan hasil yang sama dengan plain teks yang di input.
e. Panel statis "teks dari gambar", merupakan jendela teks hasil keluaran dari proses steganografi dimana cipher teks dari gambar akan ditampilkan disini.
f. Panel "Gambar Asli" dan "Gambar *Stego"*, merupakan *axes* untuk menampilkan gambar sebelum dan sesudah proses steganografi.
g. Tombol "Bersihkan" berfungsi untuk membersihkan data dari panel-panel yang ada.
h. Tombol "Super Enkripsi" merupakan *callback* untuk melakukan proses enkripsi vigenere dan enkripsi AES berdasarkan *input* yang dimasukkan berupa teks dan *key* dari panel jendela input.
i. Tombol "Dekrip" merupakan *callback* untuk melakukan proses dekripsi AES dan Vigenere berdasarkan *input key* dan teks *cipher* yang dimasukkan pada panel jendela *input*.
j. Tombol "Proses Stego" merupakan *callback* untuk melakukan proses steganografi. Ketika pengguna menekan tombol ini maka program akan langsung membuka jendela navigasi *file* untuk memilih berkas gambar seperti gambar 6. dibawah ini.



Gambar 6. jendela untuk pilih gambar penampung.

k. Tombol "Simpan Gambar" merupakan *callback* untuk melakukan proses penyimpanan gambar yang sudah dilakukan proses steganografi. Ketika pengguna menekan tombol ini maka akan muncul jendela navigasi ke direktori mana kita akn menyimpan seperti pada gambar 7. dibawah ini.



Gambar 7. jendela untuk menyimpan gambar *stego*

l. Tombol "Salin Teks" merupakan *callback* untuk menyalin teks dari jendela "Teks dari Gambar" yang kemudian akan di simpan pada clipboard agar bisa di salin kembali.
m. Tombol "Decode Gambar" merupakan *callback* untuk melakukan proses *decoding* gambar yang sudah disisipkan pesan atau *stego image* untuk mengambil teks yang tersisip. Nantinya teks tersebut akan ditampilkan pada panel teks "Teks dari Gambar"
n. Tombol "Muat Gambar" merupakan *callback* untuk menyimpan gambar stego ke dalam device atau komputer agar nanti bisa di decode kembali. Ketika pengguna menekan tombol ini maka akan muncul jendela navigasi seperti pada gambar 6.

Evaluasi Sistem

Pada tahapan ini akan dilakukan uji coba sistem untuk mengukur dan melihat proses kerja dari sistem yang sudah dirancang serta dibuat.

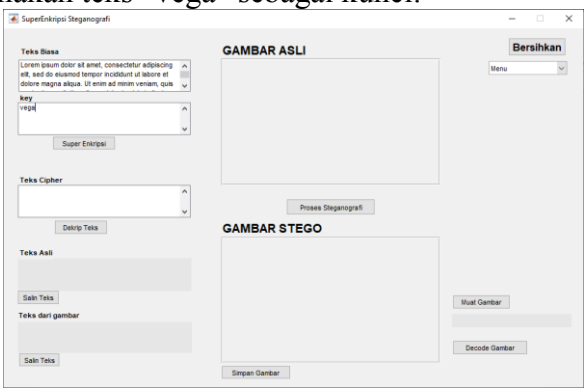
Dalam proses evaluasi ini terdapat lima berkas gambar berformat PNG dan dengan beragam ukuran resolusi serta *input* teksnya menggunakan *lorem ipsum generator* dari *web internet* sebagai karakter teks yang akan digunakan untuk bahan uji coba.

Tahap penggunaan

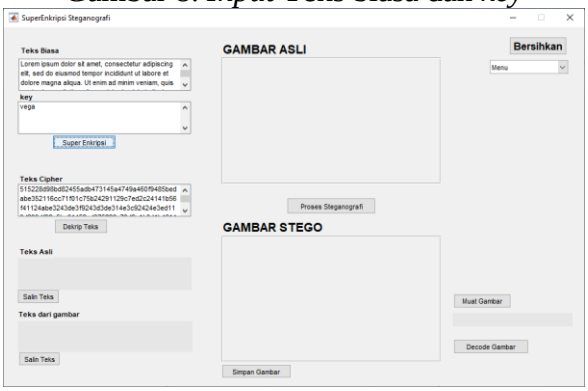
Pengujian dilakukan dengan menggunakan masukkan 500 karakter untuk melihat bagaimana kinerja program pada proses Steganografi terhadap lima berkas gambar di atas dengan parameter masukkan yang berbeda-beda.

Perlu diketahui bahwa program ini tidak memandang berapa panjang atau jumlah karakter *input* teks maupun key yang dimasukkan. Jika key lebih panjang dari jumlah teks maupun sebaliknya.

Berikut merupakan salah satu contoh proses super enkripsi sekaligus *encoding* dan *decoding* menggunakan aplikasi yang sudah di buat dengan *input* berkas citra 'black_white.png' dengan masukkan karakter *lorem Ipsum generated* berjumlah 500 karakter dan menggunakan teks "vega" sebagai kunci:



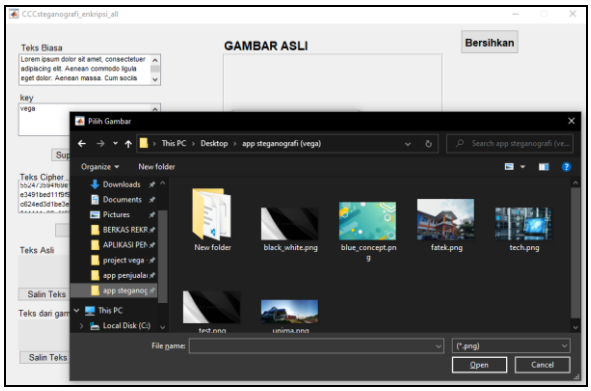
Gambar 8. *Input* Teks biasa dan *key*



Gambar 9 .Klik tombol "Super Enkripsi"

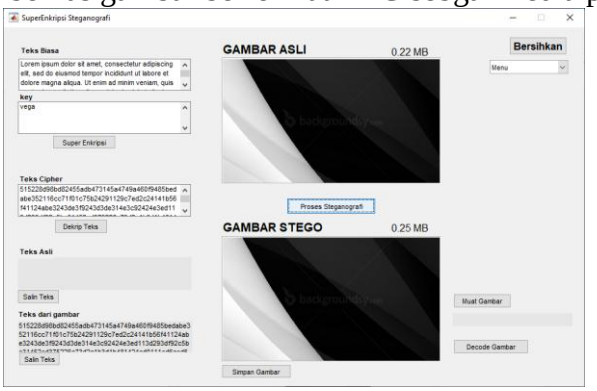
Pada gambar 8. setelah di masukkan karakter atau teks pada panel "Teks Biasa" dan "key", pengguna mengklik tombol "Super Enkripsi" seperti pada gambar 4.8 kemudian program akan melakukan proses enkripsi vigenere dan AES sehinggga menghasilkan *output* berupa karakter acak pada panel "Teks cipher".

Selanjutnya pengguna dapat mengklik tombol "Proses Steganografi" untuk menyisipkannya pada media gambar atau dengan kata lain melakukan proses steganografi.



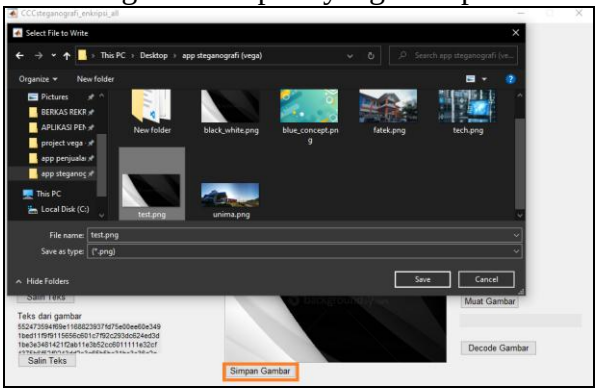
Gambar 10 Pilih Gambar

Pada Gambar 10 setelah pengguna mengklik tombol “Proses Stego” maka akan muncul jendela untuk *browse* berkas gambar berformat PNG sebgai media penampung.



Gambar 11 Hasil proses Steganografi

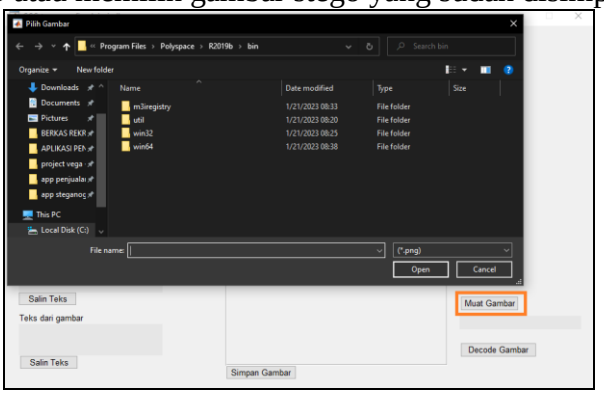
Pada gambar 11 merupakan penampakan hasil dari proses steganografi dimana pada panel gambar di atas merupakan gambar asli dan panel gambar dibawah merupakan gambar stego. Pada panel teks “Teks dari gambar” merupakan *output* teks dari gambar stego yang harusnya sama dengan teks cipher yang disisipkan.



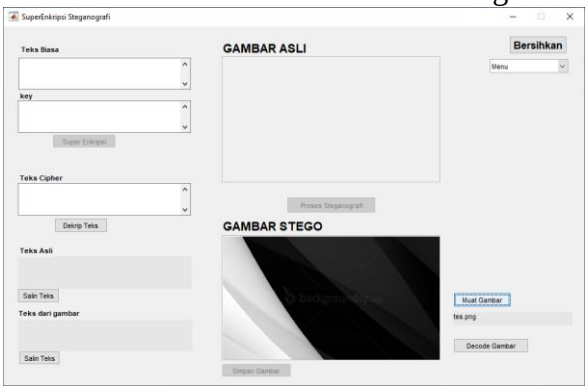
Gambar 12. Menyimpan gambar stego

Pada gambar 12. pengguna juga dapat menyimpan gambar stego untuk kemudian nanti akan di muat kembali ke program. Selama pengguna memasukkan “key” yang sebelumnya di gunakan sebagai enkripsi teks pada gambar, teks yang di dekode pada gambar stego dapat di dekripsi kembali menjadi teks yang seharusnya atau kembali menjadi *plain text*.

Pada gambar 13 ketika pengguna mengklik tombol “Muat Gambar” maka akan muncul jendela untuk *browse* atau memilih gambar stego yang sudah disimpan.

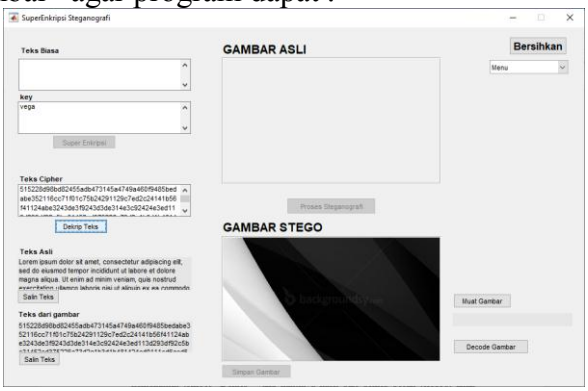


Gambar 13. Memuat Gambar stego



Gambar 14. Gambar Stego berhasil dimuat

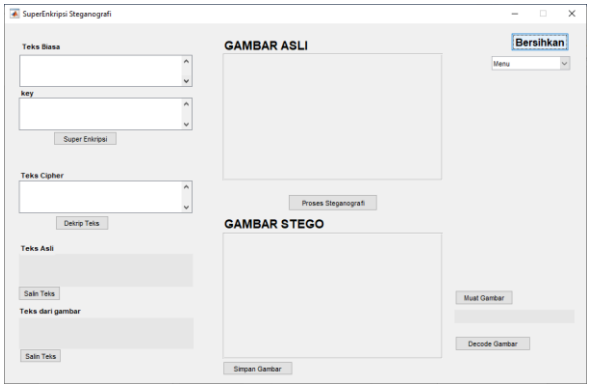
Pada gambar 14 jika gambar stego berhasil dimuat maka nama berkas akan muncul pada panel teks dibawa tombol “Muat Gambar”. Kemudian pengguna dapat mengklik tombol “Decode Gambar” agar program dapat .



Gambar 15. Dekode Gambar *stego* dan Dekripsi teks *cipher*

Pada gambar 15 terdapat hasil dari proses dekode gambar stego yang terletak pada panel teks “Teks dari gambar”. Untuk mendekrip teks cipher dari gambar stego pengguna harus memasukkan *key* pada panel teks “Key” terlebih dahulu kemudian kemengklik tombol “Dekrip” yang nantinya hasil dari dekrip pesan tersebut akan muncul pada panel teks “Teks Asli”.

Gambar 16. Membersihkan Panel

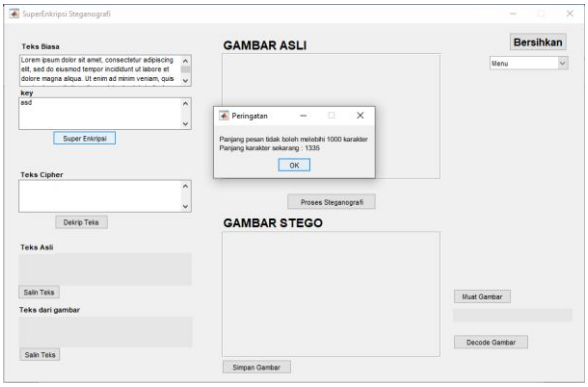


Gambar 17. Panel kembali seperti semula

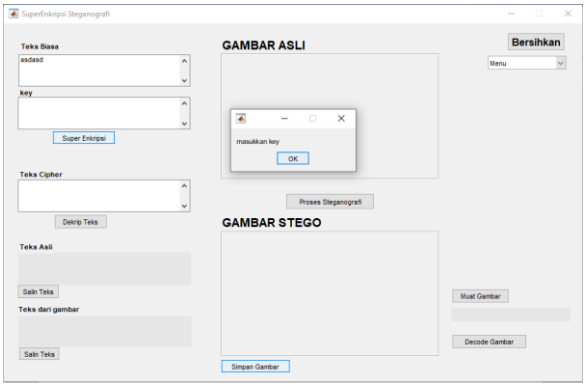
Pengguna juga dapat membersihkan atau mengembalikan panel – panel yang ada pada antarmuka seperti semula atau dalam keadaan kosong dengan mengklik tombol "Bersihkan" pada pojok kanan atas seperti pada gambar 16 dan hasilnya seperti pada gambar 17

Error Handling

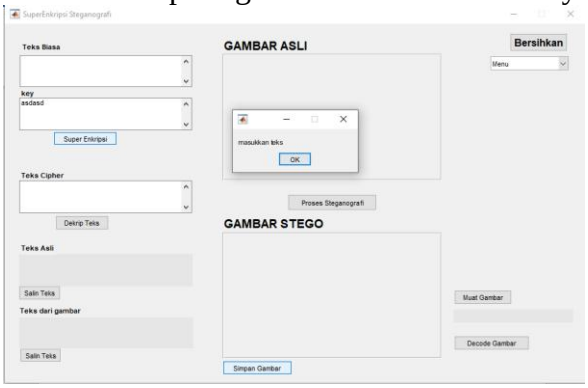
Pada program yang dibuat penulis memberikan error handling berupa peringatan atau *warning text box* ketika ada langkah yang belum dilakukan atau terlupa oleh pengguna.



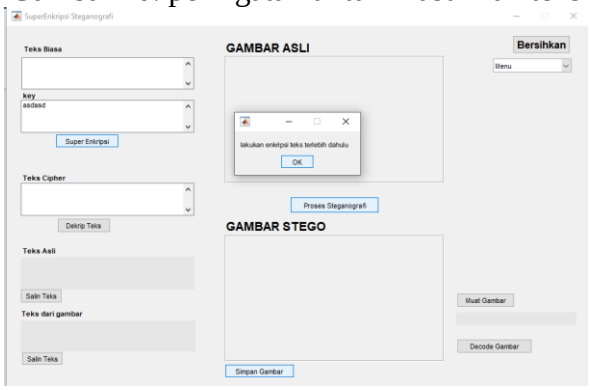
Gambar 18. peringatan jika panjang karakter melebihi 1000 karakter



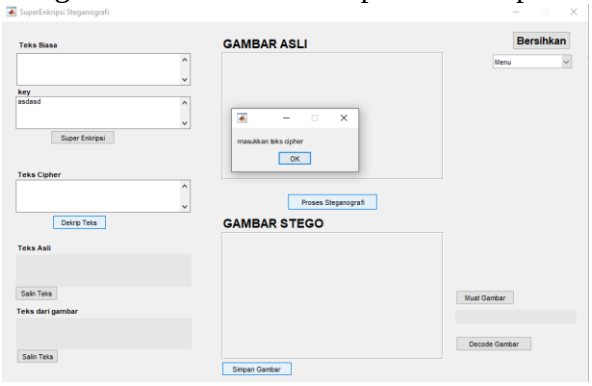
Gambar 19. peringatan untuk masukkan key



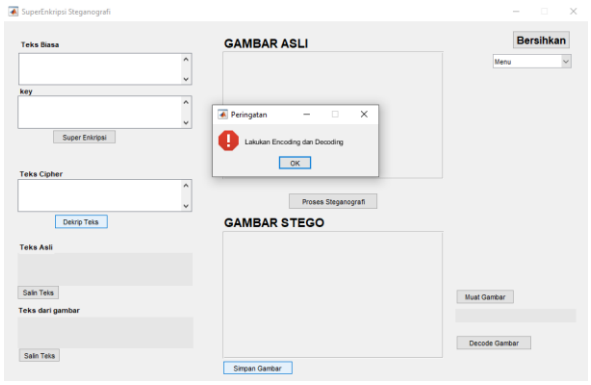
Gambar 20. peringatan untuk masukkan teks



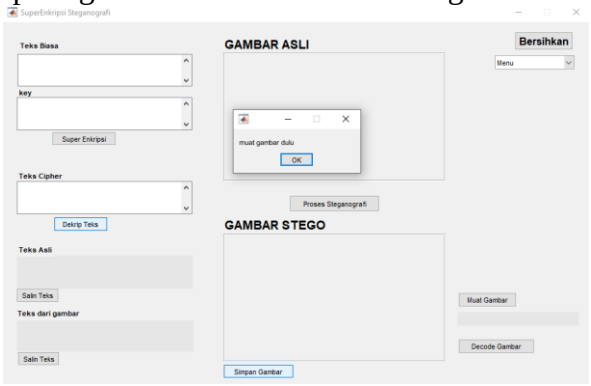
Gambar 21 peringatan untuk melakukan proses enkripsi terlebih dahulu



Gambar 22. peringatan untuk memasukkan teks cipher



Gambar 23. peringatan untuk lakukan encoding dan decoding dahulu



Gambar 24 peringatan untuk muat gambar terlebih dahulu

KESIMPULAN

Kesimpulan

Bardasarkan hasil peneletian dan pengujian yang telah dibuat, kesimpulan yang penulis dapat yaitu :

1. Peneliti berhasil membangun aplikasi atau program berbasis desktop untuk melakukan proses Super Enkripsi pada teks dengan menggunakan *Vigenere Cipher* dan *Algoritma Advanced Encryption* Standard (AES) serta menyisipkannya pada berkas gambar dengan menggunakan teknik *Steganografi Least Significant Bit* (LSB) serta aplikasi juga dapat melakukan proses dekode gambar dan melakukan dekrip teks agar mendapatkan teks asli.
2. Besar panjang teks yang di *input* mempengaruhi ukuran berkas gambar *stego* dengan peningkatan ukuran sebesar 10,88 % dari ukuran asli dengan panjang teks 25000 karakter pada evaluasi.

Saran

Dalam penelitian ini masih terdapat beberapa hal yang dapat ditingkatkan dan bisa dikembangkan. Maka dari itu, berikut merupakan beberapa saran dari penulis untuk peneliti yang ingin mengembangkan atau ingin menjadikan penelitian ini sebagai kajian pustaka:

1. Berdasarkan penelitian yang telah dibuat, pengembangan lanjutan dapat menggunakan objek tampung lain selain citra contohnya seperti berkas audio, berkas PDF dan atau berkas video untuk menyisipkan pesan atau bahkan data lain seperti audio tersembunyi pada citra digital.
2. Menyempurnakan algoritma atau menambahkan algoritma *cipher* lain berbasis teknik Super Enkripsi dan Steganografi pada penelitian ini.

UCAPAN TERIMAKASIH

Pada kesempatan ini penulis berterima kasih kepada semua pihak yang telah terlibat dalam membantu penulis untuk menyelesaikan penelitian ini

DAFTAR PUSTAKA

Naharuddin, A. 2018. Steganografi Teks Menggunakan Pemetaan Digit Biner Pada Karakter *ASCII* Untuk Keamanan *Plain Text*. Doctoral dissertation, Institut Teknologi Sepuluh Nopember.

Langi, E.R., Sambul, A.M., and Kambey, F.D. 2021. Perbandingan Metode *Least Significant Bit* dan *Discrete Wavelet Transform* dalam Teknik Steganografi pada Citra Batik Bentenan. Skripsi Program S1 Teknik Elektro Universitas Sam Ratulangi. Manado.

Ahmad, A. 2019. Implementasi *Vigenere Cipher* dengan menggunakan Matlab 2015b. Prosiding Seminar Pendidikan Matematika dan Matematika. Vol. 1, pp. 53-58.

Pricillia, T., Zulfachmi. 2021. *Survey Paper*: Perbandingan Metode Pengembangan Perangkat Lunak (*Waterfall, Prototype, RAD*). Vol. X, No. 1, pp. 6-12.

Rangkuti, A.Z.F, dan Fahmi, H. 2020. Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. Jurnal Nasional Komputasi dan Teknologi Informasi. Vol. 3, No. 2, pp. 170-175.

Yusuf, K. 2020. Penerapan Algoritma MD5 sebagai Pengaman Akun pada Aplikasi Web Emusrenbang Kota Binjai. Jurnal Teknik Informatika Kaputama. Vol. 4, No. 1, pp. 29-34.

Santoso, S.D. 2019. Implementasi Penyandian Super Enkripsi Vigenere Cipher dan Railfence Cipher menggunakan Python. Skripsi Program S1 Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Irawan, C. 2019. Implementasi ALgoritma Autokey Cipher dan AES-128 Pada Enkripsi File. Prosiding Fakultas Ilmu Komputer Universitas Dian Nuswantoro. Pp. 335-339.

Wiranata, A.D. dan Aldisa, R.T. 2021. Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA. Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi). Vol. 5, No. 3, Pp. 277-281.

Syahril, M. dan Jaya, H. 2019. August. Aplikasi steganografi pengamanan data nasabah di Standard Chartered Bank menggunakan metode Least Significant Bit dan RC4. In Seminar Nasional Sains dan Teknologi Informasi (SENSASI). Vol. 2, No. 1, Pp. 505 – 509.

Fachrozi, M.F. and Fahmi, H. 2020. Penerapan Metode AES-128 Untuk Pengamanan Data Absensi Fingerprint Di Balai Penelitian Sungei Putih. Jurnal Ilmu Komputer dan Sistem Informasi. Vol. 3, No. 1.1, pp.1 - 8.

Simanjuntak, W. 2019. Perancangan Aplikasi Steganografi Menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement. JUKI: Jurnal Komputer dan Informatika. Vol. 1, No. 1, pp. 30 - 38.

Damanik, H.A. and Anggraeni, M. 2018. Teknik Pengujian Keamanan Data Text Bertingkat dengan Metode Steganography Lsb dan Teknik Enkripsi. Jurnal Penelitian Pos dan Informatika. Vol. 8, No. 2, pp. 109 - 122.