Simposium Nasional Ilmiah dengan tema: (Peningkatan Kualitas Publikasi Ilmiah melalui Hasil Riset dan Pengabdian kepada Masyarakat), 7 November 2019, hal: 348- 357 ISBN: 978-623-90151-7-6 DOI: 10.30998/simponi.v0i0.313

PENGEMBANGAN TEKNIK MENYEMBUNYIKAN PESAN RAHASIA DENGAN KEAMANAN BERLAPIS MENGGUNAKAN PENGGABUNGAN METODE STEGANOGRAFI dan KRIPTOGRAFI CAESAR CIPHER YANG TELAH DIMODIFIKASI Dan MD5

Yesi Puspita Dewi
Universitas Budi Luhur
yesi.puspitadewi@budiluhur.ac.id

ABSTRAK

Komunikasi dalam dunia virtual menjadi cepat dan praktis. Karena faktor privasi maka perlu menjaga sifat rahasia, sehingga kemanan menjadi faktor penting. Steganografi bisa menyembunyikan pesan rahasia dengan disisipkan pada multimedia, salah satunya citra digital. Tetapi sayangnya faktor keamanan steganografi belum maksimal. Teknik steganografi kian populer sehingga banyak tersedia aplikasi untuk mengangungkap pesan rahasia dari dalam *stego image*. Pesan rahasia menjadi mudah diungkap oleh pihak yang tidak dikehendaki. Penelitian ini menigkatkan keamanan pada steganografi dengan kriptografi Caesar Cipher yang telah dimodifikasi dengan membalik urutan pesan rahasia kemudian digeser 5 karakter dan MD5, pesan rahasia kemudian disisipkan kedalam gambar digital dengan metode *Least Significant Bit (LSB)*. Pengujian dilakukan dengan metode kualitatif dengan *Power Signal Noise Ratio (PSNR)* serta perubahan ukuran file dan metode kuantitatif. Dari hasil evaluasi telah diketahui aplikasi penguji dapat menyembunyikan pesan rahasia pada gambar digital dengan ekstensi populer.
Kata kunci : Caesar Cipher, Kriptografi, *Least Significant Bit*, MD5, *Power Signal Noise Ratio*, Steganografi

ABSTRACT

Communication in the virtual world becomes fast and simple. Because of the privacy issue it needs confidential, so security becomes an important factor. Steganography can hide secret messages into multimedia such as digital image. However, risk factors for steganographic safety have not been maximum level. Steganography techniques are became popular so there are many applications available to uncover secret messages from a stego image. This research improves security on steganography with Caesar Cipher cryptography which has changed the secret message then shifted 5 characters and MD5, the secret message is then inserted using a digital image with the Least Significant Bit (LSB) method. The tests conducted using qualitative methods with Power Signal Noise Ratio (PSNR) and changes in file size and quantitative methods. From the evaluation results it is known that the test application can hide secret messages on digital images with popular extensions.
Keyword **:** *Caesar Cipher, Cryptography, Least Significant Bit, MD5, Power Signal Noise Ratio, Steganography*

PENDAHULUAN

Komunikasi melalui jaringan internet semakin popular karena dapat dilakukan dengan mudah dan melalui banyak media, sehingga faktor privasi dan keamanan adalah hal yang penting dalam berkomunikasi melalui jaringan internet. Untuk menghindari kasus kebocoran informasi yang terjadi, salah satu metode yang digunakan untuk mengamankan pesan rahasia adalah Steganografi. Teknik steganografi adalah meyisipkan pesan rahasia melalui media digital seperti citra, video, maupun suara.

Seiring waktu, banyak penelitian yang dikembangkan mengenai 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 telah diubah kedalam bentuk biner dengan cara menyisipkannya pada pixel terakhir yang menyusun file tersebut. Beberapa aplikasi menggunakan teknik ini dan dapat

digunakan secara bebas dengan mengunduhnya dari internet adalah OpenStego dan Silent Eyes. Dengan semakin populernya dan banyak digunakan, perlu kemanan tambahan pada Steganografi sehingga apabila pesan rahasia tersebut berhasil diekstrak oleh pihak yang tidak diinginkan, pesan tersebut tetap belum dapat terungkap.

Pada penelitian ini, penulis mengunakan 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.

METODE

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 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.

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 [Prasetyo 2005]

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 MD5 sehingga menjadi hash karakter yang acak, dapat dilihat padasimulasi berikut:
Pesan : ANGGA KUSUMA NUGRAHA
Tahap 1 : AHARGUN AMUSUK AGGNA
Tahap 2 : FMFWLZS4FRZXZP4FLLSF
Tahap 3 : f45e089132ec5e062eebaa4e99844afc

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*. 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.

HASIL

Setelah peneliti melakukan proses analisis dan perancangan sistem, selanjutnya peneliti akan melakukan implementasi sistem yang telah melalui tahap perancangan tersebut. Pada tahap ini peneliti akan membagi penelitian ini menjadi bagian-bagian yang menjelaskan kokmponen yang harus diperhatiakn dalam implementasi sistem. Tahap ini meliputi spesifikasi perangkat keras, perangkat lunak, dan implementasi program.

Berikut ini adalah spesifikasi dari perangkat keras yang digunakan dalam implementasi sistem dan eksperimen aplikasi Steganografi dengan keamanan berlapis.

Tabel 1. Spesifikasi Perangkat Keras

Perangkat Keras	Spesifikasi
Komputer	▪ Prosesor: Intel Core i5 2,5 Ghz ▪ Memori: 4 GB ▪ *Storage*: 500 GB ▪ Sistem operasi: Microsoft Windows 7 Professional 32 bit

Sedangkan perangkat lunak yang digunakan adalah seperti yang ditunjukkan dalam tabel di bawah ini.

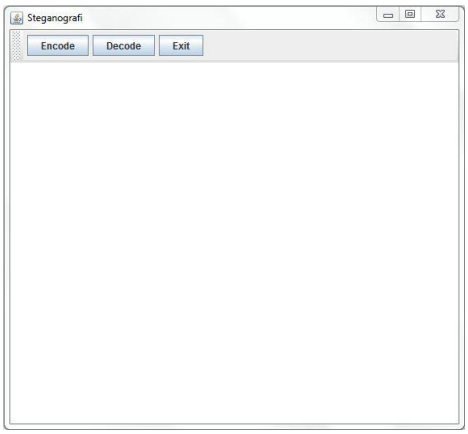
Tabel 2. Spesifikasi Perangkat Lunak

Perangkat Lunak	Spesifikasi
Java Development Kit	JDK 1.7.2.1
JCreator	Pro 3.0.0

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.

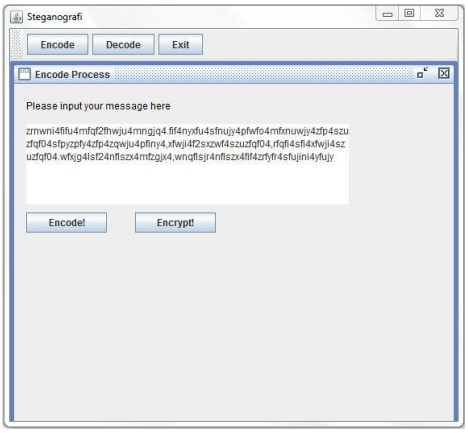
Pada saat pertama kali aplikasi Steganografi ini dijalankan, yang akan muncul adalah halaman utama dari aplikasi ini. Halaman utama ini memiliki tiga buah tombol, yaitu '*Encode*', '*Decode*' dan '*Exit*'. Tampilan layar halaman utama dapat dilihat pada gambar dibawah ini.



Gambar 1. Halaman Utama

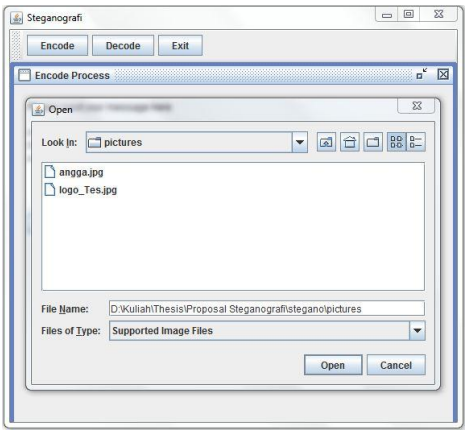
Tahap yang pertama pada mode *encode* adalah proses enkripsi. Dapat dilihat pada gambar 1 terdapat text area pada halaman *encode process* untuk memasukan pesan rahasia yang akan disisipkan. Pengirim dapat mengisi text area tersebut dengan pesan

rahasia yang dikehendaki. Setelah itu pengirim perlu menekan tombol '*Encrypt!*' untuk melakukan enkripsi terhadap pesan rahasia tersebut.



Gambar 2. Halaman *Encode Process* Setelah Enkripsi

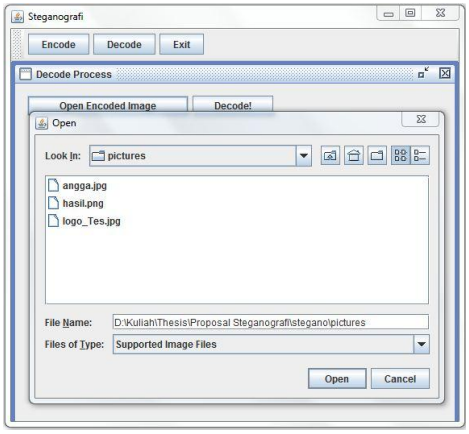
Setelah pesan rahasia dienkripsi, selanjutnya adalah memilih *cover image* dan melakukan encode pesan rahasia kedalam *cover image* yang telah dipilih. Untuk memilih *cover image*, pengirim hendaknya menekan tombol '*Encode!*'. Akan muncul jendela *browse cover image*, pengirim dapat memilih *cover image* 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 3. 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.

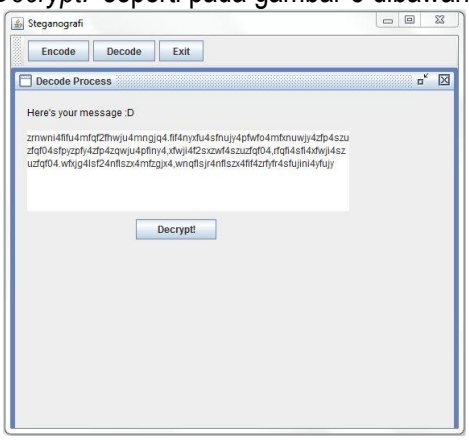
Untuk memilih *stego image* yang akan diekstrak pesan rahasianya, maka penerima pesan harus menekan tombol '*Open encoded image*'. Apabila tombol tersebut ditekan, maka akan tampil jendela *browse stego image*. pada jendela tersebut penerima pesan dapat memilih stego image dari direktori komputer penerima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



Gambar 4. Tampilan *Browse Stego Image*

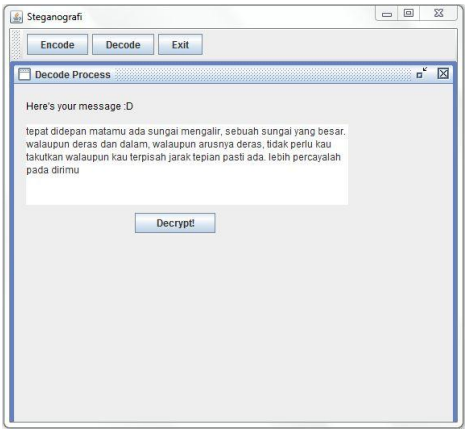
Proses selanjutnya adalah melakukan decode terhadap stego image yang dipilih. Untuk melakukan decode pada stego image yang telah dipilih pada proses sebelumnya, penerima pesan harus menekan tombol '*Decode!*' pada halaman *decode process* yang ditunjukan pada gambar 4.

Apabila penerima menekan tombol '*Decode!*' maka akan tampil halaman *decode process* dengan tombol '*Decrypt!*' seperti pada gambar 5 dibawah ini.



Gambar 9. 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*'.



Gambar 10. Halaman *Decode Process* Setelah Dekripsi

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)*.

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.

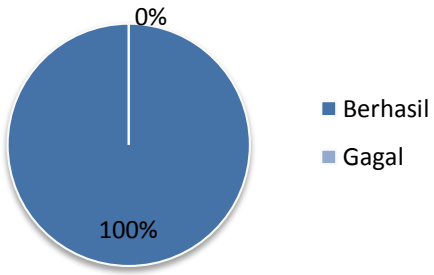
Tabel 3. Hasil Uji Kualitatif Berdasarkan Noise

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 4. 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 statistik.



Gambar 11. Hasil Uji Kualitatif

Setelah dilakukan pengujian dengan metode kualitatif dan kuantitatif, maka dapat dievaluasi bagaimana kemampuan alat penguji sebagai cerminan dari penelitian ini.

Ujicoba kualitatif dapat diketahui hasilnya dari tabel 3, terbukti aplikasi dapat 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 4, 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 yang 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%.

SIMPULAN

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 lalu dienkripsi lagi dengan MD5. 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
3. Pada penelitian selanjutnya juga disarankan dapat menerapkan aplikasi ini pada perangkat lainnya seperti smartphone dan smart TV sehingga lebih

DAFTAR RUJUKAN

Jamilia Aeni, Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ

M. Anggrie Andriawan, Solikin & Setia Juli Irzal Ismail, Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java dengan Penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit, 2012.

Khalil Challita, Hikmat Farhat, *Combining Steganography and Cryptography: New Directions* dengan kombinasi algoritma MCO *(multiple cover object*), 2011.

John Crinnion, Evolutionary Systems Development, a practical guide to the use of prototyping within a structured systems methodology - Page 18. Plenum Press, New York, 1991.

Eiji Kawaguchi, *Invitation to BPCS Steganography,* 2011, http://datahide.com/BPCSe/index.html, (Diakses 18 Juni 2013).

Shamim Ahmed Laskar dan Kattamanchi Hemachandran, *Secure Data Transmission Using Steganography And Encryption Technique* dengan kombinasi algoritma DCT (*Discrete cosine transformations*), 2012.

Miftahur Rahim A.A, Achmad Hidayanto & R. Rizal Isnanto, Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung menggunakan metode kualitatif dan algoritma CBC (*cipher block channel*), 2006.

Kavita Kadam, Ashwini Koshti & Priya Dunghav, *Steganography Using Least Signicant Bit Algorithm* dengan kombinasi algoritma DCT (*Discrete cosine transformations*), 2012.

Jithesh K, A V Senthil Kumar Dr., *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography,* 2012.

David, A. Murtado & Utin Kasma, Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode *Least Significant Bit* dengan teknik *pseudo-random number generator* (PRNG), 2012.

Namita Tiwari and Dr. Madhu Shandilya, *Evaluation of Various LSB based Methods of Image Steganography on GIF File Format*, International Journal of Computer Applications, vol. 6, September 2010.

Novi Dian Nathasia dan Anang Eko Wicaksono, Penerapan Teknik Kriptografi *Stream Cipher* Untuk Pengamanan Basis Data menggunakan algoritma *Caesar Cipher,* 2011.

Niels Provos, *First Steganographic Image in The Wild*, 2001, http://www.citi.umich.edu/u/provos/stego/abc.html, (Diakses 18 Juni 2013).