Jurnal Online Universitas Budi Luhur

SKANIKA

Sistem Komputer dan Teknik Informatika

E-ISSN : 2721-4788
Vol. 4, No. 2, Juli 2021

UNIVERSITAS BUDI LUHUR

Diterbitkan oleh:
Universitas Budi Luhur
Jl. Raya Ciledug Petukangan Utara, Jakarta Selatan

JURNAL SKANIKA
Sistem Komputer dan Teknik Informatika

Alamat Redaksi
Kantor Fakultas Teknologi Informasi
Jl. Ciledug Raya No.99, RT.10/RW.3, Petukangan Utara
Pesanggrahan, Kota Jakarta Selatan, DKI Jakarta 12260
email : skanika.fti@budiluhur.ac.id

SKANIKA: Sistem Komputer dan Teknik Informatika adalah Jurnal ilmiah yang diterbitkan secara berkala oleh Program Studi Sistem Komputer dan Program Studi Teknik Informatika di Fakultas Teknologi Informasi Universitas Budi Luhur. Jurnal Skanika mulai terbit pada tahun 2018 dan Mulai tahun 2021 mulai terbit sebanyak 2x dalam setahun yaitu bulan Januari dan Juli.

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Tuhan Yang Maha Esa atas berkat, rahmat dan karunia-Nya sehingga Jurnal Ilmiah Skanika Volume 4 Nomor 2 Juli 2021 dapat terbit sesuai yang direncanakan.

Jurnal penelitian ini terbit sebagai bentuk kepedulian Universitas Budi Luhur (UBL) dalam meningkatkan mutu penelitian dan publikasi yang dilakukan oleh Dosen, mahasiswa ataupun praktisi di perguruan tinggi. Pada Jurnal Skanika Volume 4 Nomor 2 Juli 2021 lebih banyak diisi oleh tulisan pada topik *Kriptografi, Image Processing, Artificial Intelligence dan Stenografi.* Semoga Jurnal Skanika dapat menjadi referensi bagi para peneliti di Indonesia dan meningkatkan kualitas dari publikasi penelitian di Indonesia.

Seluruh personalia Jurnal Skanika mengucapkan terima kasih kepada penulis sebagai penyumbang artikel ilmiah, karena tanpa sumbangan artikel ilmiah dan penelitian dari penulis maka mustahil jurnal ilmiah Skanika dapat diterbitkan, terima kasih juga kepada semua pihak yang selalu memberikan dukungan kepada jurnal Skanika sehingga dapat hingga saat ini.

Terima kasih dan selamat membaca

Jakarta, Juli 2021

Editor in Chief
Jurnal SKANIKA

DAFTAR ISI

PENGEMBANGAN TEKNIK MENYEMBUNYIKAN PESAN RAHASIA MENGGUNAKAN PENGGABUNGAN METODE STEGANOGRAFI DAN KRIPTOGRAFI CAESAR CIPHER YANG TELAH DIMODIFIKASI DAN SHA-512

Angga Kusuma Nugraha[1)], **Yesi Puspita Dewi**[2)]
Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : angga.kusumanugraha@budiluhur.ac.id[1)], yesi.puspitadewi@budiluhur.ac.id[2)]

Abstrak

Komunikasi melalui media digital kian hari semakin cepat dan praktis. Dalam hal ini, keamanan menjadi penting karena issue faktor privasi. Steganografi dapat menyembunyikan pesan rahasia dengan cara disisipkan pada media digital, salah satunya gambar atau citra digital. Namun faktor keamanan steganografi belum maksimal. Teknik steganografi semakin menjadi populer oleh karenanya banyak aplikasi yang disediakan untuk mengangungkap pesan rahasia yang ada didalam stego image. Pesan rahasia menjadi dapat diungkap oleh pihak yang tidak seharusnya. Penelitian ini membuat peningkatan keamanan terhadap steganografi dengan kriptografi Caesar Cipher yang telah dimodifikasi dengan membalik urutan pesan rahasia kemudian digeser 5 karakter dan SHA-512, lalu pesan rahasia disisipkan kedalam gambar digital dengan metode Least Significant Bit (LSB). Pengujian dilakukan dengan metode kualitatif yaitu Power Signal Noise Ratio (PSNR) serta perubahan ukuran file dan metode kuantitatif. Hasil evaluasi dari penelitian ini didapatkan bahwa aplikasi penguji mampu menyembunyikan pesan rahasia pada gambar digital dengan ekstensi populer.

Kata kunci: Caesar Cipher, Kriptografi, *Least Significant Bit*, LSB, *Power Signal Noise Ratio*, PSNR, SHA-512, Steganografi

1. PENDAHULUAN

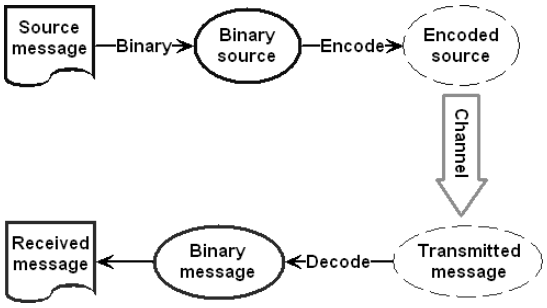
Berkomunikasi melalui jaringan internet menjadi semakin populer karena dapat dilakukan dengan mudah dan melalui beragam media, oleh sebab itu faktor privasi dan keamanan adalah hal yang penting dalam berkomunikasi melalui jaringan internet. Agar terhindar dari kasus kebocoran informasi yang terjadi, salah satu metode yang digunakan untuk pesan rahasia menjadi aman adalah Steganografi. Teknik steganografi adalah meyisipkan pesan rahasia melalui media digital seperti citra, video, maupun suara [1].

Seiring waktu, banyak penelitian yang dikembangkan terkait teknik Steganografi. Terdapat berbagai metode untuk menyisipkan pesan rahasia kedalam gambar menggunakan Steganografi. Salah satu metode yang populer adalah *Least Significant Bit* (LSB) karena metodenya yang cukup sederhana yaitu menyembunyikan pesan rahasia yang sudah diubah kedalam bentuk binari dengan cara menyisipkannya pada pixel terakhir yang menyusun suatu file citra. Beberapa aplikasi menggunakan teknik ini dan dapat digunakan secara bebas dengan mengunduhnya dari internet adalah OpenStego dan Silent Eyes. Karena semakin populer dan banyak digunakan, maka perlu kemanan tambahan pada Steganografi sehingga jika pesan rahasia berhasil diekstrak oleh pihak yang tidak diinginkan, pesan tersebut tetap belum dapat terungkap dan diketahui.

Pada penelitian ini, digunakan teknik pengamanan pesan rahasia Steganografi dengan keamanan tambahan yang berlapis, dengan menambahkan Kriptografi terhadap pesan rahasia yang disisipkan kedalam citra digital melalui Steganografi menggunakan metode LSB. Berbagai teknik Kriptografi populer yang telah banyak digunakan sehingga source code untuk memecahkannya banyak tersebar dibeberapa situs internet. Oleh karena itu diperlukan Kriptografi berlapis dan unik agar pesan rahasia menjadi acak. Dengan cara ini pesan yang disampaikan keamanannya lebih terjaga dan tidak mudah terungkap oleh pengguna yang berusaha mencuri informasi.

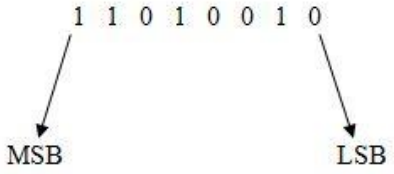
2. METODE PENELITIAN

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [2]. Dengan Steganografi, pemilik data dapat menyembunyikan informasi hak ciptanya seperti identitas pembuat, tanggal dibuat, hingga pesan kepada seseorang yang dikehendaki. Steganografi menyembunyikan informasi kedalam berbagai jenis data seperti: gambar, audio, video, teks atau file biner. Metode Steganografi sedemikian rupa dalam menyembunyikan isi suatu data didalam suatu sampul media atau data digital lain yang tidak diduga oleh orang biasa sehingga tidak menimbulkan kecurigaan kepada orang yang melihatnya [3].



Gambar 1. Ilustrasi Dasar Konsep Steganografi

Dalam Steganografi pesan rahasia disembunyikan dalam citra digital. Penyembunyian data dilakukan dengan mengganti *bit* data didalam segmen gambar dengan *bit* pesan rahasia. Metode yang paling sederhana adalah metode modifikasi *Least Significant Bit* (LSB) [4]. Pada susunan bit didalam sebuah *byte* (1 *byte* = 8 *bit*), ada *bit* yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB).



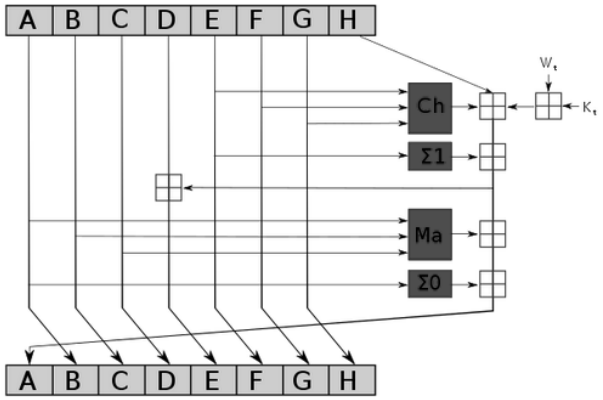
Gambar 2. Bit pada MSB dan LSB

Metode LSB adalah metode yang digunakan untuk menyembunyikan pesan dengan cara menyisipkannya pada bit rendah atau bit yang paling kanan pada data piksel yang menyusun file tersebut [5]. Pada citra bitmap 24 bit, setiap piksel (titik) pada citra tersebut terdiri dari tiga susunan warna, yaitu 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. Dengan demikian, pada setiap piksel citra bitmap 24 bit kita dapat menyisipkan 3 bit data. Kekurangan dari metode LSB ini adalah dapat secara drastis mengubah unsur pokok warna dari piksel jika tidak tepat dalam mengganti bit atau pesan yang dimasukkan terlalu panjang. Sehingga dapat menunjukkan perbedaan yang nyata dari gambar asli dengan gambar yang telah disisipkan pesan. Sementara kelebihan dari metode LSB adalah algoritma yang dipakai cepat dan mudah [6].

Sebuah *cipher* adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi. *Caesar Cipher* dikenal juga dengan Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet [7]. Misalnya, jika menggunakan geseran 3, W akan menjadi Z, I menjadi L, dan K menjadi N sehingga teks terang "wiki" akan menjadi "ZLNL" pada teks tersandi. Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet biasa:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet sandi:
DEFGHIJKLMNOPQRSTUVWXYZABC

SHA-1 (Secure Hash Algorithm 1) adalah fungsi *hash* kriptografi yang mengambil input dan menghasilkan nilai hash 160-bit (20-byte) yang dikenal sebagai intisari pesan - biasanya ditampilkan sebagai angka heksadesimal, panjang 40 digit. Ini dirancang oleh Badan Keamanan Nasional Amerika Serikat, dan merupakan Standar Pemrosesan Informasi Federal A.S. Sejak 2005 SHA-1 belum dianggap aman. SHA-512 adalah salah satu fungsi *hash* pengganti untuk SHA-1 (secara kolektif disebut sebagai SHA-2), dan merupakan salah satu fungsi hash terkuat yang tersedia. SHA-512 tidak jauh lebih kompleks untuk dikodekan daripada SHA-1, dan belum dikompromikan dengan cara apa pun. Kunci 256-bit menjadikannya fungsi mitra yang baik untuk AES. Hal ini didefinisikan dalam standar NIST (Institut Standar dan Teknologi Nasional) 'FIPS 180-4'. NIST juga menyediakan sejumlah vektor uji untuk memverifikasi kebenaran implementasi [5].



Gambar 3. Bagan Satu Iterasi Pada Proses SHA-2

Dalam penelitian ini metode yang dilakukan sebagai langkah awal dalam observasi terhadap teknik Steganografi dan Kriptografi adalah metode studi pustaka dengan mempelajari landasan teori yang dibutuhkan mengenai Steganografi dan mempelajari Kriptografi pada beberapa literatur dan referensi lainnya. Referensi tersebut berupa data-data dari internet, buku elektronik, publikasi, paper dan dokumen lain yang terkait dalam hal menentukan dan membangun alat penguji penelitian.

Tujuan dari penelitian ini yaitu untuk memberikan keamanan berlapis pada Steganografi dengan cara menambahkan Kriptografi pada pesan rahasia yang disisipkan pada *cover image*, dan Kriptografi yang digunakan merupakan modifikasi Kriptografi Caesar Cipher dengan membalikan urutan pesan rahasia kemudian mengesernya 5 karakter. Berdasar kepada tujuan yang disebutkan diatas, penelitian kali ini akan menggunakan metode penelitian eksperimen sebagai metode pengujian. Penelitian eksperimen adalah penelitian dimana peneliti dapat melakukan manipulasi kondisi yang ada sesuai dengan keinginan dan harapan peneliti, berdasar kepada kondisi nyata atau kondisi sebenarnya [8].

Dalam kondisi yang telah dimanipulasi pada metode eksperimen, biasanya dibuat dua kelompok yaitu kelompok kontrol dan kelompok pembanding. Kelompok kontrol akan diberikan perlakuan tertentu sesuai dengan tujuan penelitian dan kemudian hasil dari perlakuan ini yang akan dijadikan pembanding terhadap kelompok pembanding [9].

Teknik analisis data dalam penelitian ini menggunakan pendekatan kualitatif dimana data yang telah dikumpulkan sebelumnya dianalisis tidak dengan menggunakan analisis data statistik. Analisis data secara kualitatif dilakukan dengan menganalisis hasil pencatatan teknik Steganografi yang digunakan, penyisipan pesan, keamanan tambahan yang digunakan dan jenis Kriptografi yang digunakan, yaitu dengan membandingkan langkah-langkah dari setiap instrumen yang ada.

Salah satu fokus utama penelitian ini adalah keamanan berlapis berupa Kriptografi. Dasar teknik Kriptografi yang digunakan pada penelitian ini adalah Caesar Cipher. Caesar Cipher merupakan teknik Kriptografi dengan menggeser urutan abjad sejumlah n sehingga membentuk kata yang acak. Secara sederhana, Kriptografi Caesar Cipher dengan menggeser 5 karakter dapat dilihat pada simulasi dibawah ini:

Kunci Urutan:
'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','','0','1','2','3','4','5','6','7','8','9','!','@','#','$','%','^','&','(',')','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','+','-','*','/','[',']','{','}','<','>','?','_'

Pesan : ANGGA KUSUMA NUGRAHA
Hasil : FSLLF4PZXZRF4SZLWFMF

Pada penelitian kali ini dilakukan modifikasi terhadap teknik Kriptografi Caesar Cipher menjadi dua tahap. Pada tahap pertama pesan rahasia akan dibalik urutan abjad nya sehingga yang pertama menjadi terakhir sedangkan yang terakhir menjadi yang pertama. Tahap yang kedua pesan rahasia yang telah dibalik urutannya akan di geser sebanyak 5 karakter. Secara sederhana proses Kriptografi pada penelitian dapat disimulasikan sebagai berikut:

Pesan : ANGGA KUSUMA NUGRAHA
Tahap 1 : AHARGUN AMUSUK AGGNA
Tahap 2 : FMFWLZS4FRZXZP4FLLSF

Setelah dilakukan kriptografi Caesar Chiper yang telah dimodifikasi kemudian pesan dienkripsi dengan SHA-512 sehingga menjadi hash karakter yang acak, dapat dilihat pada simulasi berikut:

Pesan : ANGGA KUSUMA NUGRAHA
Tahap 1 : AHARGUN AMUSUK AGGNA
Tahap 2 : FMFWLZS4FRZXZP4FLLSF
Tahap 3 :
FCBCA0864C04A7E92554721206ECDAB0E3F518AFB40D1984713A4F61897B49702AF84FC7CF7D2DB49CFBFE637037FF7A0879F2BA3BF5C23DE9FD915F2CBD07BA

Hasil dari tahap 3 diatas yang akan disisipkan pada citra digital menggunakan steganografi.

Pada penelitian ini pengujian sistem atau uji coba terhadap alat penguji dilakukan dengan metode kualitatif dan kuantitatif. Metode kualitatif dengan cara melakukan ujicoba terhadap alat penguji dengan berbagai jenis gambar sebagai cover image dan berbagai jenis karakter sebagai pesan rahasia yang akan disisipkan, kemuadian akan diuji tingkat Power Signal Noise Ratio (PSNR) yang terdapat pada antara file gambar yang belum disisipi pesan dengan gambar setelah menjadi stego image. Power Signal Noise Ratio (PSNR) adalah ukuran yang digunakan secara ilmiah yang membandingkan tingkat sinyal yang diinginkan dengan tingkat kebisingan latar belakang [10].

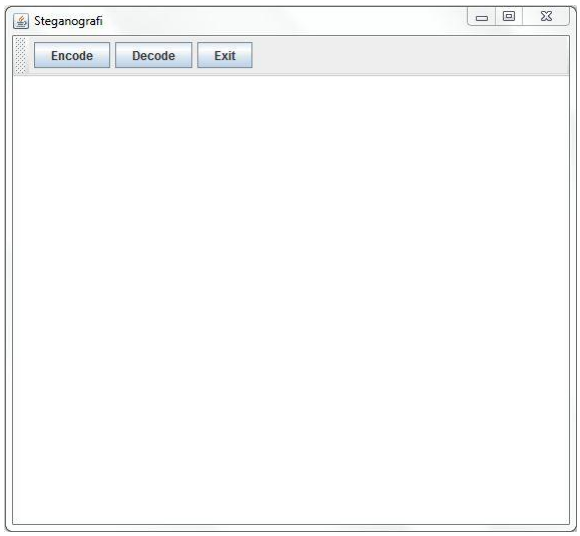
Sedangkan metode kuantitatif dilakukan dengan melakukan ujicoba terhadap alat penguji dengan sejumlah gambar sehingga diketaui tingkat keberhasilan secara statistik. Dengan hal tersebut dapat diketahui tingkat keberhasilan penelitian yang dilakukan.

3. HASIL DAN PEMBAHASAN

Setelah peneliti melakukan proses analisis dan perancangan sistem, selanjutnya peneliti akan melakukan implementasi sistem yang telah melalui tahap perancangan tersebut. Pada tahap implementasi program akan dilakukan penerjemahan rancangan yang dibuat menjadi baris code bahasa pemrograman Java agar dimengerti oleh perangkat komputer untuk mengeksekusi suatu proses. Selain implementasi program untuk mengeksekusi suatu proses akan diimplementasikan pula tampilan GUI dari perancangan layar aplikasi yang dilakukan sebelumnya.

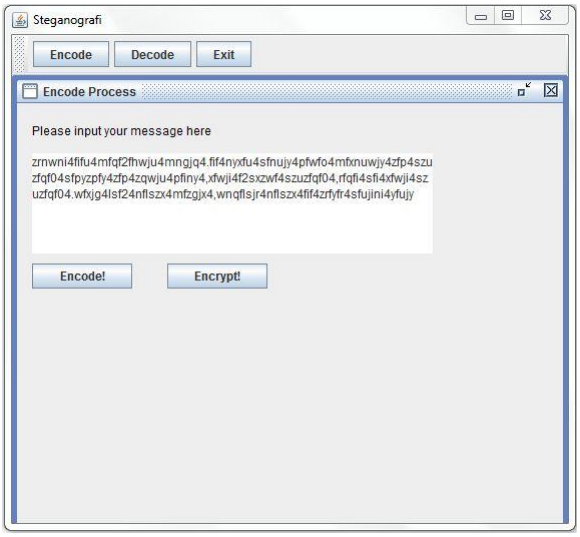
Tahap development dilakuka secara manual menggunakan software JCreator Pro 3.0. Pada bagian ini peneliti akan menjelaskan sistem secara urut dan berdasarkan halaman yang ada pada program dan proses yang terjadi.

Pada saat pertama kali aplikasi Steganografi ini dijalankan, yang akan muncul adalah halaman utama dari aplikasi ini. Halaman utama ini memiliki tiga buah tombol, yaitu '*Encode*', '*Decode*' dan '*Exit*'. Tampilan layar halaman utama dapat dilihat pada gambar dibawah ini.



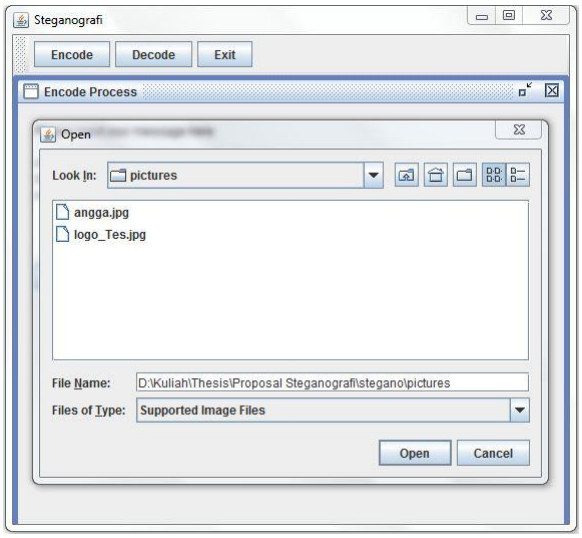
Gambar 4. Halaman Utama

Tahap yang pertama pada mode *encode* adalah proses enkripsi. Dapat dilihat pada gambar 5 terdapat text area pada halaman *encode process* untuk memasukan pesan rahasia yang akan disisipkan. Pengirim dapat mengisi text area tersebut dengan pesan rahasia yang dikehendaki. Setelah itu pengirim perlu menekan tombol '*Encrypt!*' untuk melakukan enkripsi terhadap pesan rahasia tersebut.



Gambar 5. Halaman Encode Process Setelah Enkripsi

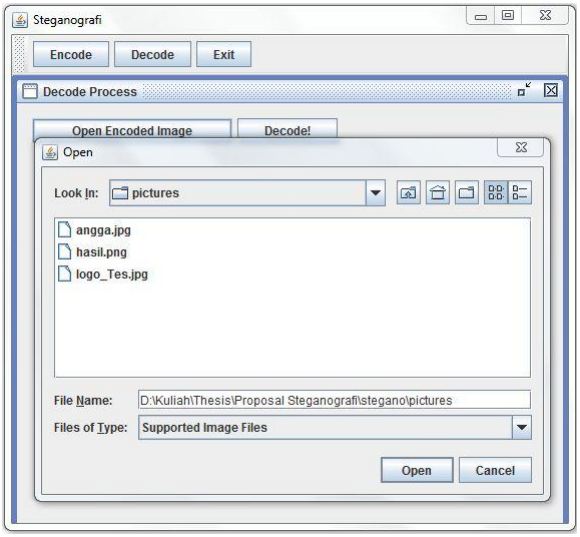
Setelah pesan rahasia dienkripsi, selanjutnya adalah memilih *cover image* dan melakukan encode pesan rahasia kedalam *cover image* yang telah dipilih. Untuk memilih *cover image*, pengirim hendaknya menekan tombol '*Encode!*'. Akan muncul jendela *browse cover image*, pengirim dapat memilih *cover image* dari direktori yang ada pada komputer pengirim. Setelah memilih *cover image* pengirim dapat menekan tombol '*Open*', maka gambar tersebut akan terpilih sebagai *cover image* dan proses encode pesan rahasia kedalam *cover image* tersebut otomatis berjalan.



Gambar 6. Tampilan Browse Cover Image

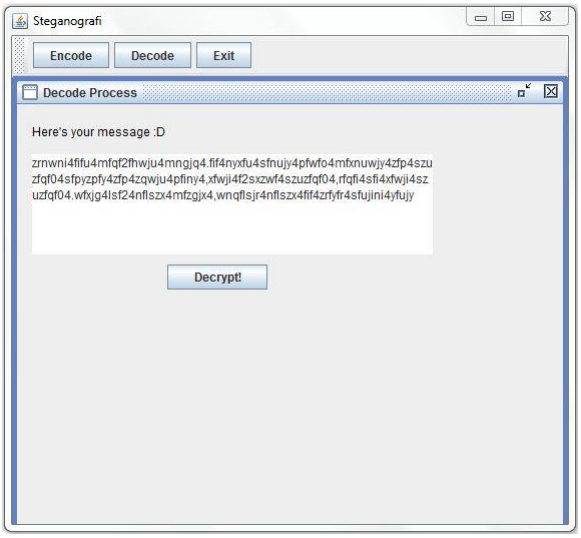
Saat memasuki mode *decode*, penerima pesan akan menemukan dua tombol pada halaman *decode process*. Tombol '*Decode!*' berfungsi untuk melakukan *decode* terhadap pesan rahasia yang ada didalam *stego image*, tombol ini akan dijelaskan pada bagian berikutnya.

Untuk memilih *stego image* yang akan diekstrak pesan rahasianya, maka penerima pesan harus menekan tombol '*Open encoded image*'. Apabila tombol tersebut ditekan, maka akan tampil jendela *browse stego image*. pada jendela tersebut penerima pesan dapat memilih stego image dari direktori komputer penerima pesan.



Gambar 7. Tampilan *Browse Stego Image*

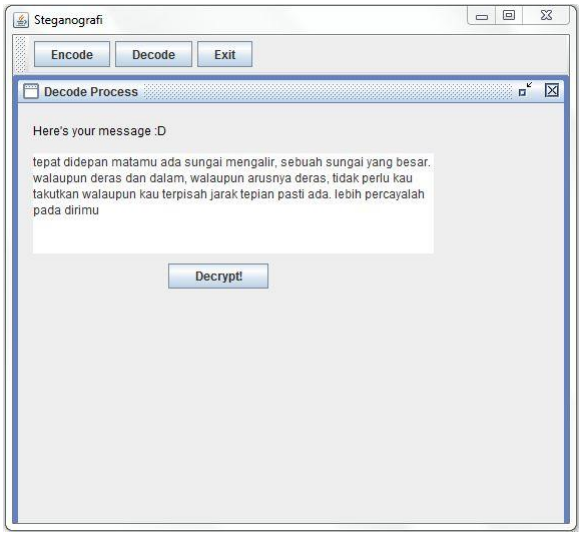
Proses selanjutnya adalah melakukan decode terhadap stego image yang dipilih. Untuk melakukan decode pada stego image yang telah dipilih pada proses sebelumnya, penerima pesan harus menekan tombol '*Decode!*' pada halaman *decode process* yang ditunjukan pada gambar 8. Apabila penerima menekan tombol '*Decode!*' maka akan tampil halaman *decode process* dengan tombol '*Decrypt!*' seperti pada gambar 8 dibawah ini.



Gambar 8. Halaman Decode Process Sebelum Dekripsi

Untuk melakukan dekripsi terhadap pesan rahasia yang masih acak tersebut, penerima pesan harus menekan tombol '*Decrypt!*'. Setelah ditekan, maka akan muncul pesan rahasia yang sudah dapat dibaca karena sudah tidak acak. Dengan demikian proses decode sudah selesai, penerima dapat kembali kehalaman utama aplikasi atau keuar dari aplikasi dengan menekan tombol '*Exit*'.

Pengujian kualitatif dilakukan pada alat penguji dengan sample 2 buah citra digital dengan format ekstensi yang berbeda. Gambar tersebut akan disispi pesan rahasia menggunakan alat penguji, kemudian akan diuji menggunakan Power Signal Noise Ratio (PSNR).



Gambar 9. Halaman Decode Process Setelah Dekripsi

Selain noise yang menjadi aspek pertimbangan adalah ukuran file, sehingga pada pengujian ini juga akan dibandingkan ukuran file sebelum disisipi pesan dan setelah disisipi pesan dan dicari selisihnya. Dengan demikian bisa didapatkan jenis ekstensi gambar digital yang paling baik untuk digunakan dan yang paling buruk. Berikut adalah sampel gambar yang ekstensi yang telah disediakan oleh peneliti beserta hasil dari uji kualitatif yang dilakukan.

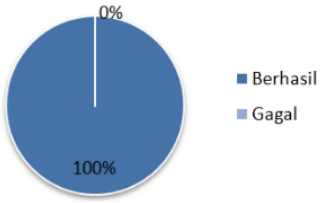
Tabel 1. Hasil Uji Kualitatif Berdasarkan Noise

No	File Sebelum	File Sesudah	PSNR
1	jerapah.jpg	jerapah_hasil.png	79.964708586
2	jerapah.png	jerapah_hasil.png	79.955517164
3	jerapah.gif	jerapah_hasil.gif	79.955517165
4	jerapah.bmp	jerapah_hasil.bmp	79.992400145

Tabel 2. Hasil Uji Kualitatif Berdasarkan Ukuran

No	Nama File	Ukuran Sebelum	Ukuran Sesudah	Selisih Ukuran
1	jerapah.jpg	92 KB	611 KB	519 KB
2	jerapah.png	751 KB	677 KB	74 KB
3	jerapah.gif	335 KB	173 KB	166 KB
4	jerapah.bmp	938 KB	199 KB	739 KB

Pengujian kualitatif dilakukan pada alat penguji dengan melakukan percobaan sebanyak 50 kali pada 50 file citra digital baik proses encode maupun proses decode, sehingga diketahui jumlah keberhasilan dan kegagalan secara statistic.



Gambar 10. Hasil Uji Kualitatif

4. KESIMPULAN

Ujicoba kualitatif dapat diketahui hasilnya pada Tabel 1, dapat dibuktikan bahwa aplikasi bisa memproses gambar digital dengan format *.JPG, *.PNG, *.GIF dan *.BMP. Format ekstensi tersebut adalah ekstensi yang populer dan banyak digunakan sebagai gambar digital terutama pada komunikasi dengan jaringan internet, sehingga terbukti aplikasi penguji berhasil menyembunyikan pesan rahasia.

Selain itu pada pengujian ini juga dapat diketahui bahwa gambar digital dengan ekstensi *.PNG setelah melalui proses, adalah gambar dengan tingkat noise paling rendah dan ekstensi *.BMP memiliki tingkat noise yang tinggi.

Apabila dilihat dari perbandingan ukuran file yang ditunjukan pada tabel 2, gambar digital dengan ekstensi *.PNG memiliki selisih paling kecil antara stego image dengan gambar asal. Sedangkan gambar dengan ekstensi *.BMP memiliki selisih ukuran yang besar.

Tingkat noise yang rendah menunjukkan bahwa gambar digital dengan ekstensi tersebut baik digunakan untuk Steganografi dengan keamanan berlapis pada penelitian ini. Hal tersebut karena pada gambar dengan tingkat noise yang rendah, perbedaan antara gambar asal dan stego image rendah sehingga paling mirip sengan aslinya dan paling sulit dibedakan. Oleh karena itu gambar digital dengan ekstensi *.PNG adalah yang terbaik digunakan untuk Steganografi dengan keamanan berlapis dilihat dari faktor banyaknya noise yang dihasilkan.

Selain memiliki tingkat noise yang rendah, gambar digital dengan ekstensi *.PNG juga memiliki selisih ukuran yang paling kecil sehingga gambar digital dengan ekstensi *.PNG juga merupakan terbaik digunakan untuk Steganografi dengan keamanan berlapis dilihat dari faktor selisih ukuran gambar.

Kebalikan dari gambar digital dengan ekstensi *.PNG, gambar digital dengan extensi *.BMP memiliki noise yang tinggi sehingga kurang baik digunakan untuk Steganografi dengan keamanan berlapis pada penenlitian ini dilihat dari faktor tingkat noise. Sedangkan untuk faktor besarnya ukuran file, gambar digital dengan ekstensi *.BMP juga adalah yang paling buruk karena memilik selisih ukuran paling tinggi dengan gambar asal sehingga akan lebih mudah dicurigai oleh pihak ang tidak diinginkan.

Pada ujicoba dengan metode kuantitatif dapat dilihat hasil pada gambar 10 bahwa 50 sampel gambar digital yang diuji semuanya berhasil, maka pada ujicoba kuantitatif ujicoba yang berhasil adalah 100% dan yang gagal adalah 0%.

Salah satu solusi keamanan yang dapat ditambahkan adalah kriptografi terhadap pesan rahasia yang akan disampaikan. Pada penelitian ini diterapkan keamanan pada steganografi dengan menambahkan kriptografi Caesar Cipher yang telah dimodifikasi dengan membalik urutan pesan rahasia kemudian digeser 5 karakter kemudian menggunakan enkripsi SHA-512. Setelah mengalami enkripsi tersebut pesan rahasia kemudian disisipkan kedalam gambar digital dengan metode Least Significant Bit (LSB) yaitu setiap bit pesan rahasia disisipkan pada bit terakhir gambar digital.

Setelah dilakukan pengujian dapat diketahui bahwa aplikasi dapat menyembunyikan pesan rahasia dengan keamanan berlapis dan bekerja pada gambar digital dengan ekstensi populer dan sering digunakan terutama dalam komunikasi pada jaringan internet, yaitu *.JPG, *.PNG, *.GIF dan *.BMP. Dari hasil evaluasi diketahui file dengan ekstensi *.PNG memiliki sifat paling baik untuk digunakan sebagai cover image pada steganografi dengan keamanan berlapis. Dengan demikian steganografi memiliki keamanan berlapis yang memberikan tingkat keamanan lebih baik

Berdasarkan hasil penelitian yang telah dilakukan, maka saran yang dapat diberikan penulis sebagai acuan untuk penelitian lebih lanjut adalah sebagai berikut:

1) Pada penelitian lebih lanjut disarankan bahwa media yang disisipi pesan rahasia bisa berupa file audio atau video.
2) Penelitian juga dapat dilanjutkan dengan membangun aplikasi yang disarankan dilengkapi dengan user login

Pada penelitian selanjutnya juga disarankan dapat menerapkan aplikasi ini pada perangkat lainnya seperti smartphone dan smart TV sehingga lebih.

DAFTAR PUSTAKA

[1] S. Anwar, “Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES,” *J. Format*, vol. 6, no. 1, pp. 2089–5615, 2017.

[2] A. M. A., Solikin, and Ismail, *Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java dengan Penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit*. 2012.

[3] “M. Definition of Steganography,” *Webster*, 2000. http://www.merriam-webster.com/dictionary/steganography.

[4] N. Tiwari and D. M. Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format," *Int. J. Comput. Appl.*, vol. 6, no. 2, pp. 1–4, 2010, doi: 10.5120/1057-1378.

[5] "Secure Hash Algorithm," *Wikipedia*. https://en.wikipedia.org/wiki/SHA-2.

[6] "Least Significant Bit," *Wikipedia*. http://en.wikipedia.org/wiki/Least_significant_bit.

[7] N. D. Nathasia and a. E. Wicaksono, "Penerapan Teknik Kriptografi Stream-Cipher Untuk Pengaman Basis Data," *ICT Research Center UNAS*, vol. 6, no. 1. pp. 1–22, 2011.

[8] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Alfabeta, 2012.

[9] Prasetyo, Bambang, and J. L. M., *Metode Penelitian Kuantitatif*. Jakarta: PT. Rajagrafindo Persada, 2005.

[10] "Signal to noise ratio," *Wikipedia*. http://en.wikipedia.org/wiki/Signal-to-noise_ratio.