Jurnal Ilmu Komputer dan Desain Komunikasi Visual Volume 5, Nomor 1, Juli 2020
ISSN (Cetak) : 2541-4550 ISSN (Online) : 2541-4585

Pengembangan Teknik Steganografi dengan Kriptografi Modifikasi dari *Caesar Cipher* dan SHA-256 untuk Merahasiakan Pesan

Yesi Puspita Dewi

Program Studi Sistem Informasi, Fakultas Teknologi Informasi,
Universitas Budi Luhur
Jln. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260.
yesi.puspitadewi@budiluhur.ac.id

Abstrak

*Komunikasi menggunakan media digital menjadi cepat dan praktis. Dengan adanya faktor privasi maka diperlukan sifat rahasia, sehingga kemanan menjadi 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 dapat 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 SHA-256, 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 dengan metode kualitatif didapatkan file dengan ekstensi *.PNG memiliki hasil terbaik, sedangkan metode kuantitatif menunjukan tingkat keberhasilan 100%.*

Kata kunci *— Caesar Cipher, Least Significant Bit, Power Signal Noise Ratio, SHA-256, Steganografi*

Abstract

*Communication using digital media becomes fast and simple. Because of the privacy issue it needs confidential, so security becomes an important. Steganography can hide secret messages into multimedia such as digital image. However, risk factors for steganographic safety is not maximum yet. Steganography techniques are became popular so there are many applications available to uncover secret messages from a stego image, so that the secret messages can be revealed by wrong people. This research improves security on steganography with Caesar Cipher cryptography which has been modified, the secret message then shifted 5 characters and SHA-256, the secret message is then inserted into 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 with kualitatif method results it is known that file with *.PNG extension have the best result, while kuantitatif method has result 100% success.*

Kata kunci *— Caesar Cipher, Least Significant Bit, Power Signal Noise Ratio, SHA-256, Steganografi*

1. PENDAHULUAN

Komunikasi melalui jaringan internet menjadi semakin populer sebab dapat dilakukan dengan mudah dan melalui berbagai media, oleh sebab itu faktor privasi dan keamanan adalah hal yang penting dalam berkomunikasi melalui jaringan internet (Janssen, 2018). Agar terhindar dari kasus kebocoran informasi yang terjadi, salah satu metode yang digunakan untuk pesan rahasia menjadi aman adalah Steganografi. Teknik steganografi dapat diartikan penyisipan pesan rahasia melalui media digital seperti halnya citra, video, maupun suara (Jitesh, 2012).

Seiring waktu, banyak penelitian yang dikembangkan terkait teknik Steganografi. Ditemui terdapat berbagai metode untuk dapat menyisipkan pesan rahasia kedalam gambar dengan 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 binari dengan cara menyisipkannya pada *pixel* terakhir yang menyusun suatu file citra (Hutapea, 2018). Sayangnya 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 apabila pesan rahasia berhasil diambil oleh pihak yang tidak diinginkan, pesan tersebut tetap belum dapat terungkap dan diketahui.

Penelitian yang dijadikan acuan pada penelitian ini yaitu sebagai berikut, Penelitian mengenai *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography*. Penelitian ini melakukan enkripsi gambar rahasia menjadi *n* image sharing. Gambar dipecah menjadi beberapa (‘n’), setiap n-1 tidak menunjukkan informasi tentang gambar asli. Setiap gambar dicetak terpisah, dan dekripsi dilakukan dengan menggabungkan file sharing tersebut. Ketika semua *n* yang digabung, gambar asli akan muncul. Sebagai perbandingan, satu gambar digital bermuatan piksel acak dan gambar digital lain bermuatan informasi rahasia. Keamanan berlapis pada penelitian ini efektif namun terlalu rumit dan membutuhkan *resource* dan waktu yang lama untuk proses (Jitesh, 2012). Selain itu penelitian mengenai *Secure Data Transmission Using Steganography And Encryption Technique* dengan kombinasi algoritma DCT (*Discrete cosine transformations*). Proses enkripsi dengan cara menggeser ke kanan sebanyak *‘n’* dan menggeser ke kiri sebanyak *‘n’* karakter sebagai deskripsi (Laskar, 2012).

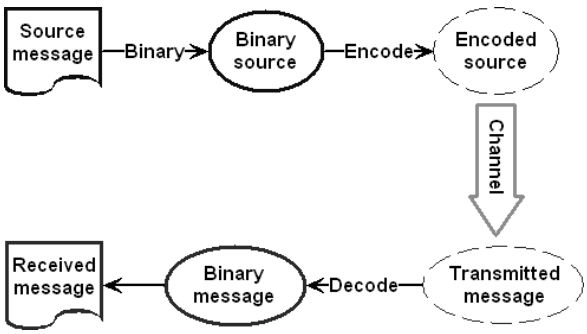
Sedangkan penelitian dengan judul *Steganography Using Least Signicant Bit Algorithm* dengan kombinasi algoritma DCT (*Discrete cosine transformations*), menyisipkan pesan rahasia kedalam gambar yang dilindungi dengan password pribadi yang terenkripsi (Kadam, 2012). Dan juga penelitian mengenai kriptografi yaitu Implementasi Enkripsi Data *Secure Hash Algorithm* (SHA-256) dan *Message Digest Algorithm* (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. Mengembangkan sistem dengan kamanan berlapis menggunakan kriptografi berlapis

melibatkan Data *Secure Hash Algorithm* (SHA-256). Dari hasil pengujian yang dilakukan yaitu dengan menggunakan *software attack* hasil penyandian cukup aman dari serangan *brute force*. Dari pengujian *avalanche effect* (AE) diperoleh hasil dengan nilai 71% yang artinya hasil baik (Sulastri, 2018).

Berdasarkan beberapa tersebut, dapat disimpulkan bahwa Steganografi efektif untuk menyembunyikan pesan rahasia, tetapi perlu tambahan keamanan berupa kriptografi, dan kriptografi *Secure Hash Algorithm* (SHA-256) adalah kriptografi yang dapat diandalkan terlebih jika digabungkan dengan kriptografi berlapis sehingga kemanan pesan rahasia lebih terjaga. 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 menggunakan metode LSB. Dengan cara ini pesan yang disampaikan keamanannya lebih terjaga dan tidak mudah terungkap oleh pengguna yang berusaha mencuri informasi.

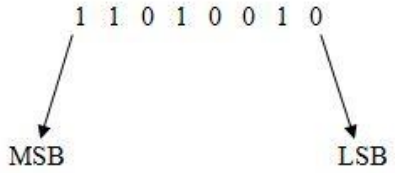
2. METODE PENELITIAN

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 (Kawaguchi, 2019).



Gambar 1. Ilustrasi Dasar Konsep Steganografi

Dalam Steganografi pesan rahasia disembunyikan dalam citra digital dengan mengganti *bit* data didalam segmen gambar dengan *bit* pesan rahasia. *Least Significant Bit* (LSB) adalah metode modifikasi yang paling sederhana . 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).

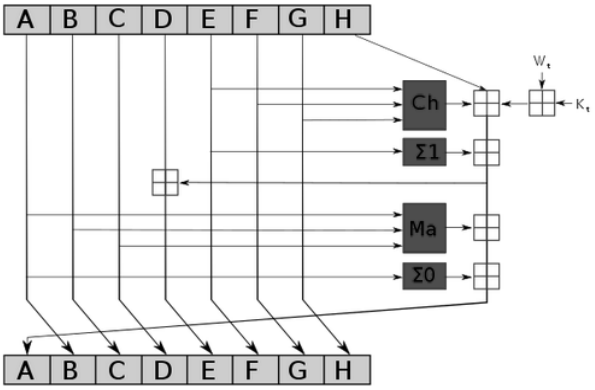


Gambar 2. Bit pada MSB dan LSB

Least Significant Bit adalah metode penyisipan pesan rahasia pada bit rendah atau bit yang paling kanan pada piksel yang menyusun file gambar tersebut. (Hutapea, 2018). Sebuah *cipher* adalah algoritma yang digunakan untuk enkripsi dan kebalikannya dekripsi. *Caesar Cipher* dikenal juga dengan Geseran Caesar adalah sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Ilustrasi cara kerja sandi ini seperti membuat barisan dua set alfabet sandi disusun dengan menggeser alfabet pada umumnya kekanan atau kekiri dengan angka tertentu (angka ini disebut kunci). Dapat dilihat sandi Caesar dengan kunci 3, sebagai berikut:

Alfabet biasa : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet sandi : DEFGHIJKLMNOPQRSTUVWXYZABC

SHA-256 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-256 tidak jauh lebih kompleks untuk dikodekan daripada SHA-1, dan belum dikompromikan dengan cara apapun. Kunci 256-bit menjadikannya fungsi kunci yang baik untuk AES. Hal ini didefinisikan dalam standar NIST (Institut Standar dan Teknologi Nasional) 'FIPS 180-4' (Munir, 2006).



Gambar 3. Bagan Satu Iterasi Pada Proses SHA-2

Metode yang dilakukan sebagai langkah awal dalam observasi teknik Steganografi dan Kriptografi adalah studi pustaka dengan mempelajari landasan teori yang dibutuhkan 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.

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-256 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 :
797FB69E7D2A21342D0BEBDAD0C705ADC08E59F536662036E70AF97F84BA7BFF

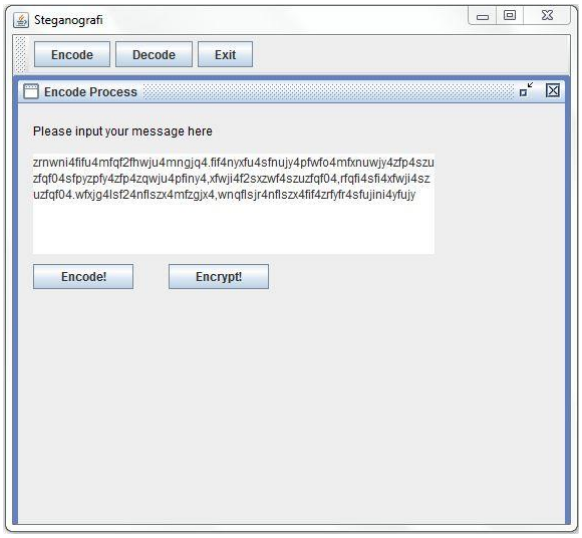
Hasil dari tahap 3 diatas yang akan disisipkan pada citra digital menggunakan steganografi. Hasil dari penelitian ini bukan aplikasi melainkan pemgembangan sistem steganografi, akan tetapi untuk membuktikannya perlu dibuat sistem penguji. Metode yang digunakan dan desain untuk membangun sistem penguji tidak akan dibahas karena bukan merupakan fokus pada penelitian ini. Pada penelitian ini ujicoba 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*, kemudian akan diuji tingkat *Power Signal Noise Ratio* (PSNR) antara file gambar yang belum disisipi pesan dengan gambar setelah menjadi *stego image*. PSNR

adalah tingkat kerusakan atau *noise* pada suatu citra digital yang disebabkan oleh *image processing* (Purwadi, 2015). 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

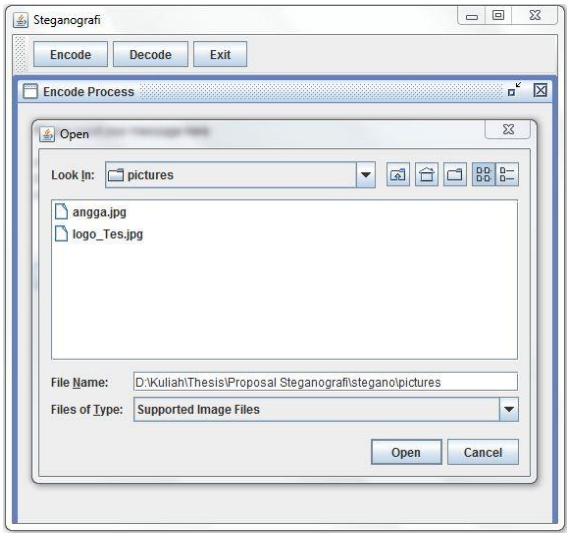
Peneliti ini telah melakukan implementasi sistem dengan penerjemahan teknik steganografi dengan kriptografi modifikasi dari *Caesar Cipher* dan SHA-256 menjadi baris code bahasa pemrograman Java, sehingga untuk melakukan pengujian dapat dilakukan dengan tampilan layar program. Pada saat pertama kali aplikasi Steganografi ini dijalankan, yang akan muncul adalah halaman utama yang memiliki tiga buah tombol, yaitu '*Encode*', 'D*ecode*' dan '*Exit*'.

Tahap yang pertama pada mode *encode* adalah proses enkripsi. Dapat dilihat pada gambar 4 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, hal ini ditunjukan pada Gambar 4.



Gambar 4. Halaman *Encode Process* Setelah Enkripsi

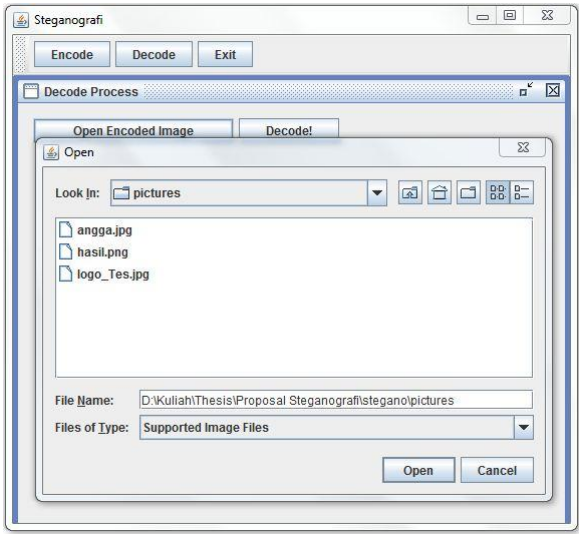
Setelah pesan rahasia dienkripsi, selanjutnya adalah memilih *cover image* dan melakukan encode pesan rahasia kedalam *cover image* yang telah dipilih. Untuk memilih *cover image*, pengirim hendaknya menekan tombol '*Encode!*'. Akan muncul jendela *browse cover image*, pengirim dapat memilih *cover image* 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, hal ini ditunjukan pada Gambar 5.



Gambar 5. 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.

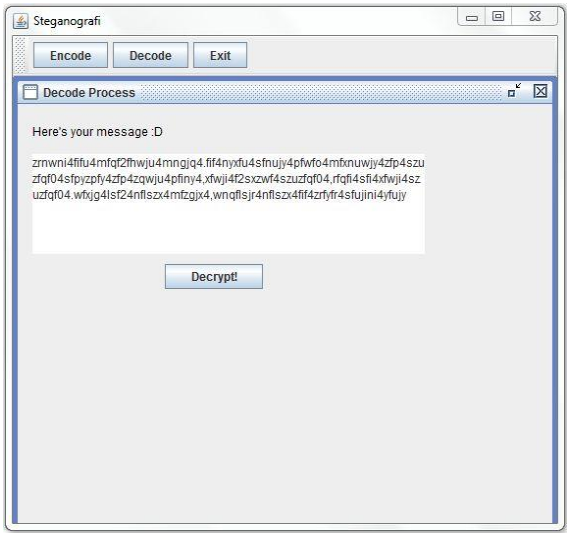
Untuk memilih *stego image* yang akan diekstrak pesan rahasianya, maka penerima pesan harus menekan tombol '*Open encoded image*'. Apabila tombol tersebut ditekan, maka akan tampil jendela *browse stego image*. pada jendela tersebut penerima pesan dapat memilih stego image dari direktori komputer penerima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



Gambar 6. Tampilan *Browse Stego Image*

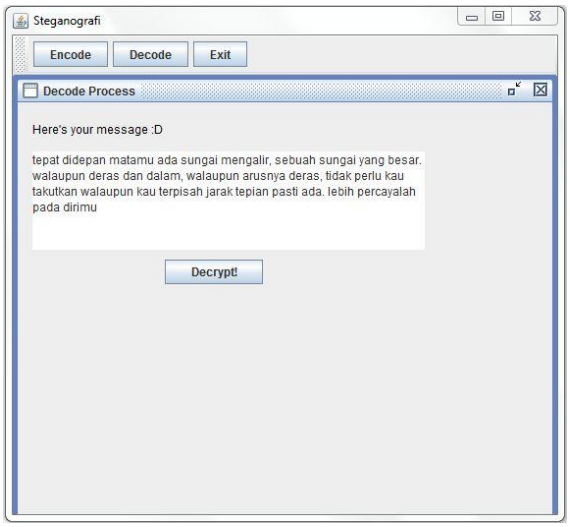
Proses selanjutnya adalah melakukan decode terhadap stego image yang dipilih. Untuk melakukan decode pada stego image yang telah dipilih pada proses sebelumnya, penerima pesan harus menekan tombol '*Decode!*' pada halaman *decode process* yang ditunjukan pada gambar 7. Apabila penerima menekan tombol '*Decode!*' maka akan

tampil halaman *decode process* dengan tombol '*Decrypt!*' seperti pada Gambar 7 dibawah ini.



Gambar 7. 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 8. Halaman *Decode Process* Setelah Dekripsi

Pengujian kualitatif dilakukan pada alat penguji dengan sample 4 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.

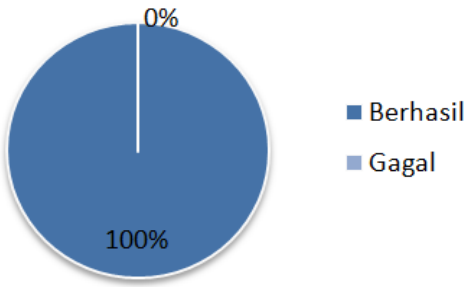
Tabel 1. Hasil Uji Kualitatif Berdasarkan *Noise*

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 statistik.



Gambar 9. Hasil Uji Kualitatif

Ujicoba kualitatif dapat diketahui hasilnya dari Tabel 1, 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 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%.

4. KESIMPULAN

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. 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

5. SARAN

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

UCAPAN TERIMA KASIH

Pada kesempatan ini peneliti mengucapkan terima kasih kepada Universitas Budi Luhur yang telah memberikan fasilitas dan sarana sehingga dapat terlaksananya penelitian ini.

DAFTAR PUSTAKA

Andriawan, M. A., Solikin & Ismail, S. (2012*). Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java dengan Penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit.* Jurnal Telkom University. Diakses dari https://www.academia.edu/40397360/IMPLEMENTASI_STEGANOGRAFI_PADA_CITRA_DIGITAL_FILE_GAMBAR_BITMAP_BMP_MENGGUNAKAN_JAVA

Hutapea, D. Y. & Hutapea, O. (2018). *Watermarking Method Of Remote Sensing Data Using Steganography Technique Based On Least Significant Bit Hiding*. *International Journal of Remote Sensing and Earth Sciences* Vol.15. Diambil dari http://jurnal.lapan.go.id/index.php/ijreses/article/download/2824/2395

Janssen, C. (2018). *Share*. Diakses dari http://www.techopedia.com/definition/24839/information-sharing.

Jithesh, K. & Kumar, A. V. S., (2012). *Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography. Journal of Theoritical and Applied Information Technology,* 42-47.

Kadam, K., Koshti, A. & Dunghav, P. (2012). *Steganography Using Least Signicant Bit Algorithm dengan kombinasi algoritma DCT (Discrete cosine transformations).* International Journal of Engineering Research and Applications (IJERA). Diambil dari http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=B045064AF73AE754084 3C7C1DA569084?doi=10.1.1.417.10&rep=rep1&type=pdf

Kawaguchi, E. (2019) *Invitation to BPCS Steganography*, Diakses dari http://datahide.com/BPCSe/index.html.

Laskar, S. A. & Hemachandran, K. (2012). *Secure Data Transmission Using Steganography And Encryption Technique* dengan kombinasi algoritma DCT (*Discrete cosine transformations*). *International Journal of Cooperative Information Systems*. Diakses dari https://www.semanticscholar.org/paper/SECURE-DATA-TRANSMISSION-USING-STEGANOGRAPHY-AND-Laskar-Hemachandran/e53eec0df772f13bbac83f3722ad64206faeab65

Munir, R. (2006) Kriptografi. Penerbit Informatika. 11-12.

Murtado, D. A. & Kasma, U. (2012). *Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode Least Significant Bit dengan teknik pseudo-random number generator (PRNG).* Jurnal Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak. Diakses dari http://sisfotenika.stmikpontianak.ac.id/index.php/ST/article/view/65/69

Petitcolas, A. P., Anderson, R. J. & Kuhn, M. G. (1999). *Information Hiding -A Survey*, Proceeding of the IEEE, vol. 87, Issue 7, pp. 1062-1078.

Purwadi, A. (2015). *Skalabilitas Signal to Noise Ratio (SNR) pada Pengkodean Video dengan Error Gaussian*. Jurnal Rekayasa Elektrika Vol. 11 Universitas Syiah Kuala (Unsyiah). Diakses dari http://jurnal.unsyiah.ac.id/JRE/article/download/2243/pdf_2

Sulastri, S. & Putri, R. (2018) *Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan*. Jural Fakultas Teknik Universitas Negeri Semarang. Diakses dari https://journal.unnes.ac.id/nju/index.php/jte/article/view/18628

Tiwari N. & Shandilya, M. (2010). *Evaluation of Various LSB based Methods of Image Steganography on GIF File Format*, International Journal of Computer Applications. Diakses dari https://www.researchgate.net/publication/46279981_Evaluation_of_Various_LSB_based_Methods_of_Image_Steganography_on_GIF_File_Format

Webster, M. (2000). *Definition of Steganography*. Diakses dari http://www.merriam-webster.com/dictionary/steganography.