Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202294852
Vol. 9, No. 2, April 2022, hlm. 279-286 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

ANALISIS PENGARUH CITRA TERHADAP KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB

Agus Rakhmadi Mido[*1], Erik Iman Heri Ujianto[2]

[1,2]Universitas Teknologi Yogyakarta, Kabupaten Sleman
Email: [1] agus.rakhmadi.mido@student.uty.ac.id, [2] erik.iman@uty.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 18 Maret 2021, diterima untuk diterbitkan: 17 Februari 2022)

Abstrak

Keamanan data dan informasi saat ini merupakan aspek penting dalam proses pertukaran pesan melalui jaringan internet. Tanpa adanya keamanan sering kali pesan tersebut dimanfaatkan oleh oknums yang tidak bertanggung jawab. Oleh karena itu, keamanan data dibutuhkan perlindungan informasi yang akan dikirimkan kepada penerima. Teknik keamanan data dan informasi yang saat ini banyak digunakan yaitu kriptografi dan steganografi. Kriptografi dan steganografi adalah teknik keamanan informasi yang memiliki persamaan dalam hal keamanan. Pada penelitian ini, teknik yang digunakan adalah algoritma Kriptografi Rivest Shamir Adleman (RSA) dan algoritma Steganografi Least Significant Bit (LSB) untuk keamanan pesan. Analisis yang dilakukan terhadap kombinasi algoritma dalam penelitian ini meliputi analisis pengaruh variabel citra pada proses enkripsi dan dekripsi. Pengujian kualitas citra menggunakan teknik Normalized Cross Correlation (NCC), Structured Similarity Index Method (SSIM), Peak Signal to Noise Ratio (PSNR), dan Mean Square Error (MSE). Berdasarkan hasil pengujian menggunakan skema kriptografi RSA dan skema steganografi LSB mampu direkonstruksi dengan baik. Pengujian MSE pada ukuran citra 128x128 menghasilkan *error* terbesar dan terkecil pada ukuran 1024x1024. Pengujian PSNR citra berukuran 64x64 dan 128x128 menghasilkan nilai kurang dari 40 dB. Sedangkan ukuran 512x512 dan 1024x1024 memiliki nilai lebih dari 40 dB. Pengujian NCC dan SSIM menghasilkan nilai yang mendekati 1 dengan semakin besarnya ukuran citra.

Kata kunci: *Kriptografi, LSB, RSA, Steganografi*

ANALYSIS OF IMAGE EFFECT ON THE COMBINATION OF RSA CRYPTOGRAPHY AND LSB STEGANOGRAPHY

Abstract

Data and information security are currently an important aspect in the process of exchanging messages through the internet network. Without security, the message is often utilized by an irresponsible person. Therefore, data security is required to protect the information that will be sent to the recipient. Data security techniques and information that is currently widely used are cryptography and steganography. Cryptography is a technique for encoding data into encrypted data that is not understood, while steganography is a technique for hiding data into a medium that aims to protect messages from unauthorized. Cryptography and steganography have similarities in terms of security. In this study, the technique is Rivest Shamir Adleman (RSA) Cryptographic algorithm and the Least Significant Bit (LSB) Steganography algorithm for message security. The analysis of an algorithmic combination in this research includes analysis of variable influence image of the encryption and decryption process. Image quality testing uses the Normalized Cross Correlation (NCC), Structured Similarity Index Method (SSIM), Peak Signal to Noise Ratio (PSNR), dan Mean Square Error (MSE) techniques. Based on the testing using the scheme RSA cryptography and the scheme LSB steganography capable of reconstructed well. MSE testing on the size of the image of 128x128 produces the error biggest and the smallest on the size of 1024x1024. PSNR testing on the size of images 64x64 and 128x128 produces values under 40 dB. Meanwhile, the image sizes of 512x512 and 1024x1024 have values above 40 dB. Testing NCC and SSIM produce a value close to 1 with increasing size of the image.

Keywords: *Cryptography, LSB, RSA, Steganography*

1. PENDAHULUAN

Pertukaran informasi menjadi sangat mudah dan cepat seiring dengan perkembangan teknologi saat ini. Menurut Badan Pusat Statistik (BPS) dalam publikasinya pada tanggal 2 Desember 2019 yang berjudul Statistik Telekomunikasi Indonesia 2018. Pengguna internet mengalami kenaikan selama kurun waktu 2014-2018, yang ditunjukkan dari

meningkatnya persentase penduduk yang mengakses internet pada tahun 2014 sekitar 17,14 persen menjadi 39,90 persen pada tahun 2018. Data tersebut membuktikan pertukaran informasi melalui jaringan internet terus meningkat setiap tahunnya. Berdasarkan tingginya persentase tersebut, tidak hanya memberikan dampak yang baik tetapi juga memberikan dampak yang buruk.

Keamanan informasi adalah aspek terpenting dalam proses pertukaran informasi seperti mengirim pesan melalui media elektronik. Tanpa adanya keamanan sering kali terjadi penyalahgunaan informasi yang dapat merugikan sumber tersebut. Dengan demikian, keamanan informasi yang dipertukarkan turut menjadi hal yang sangat penting untuk dijaga, agar informasi tersebut hanya dapat di akses oleh orang-orang yang berhak. Salah satu teknik pengamanan data yang sering digunakan adalah kriptografi dan steganografi. Pengamanan data digunakan proses kriptografi dan steganografi. Perlindungan yang ditawarkan oleh steganografi dapat lebih ditingkatkan dan lebih kuat dengan menggunakan teknik enkripsi kriptografi sebelum menyembunyikan teks di dalam gambar (Rejani dkk., 2016). Kriptografi dan steganografi adalah teknik terbaik untuk meniadakan ancaman ini. Para peneliti saat ini mengusulkan pendekatan campuran dari kedua teknik karena tingkat keamanan yang lebih tinggi dicapai ketika kedua teknik digunakan (AL-Shaaby & AlKharobi, 2017)

Kriptografi adalah cara untuk mengacak informasi ke dalam berbagai bentuk yang tidak dapat dibaca sebelum diterjemahkan. Kelemahan dari pesan yang telah di acak dapat menimbulkan kecurigaan karena memungkinkan pelaku kejahatan untuk memanipulasi serta mengubah pesan acak yang mengakibatkan pesan rahasia menjadi rusak (Setiadi dkk., 2017).

Kriptografi asimetris adalah proses enkripsi dan dekripsi menggunakan kunci yang berbeda (Darwis, Prabowo, & Hotimah, 2018). Rivest Shamir Adleman (RSA) adalah salah satu kriptografi asimetris yang sering digunakan (Sulistiyorini & Prihanto, 2019). Algoritma RSA menggunakan sistem modern untuk dekripsi dan juga enkripsi informasi (AbdelWahab dkk., 2021). Tingkat keamanan yang tinggi menggunakan dua kunci yang berbeda yaitu kunci publik untuk enkripsi dan kunci *private* untuk dekripsi. Kunci yang digunakan didapatkan dari faktor bilangan menjadi faktor prima (Zulfikar dkk., 2019).

Steganografi merupakan cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainnya (Darwis, 2017). Metode steganografi yang baik, seharusnya dapat mengembalikan pesan dengan sempurna (Rehman dkk., 2019). Steganografi mempunyai dua domain yang umum digunakan yaitu spasial dan *transform*. Teknik yang sering digunakan adalah teknik Least Significant Bit (LSB) dengan domain spasial. Least Significant Bit (LSB) merupakan salah satu metode steganografi yang paling mudah diimplementasikan, yaitu dengan cara mengubah bit yang paling kurang berarti dalam sebuah *file*. Perubahan pada Least Significant Bit (LSB) hanya akan mengakibatkan perubahan yang hampir tidak berarti pada *file*. Implementasi teknik Least Significant Bit (LSB) dan teknik steganografi terbukti memberikan keuntungan dalam memberikan kualitas citra *stego* yang baik dan menjaga aspek *imperceptibility* (Handoyo dkk., 2018)

Citra digital menggunakan format *.bmp lebih baik dibandingkan dengan menggunakan gambar dengan format *.tiff, *.jpg dan *.png. Hal ini dikarenakan gambar dengan format *.bmp terdiri dari piksel yang berdiri sendiri dan mempunyai warna sendiri (Sekarwati & Budiman, 2017). Berdasarkan hal tersebut penggunaan gambar dengan format *.bmp lebih baik untuk melakukan *encoding* atau penyisipan karena ukuran gambar asli dengan gambar yang telah disisipi sama sehingga tidak terlihat kecurigaan (Hermansa dkk., 2019).

Pengujian kualitas citra banyak digunakan untuk mengevaluasi dan menilai kualitas citra asli dan *stego* citra seperti Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structured Similarity Index Method (SSIM), Human Vision System (HVS), Feature Similarity Index Method (FSIM), dan Normalized Cross Correlation (NCC) (Singh, 2019). Kualitas citra dari perspektif representasi, SSIM dan FSIM dinormalisasi, tetapi MSE dan PSNR tidak. Hal ini disebabkan oleh fakta bahwa MSE dan PSNR adalah *error* absolut, namun SSIM dan NCC memberikan kesalahan berbasis persepsi dan kesalahan pengartian. SSIM dan NCC secara komparatif lebih baik daripada metrik MSE dan PSNR dari perspektif visual manusia (Kasapbasi, 2019). Hasil pengujian kualitas yang baik digunakan tiga parameter PSNR, MSE dan NCC. PSNR, NCC semakin meningkat dan MSE semakin berkurang (Singh, 2017).

Penelitian (Kuncoro & Aditama, 2019) menggunakan kombinasi RSA dan LSB menunjukan waktu proses lebih banyak dipengaruhi oleh ukuran citra. Pada citra berukuran 250x250 piksel dibutuhkan waktu proses rata-rata 0.139 detik dan terus meningkat hingga 1.2 detik pada citra berukuran 1000x1000 piksel, sedangkan panjang pesan tidak terlalu berpengaruh terhadap lamanya waktu proses. Nilai PSNR tertinggi adalah 66.2185 dB sedangkan nilai PSNR terendah adalah 53.0696 dB. Sama seperti pada waktu proses, ukuran citra juga paling berpengaruh terhadap nilai PSNR dibandingkan data lain.

Penelitian (Jatmoko dkk., 2018) membandingkan metode LSB dan MSB. Data yang digunakan citra *cover* grayscale ukuran 256*256. Sedangkan citra pesan juga menggunakan citra grayscale dengan ukuran 128*64. Berdasarkan hasil uji komparasi pada penelitian ini dapat disimpulkan

bahwa metode LSB memiliki keunggulan pada kualitas citra *stego*. Terbukti bahwa nilai PSNR yang mencapai lebih dari 54 dB, nilai PSNR juga stabil.

Pada penelitian (Handoyo dkk., 2018) dengan metode LSB–RSA digunakan dua macam ukuran citra cover, yaitu dengan ukuran 512 × 512 piksel dengan ukuran pesan 128 × 128 piksel dan 256 × 256 piksel dengan ukuran pesan 64 × 64 piksel. Berdasarkan hasil pengujian tingkat *imperceptibility* yang tetap terjaga. Hal ini terbukti pada nilai PSNR 57.2258 dB, MSE 0.1232 dB, metode ini juga memiliki ketahanan pada serangan *salt* dan *pepper*.

Pada penelitian ini, peneliti menganalisis citra digital dengan metode kriptografi RSA dan steganografi LSB menggunakan pengujian kualitas citra NCC, SSIM, PSNR, dan MSE. Adapun bagian yang akan dijadikan bahan penelitian adalah media penampung yaitu citra pada proses enkripsi dan dekripsi. Tujuan dari penelitian ini untuk mengetahui pengaruh variabel citra terhadap tingkat keamanan pesan.

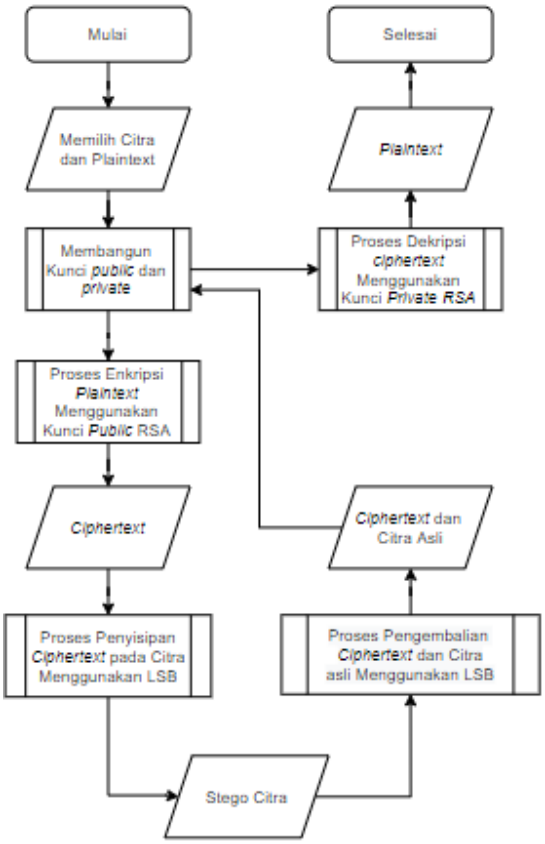
2. METODE PENELITIAN

Bahan yang digunakan dalam penelitian ini untuk steganografi adalah citra digital warna dari jurnal terkait. Sedangkan pada kriptografi digunakan *file* *txt untuk menuliskan pesan rahasia yang akan disisipkan kedalam media penampung. Pesan rahasia memiliki panjang bit yaitu 336, 3488, 14064, dan 149360 bit. Citra yang digunakan mempunyai ukuran ukuran 24x24, 128x128, 512x512, dan lebih dari 1024x1024. Pada setiap ukuran memiliki format *bmp, *png, *tiff, dan *jpeg/jpg.

Pengujian sistem dilakukan untuk membuktikan pengaruh variable citra terhadap proses enkripsi dan dekripsi pada steganografi dan kriptografi. Steganografi yang diusulkan menggunakan teknik LSB dan pada kriptografi digunakan algoritma RSA. Pada penelitian ini proses enkripsi dan dekripsi menggunakan algoritma RSA seperti berikut:

a. Bilangan prima p = 11 dan q = 19.
b. Menghitung nilai n dari perkalian p dan q.
c. Menghitung nilai phi dengan cara $\boldsymbol{\varphi = (p - 1) \times (q - 1)}$
d. Bilangan sebagai kunci enkripsi $(\boldsymbol{e})$ dimana bilangan tersebut lebih besar dari 1 dan lebih kecil dari phi $(\boldsymbol{\varphi})$.
e. Hitung nilai untuk kunci dekripsi dengan rumus $\boldsymbol{(d \times e)\ \%\ \varphi = 1}$
f. Kemudian pilih sebuah pesan $(\boldsymbol{M})$.
g. $\boldsymbol{M}$ adalah enkripsi dari $\boldsymbol{C = Me\ \%\ n}$.
h. $\boldsymbol{C}$ adalah enkripsi dari $\boldsymbol{M = Cd\ \%\ n}$.

Dimana p dan q bilangan prima (rahasia), $n = p \times q$ (tidak rahasia), $phi(n) = (p - 1)(q - 1)$ (rahasia), e (kunci enkripsi) (tidak rahasia), d (kunci dekripsi) (rahasia), M (*plainteks*) (rahasia), C (cipherteks) (tidak rahasia). Teknik LSB digunakan *embedding* dan ekstraksi, konsep dasar dari subtitusi LSB adalah dengan menggantikan data rahasia di paling kanan bit (bit dengan bobot terkecil) sehingga prosedur *embedding* tidak signifikan mempengaruhi nilai piksel aslinya.



Gambar 1. Proses Enkripsi dan Dekripsi

Penelitian ini menerapkan kombinasi antara metode kriptografi RSA dengan metode steganografi LSB seperti pada gambar 1. *Plaintext* yang akan digunakan adalah teks yang dituliskan kedalam *file* berformat *txt, sedangkan format *file cover image* yang berperan sebagai wadah menggunakan berbagai varisi citra. Pesan rahasia atau *plaintext* dienkripsi dengan kunci umum menghasilkan pesan acak (*ciphertext*), selanjutnya pesan acak diubah bentuknya menjadi *ciphertext* untuk disisipkan ke dalam media penampung citra digital menggunakan teknik Least Significant Bit (LSB) sehingga menghasilkan *stego* citra. Pada proses pengembalian pesan rahasia *stego citra* di ekstraksi menggunakan teknik LSB untuk mendapatkan *ciphertext* dan selanjutnya *ciphertext* di dekripsi menggunakan kunci *private* sehingga menghasilkan pesan rahasia atau *plaintext*. Sistem ini diterapkan menggunakan *software* Matlab R2018a.

Analisis hasil dilakukan untuk dapat mengetahui apakah sistem yang telah diujikan memiliki pengaruh terhadap proses kriptografi dan steganografi. Pengujian kualitas citra antara *stego* citra dan citra asli menggunakan beberapa parameter yang dijadikan sebagai kriteria penilaian objektif pada penelitian ini

adalah: Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Cross-Correlation (NCC), Structural Similary Index Measure (SSIM).

Pada pengukuran Mean Square Error (MSE) digunakan untuk mengetahui rata-rata kuadrat dari nilai kesalahan. Semakin rendah nilai MSE maka proses rekonstruksi sangat baik. PSNR digunakan setelah mendapatkan nilai MSE yang bertujuan untuk menentukan kualitas gambar setelah disisipi pesan. *Stego* citra dibandingkan dengan citra asli untuk mengatahui kualitas citra (Garg & Sharma, 2016). Semakin besar nilai PSNR artinya penyisipan pesan rahasia ke dalam citra asli tidak mengalami penurunan kualitas *stego* citra. Sebaliknya, semakin kecil nilai PSNR maka pada *stego* citra mengalami penurunan kualitas citra (Arun & Murugan, 2018).

Perhitungan NCC digunakan dalam proses pengenalan citra untuk menghasilkan nilai korelasi terbesar antara citra asli dan *stego* citra. Pengujian ini bertujuan untuk menunjukan tingkat akurasi kemiripan suatu citra. NCC dikatakan baik jika nilai mendekati nilai 1 (Saleh dkk., 2020).

Perhitungan SSIM digunakan untuk mengukur kesamaan antara dua gambar (citra asli dan *stego* citra). Indeks SSIM adalah metrik atau pengukuran atau prediksi kualitas citra didasarkan pada citra awal yang tidak terkompresi atau distorsi sebagai acuan. Perbedaannya dengan teknik lain seperti MSE atau PSNR adalah bahwa pendekatan ini memperkirakan kesalahan absolut (Sara dkk., 2019).

3. TINJAUAN PUSTAKA

Keamanan data dan informasi adalah salah satu aspek terpenting dalam pertukaran informasi melalui jaringan internet. Masalah ini mendorong para peneliti untuk melakukan banyak penelitian untuk meningkatkan kemampuan memecahkan masalah keamanan. Solusi untuk masalah ini adalah menggunakan citra yang baik untuk implementasi kombinasi kriptografi dan steganografi dalam satu sistem. Banyak penelitian mengusulkan metode untuk menggabungkan kriptografi dengan steganografi sistem dalam satu sistem.

Ada begitu banyak teknik kualitas gambar yang banyak digunakan untuk mengevaluasi dan menilai kualitas citra. Penelitian ini, peneliti menggunakan teknik MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), Normalized Cross Correlation (NCC), dan SSIM (Structured Similarity Metode Indeks) untuk menemukan kesesuaiannya. Adapun pembahasannya sebagai berikut:

Mean Square Error (MSE) adalah penaksir paling umum untuk metrik pengukuran kualitas gambar dengan sebuah metrik referensi lengkap dan nilai yang mendekati nol adalah lebih baik. Ukuran penduga yang menunjukkan bagaimana penaksir bervariasi dari yang diperkirakan. Dalam kaitannya dengan varians dan derajat distorsi dari rahasia asli MSE mengakses kualitas gambar yang direproduksi. Persamaan MSE seperti persamaan 1:

$$MSE = \frac{1}{YXZ}\sum_{i=1}^{Y}\sum_{j=1}^{Z}(m_{ij} - n_{ij}) \quad (1)$$

Peak Signal to Noise Ratio (PSNR) digunakan untuk menentukan kualitas gambar setelah disisipi pesan. *Stego* citra dibandingkan dengan citra asli untuk mengetahui kualitas citra. Semakin besar nilai PSNR artinya penyisipan pesan rahasia ke dalam citra asli tidak mengalami penurunan kualitas *stego* citra. Sebaliknya, semakin kecil nilai PSNR maka pada *stego* citra mengalami penurunan kualitas citra Baiknya nilai PSNR memiliki rentang nilai antara 20 dB sampai dengan 60 dB. Tertinggi sinyal yang mungkin dan nilai yang rusak karena kebisingan, yang mempengaruhi kesetiaan representasi antara direkonstruksi dan data asli ditentukan menggunakan PSNR (Jani Anbarasi dkk., 2020). Persamaan PSNR seperti persamaan 2.

$$PSNR = 10 \times 10\log\left[\frac{255^2}{MSE}\right] \quad (2)$$

Normalized Cross Correlation (NCC) adalah Metode untuk mengukur kemiripan citra berdasarkan fungsi korelasi (Sara dkk., 2019). Metode ini sering digunakan untuk menentukan kemiripan dua buah citra berdasarkan nilai ekstraksi ciri yang telah diolah sebelumnya (Saleh dkk., 2020). Persamaan yang digunakan untuk mencari nilai kemiripan tersebut dapat dinyatakan sebagai persamaan 3.

$$NCC = \frac{\sum_{X=1}^{N}\sum_{y=1}^{M}[a(x,y).b(x,y)]}{\sqrt{(\sum_{X}^{N}\sum_{y}^{M}[a(x,y)]^2)}.\sqrt{(\sum_{X}^{N}\sum_{y}^{M}[b(x,y)]^2)}} \quad (3)$$

Structural Similary Index Measure (SSIM) adalah model berbasis persepsi. Dalam metode ini, degradasi citra dianggap sebagai perubahan persepsi dalam informasi structural penggabungan. Metode SSIM digunakan untuk menilai tingkat kemiripan citra asli dan *stego* citra. Jika *stego* citra semakin mendekati nilai 1 maka semakin mirip dengan citra asli (Nurfitri & Suyanto, 2016). SSIM dapat dihitung dengan persamaan 4.

$$\mathrm{SSIM}(x,y) = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \quad (4)$$

4. HASIL DAN PEMBAHASAN

Pada penelitian ini, peneliti menggunakan citra warna dengan ukuran dan format *file* yang berbeda. Sedangkan pada kriptografi digunakan *file* dengan format **txt* yang terdapat pesan di dalamnya. Pesan yang digunakan juga memiliki panjang pesan yang berbeda dengan yang lain. Adapun pesan yang digunakan terdapat pada tabel 1.

Pesan rahasia tabel 1 digunakan untuk proses menyisipkan dalam media penampung. Sebelum penyisipan *plaintext* atau pesan rahasia tersebut dilakukan proses enkripsi. Proses enkripsi menghasilkan *ciphertext* yang lebih panjang dari *plaintext*. Dekripsi memiliki waktu yang lebih lama dibandingkan saat enkripsi. Panjang pesan juga

mempengaruhi waktu enkripsi dan dekripsi, semakin panjang pesan semakin lama waktu proses yang dibutuhkan.

Tabel 1. Daftar Pesan Rahasia (*Plaintext*)

Nama *File*	Panjang *Plaintext* (bit)	Waktu Enkripsi (*Second*)	*Plaintext* dan *Ciphertext*	Panjang *Ciphertext* (bit)	Waktu Dekripsi (*Second*)
Text 1	336	0.00089	99 161 38 52 161 98 116…	1168	0.001209
Text 2	3488	0.002316	99 161 38 52 161…	13128	0.003546
Text 3	14064	0.006048	15 129 58 129 20…	50120	0.012925
Text 4	149360	0.06843	140 52 161 27 147…	527048	0.136556

Proses dekripsi dilakukan dengan mengembalikan pesan seperti sebelum disisipkan atau *plaintext*. Teknik steganografi LSB dilakukan setelah proses enkripsi menghasilkan *ciphertext*. Penyisipan pesan acak atau *ciphertext* disisipkan dalam media penampung. Adapun media penampung yang digunakan yaitu terdapat pada tabel 2. Proses *decode* pada *stego* citra menghasilkan pesan acak. Pesan acak akan di dekripsi untuk mengembalikan pesan rahasia menjadi *plaintext*.

Tabel 2. Daftar Citra

Nama	Format	Ukuran (piksel)	Besar *file* (kb)
Jelly	bmp	64x64	17
Koala	jpg	64x64	13
Fruits	png	64x64	12
Wildflowers	tiff	64x64	17
Baboon	bmp	128x128	65
Hydrangeas	jpg	128x128	41
Parrot	png	128x128	40
House Color	tiff	128x128	65
Pepper	bmp	512x512	1025
Penguins	jpg	512x512	567
Airplane	png	512x512	440
Lena Color	tiff	512x512	769
Tiger	bmp	1200x1200	5656
London Bridge	jpg	1968x1968	940
Frymire	png	1118x1105	247
Marbles	tiff	1419x1001	2579

Tabel 2 adalah daftar citra yang digunakan sebagai media penampung. Citra tersebut memiliki 4 kelompok format citra dan 4 kelompok dimensi. Pada proses penyisipan atau proses *encode* menggunakan teknik LSB menghasilkan *stego* citra yang tidak memiliki perubahan pada ukuran dan format citra. Sedangkan, pengembalian pesan yang disisipkan atau proses *decode* pada teknik LSB juga tidak mengalami perubahan pada pesan rahasia.

Berikut adalah data hasil pengujian enkripsi dekripsi kriptografi dan steganografi. Data yang tertera merupakan hasil setiap kelompok berdasarkan ukuran citra dapat dilihat pada tabel 3 sampai dengan tabel 5.

Tabel 3. Hasil Pengujian Citra Ukuran 64x64

Nama dan Format	Enkripsi dan Ekstraksi			
	Text1	Text2	Text3	Text4
Jelly.bmp	✓	✓	×	×
Koala.jpg	✓	✓	×	×
Fruits.png	✓	✓	×	×
Wildflowers.tiff	×	×	×	×

Tabel 3 menunjukkan bahwa format tiff dengan ukuran 64x64 tidak dapat menyisipkan pesan rahasia. Sedangkan, format bmp, png, dan jpg dengan ukuran yang sama mampu menyisipkan text2 dengan panjang pesan 13128 bit. Pesan rahasia text3 dan text4 tidak dapat disisipkan karena panjang pesan melewati batas muatan citra.

Tabel 4. Hasil Pengujian Citra Ukuran 128x128

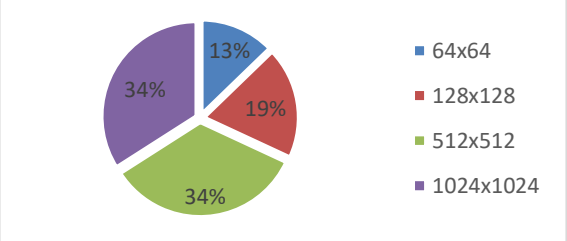
Nama dan Format	Enkripsi dan Ekstraksi			
	Text1	Text2	Text3	Text4
Baboon.bmp	✓	✓	✓	×
Hydrangeas.jpg	✓	✓	✓	×
Parrot.png	✓	✓	✓	×
House Color.tiff	×	×	×	×

Tabel 4 menunjukkan bahwa format tiff dengan ukuran 128x128 juga tidak dapat menyisipkan pesan. Sedangkan, format bmp, png, dan jpg dengan ukuran yang sama berhasil menyisipkan pesan text3 dengan panjang pesan hingga 50120 bit.

Tabel 5. Hasil Pengujian Citra Ukuran 512x512 dan 1024x1024

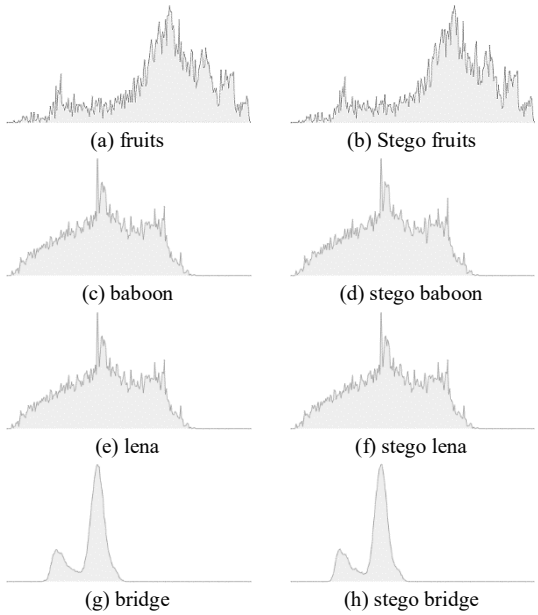
Nama dan Format	Ukuran (piksel)	Enkripsi dan Ekstraksi			
		Text1	Text2	Text3	Text4
Pepper.bmp		✓	✓	✓	✓
Penguins.jpg		✓	✓	✓	✓
Airplane.png	512	✓	✓	✓	✓
Lena Color.tiff		✓	✓	✓	✓
Tiger.bmp		✓	✓	✓	✓
London Bridge.jpg	1024	✓	✓	✓	✓
Frymire.png		✓	✓	✓	✓
Marbles.tiff		✓	✓	✓	✓

Tabel 5 menunjukkan bahwa setiap format dengan ukuran lebih dari 512x512 dapat menyisipkan pesan dengan panjang pesan hingga 527048. Hasil pengujian tabel 3-5 dibuat rangkuman keseluruhan digambarkan dalam diagram pie seperti berikut.



Gambar 2. Ringkasan Hasil Pengujian

Gambar 2 ringkasan hasil pengujian menunjukkan bahwa dalam proses penyisipan pesan citra dengan ukuran 64x64 memiliki persentase tingkat keberhasilan terendah yaitu 13%, disusul pada ukuran 128x128 juga memiliki persentase terendah kedua dengan nilai 19%. Sedangkan ukuran lebih dari 512x512 piksel mempunyai persentase yang baik dengan nilai 34%. Hal ini membuktikan citra dengan ukuran yang lebih besar baik digunakan untuk proses enkripsi-*embedding* maupun ekstraksi-dekripsi kombinasi kriptografi dan steganografi.



Gambar 3. (a), (c), (e), (g) histogram citra asli dan (b), (d), (f), (h) histogram dari stego citra

Gambar 3 menunjukan histogram antara citra asli dan citra *stego* dimana terdapat hanya sedikit perbedaan bahkan tidak terlihat adanya perbedaan. Hal ini menunjukkan bahwa teknik steganografi LSB terbukti memberikan keuntungan dalam memberikan kualitas citra *stego* yang baik dan menjaga aspek *imperceptibility*.

Berdasarkan hasil pengujian dilakukan pengukuran kualitas citra antara citra asli dan *stego* citra. Pengukuran kualitas citra yang digunakan yaitu MSE, PSNR, NCC, dan SSIM. Berikut pengukuran kualitas citra MSE disajikan dalam bentuk grafik pada tabel 6.

Tabel 6. Nilai Rerata Pengukuran MSE

Ukuran Citra (Piksel)	Mean Square Error (MSE)
64x64	0.0286357
128x128	0.0341504
512x512	0.0265277
1024x1024	0.0042826

Berdasarkan tabel 6 diketahui bahwa nilai MSE antara *stego* citra dengan *cover* citra memiliki *error* tertinggi pada citra berukuran 128x128 piksel. Hal ini disebabkan pada citra 64x64 memiliki banyak nilai *null*. Sehingga, perhitungan dari rata-rata citra ukuran 128x128 lebih besar dibandingkan citra terkecil berukuran 64x64. Dapat dilihat pada citra berukuran 64x64 piksel nilai MSE menunjukkan angka 0.028635669, citra berukuran 128x128 piksel nilai MSE naik menjadi 0.034150413, citra berukuran 512x512 piksel nilai MSE turun menjadi 0.026527725, dan terakhir pada citra berukuran 1024x1024 piksel nilai MSE kembali turun ke angka 0.004282579.

Tabel 7. Nilai Rerata Pengukuran PSNR

Ukuran Citra (Piksel)	Peak Signal to Noise Ratio (PSNR)
64x64	23.163125
128x128	36.01963125
512x512	71.61805
1024x1024	79.96560625

Tabel 7 menunjukkan bahwa ukuran citra mempengaruhi tingkat kemiripan antara *stego* citra dengan cover citra. Citra berukuran 64x64 piksel memiliki nilai PSNR 23.163125 dB. Citra berukuran 128x128 piksel nilai PSNR meningkat menjadi 36.01963125 dB. Citra 64x64 dan 128x128 memiliki banyak nilai null menyebabkan perhitungan rata-rata menghasilkan nilai kurang dari 40 dB. Citra berukuran 512x512 piksel meningkat menjadi 71.61805 dB, dan nilai PSNR meningkat lagi pada citra berukuran 1024x1024 piksel dengan nilai 79.96560625 dB. Hal ini dipengaruhi karena jumlah piksel yang disisipi pesan tidak berubah sedangkan ukuran gambar meningkat, sehingga rasio piksel yang mengalami perubahan semakin kecil pada gambar yang memiliki ukuran lebih besar.

Tabel 8. Nilai Rerata Pengukuran NCC

Ukuran Citra (Piksel)	Normalized Cross-Correlation (NCC)
64x64	0.374883563
128x128	0.562377063
512x512	0.99992825
1024x1024	0.99996575

Berdasarkan tabel 8 diketahui bahwa nilai antara *stego* citra dengan cover citra cenderung naik mendekati nilai 1 pada citra yang berukuran lebih besar. Dapat dilihat bahwa pada citra berukuran 64x64 piksel nilai NCC menunjukkan angka 0.374883563. Citra berukuran 128x128 piksel nilai MSE naik menjadi 0.562377063, pada citra 512x512 piksel mengalami kenaikan lagi menjadi 0.99992825 dan terakhir pada citra berukuran 1024x1024 piksel nilai NCC naik ke angka 0.99996575.

Tabel 9. Nilai Rerata Pengukuran SSIM

Ukuran Citra (Piksel)	Structural Similarly Index Measure (SSIM)
64x64	0.3749381
128x128	0.5624034
512x512	0.9997704
1024x1024	0.9999849

Tabel 9 menunjukkan hasil dari perhitungan SSIM cenderung naik pada citra yang berukuran lebih besar.

Pada citra berukuran 64x64 piksel nilai SSIM 0.374938125, citra ukuran 128x128 meningkat menjadi 0.562403375, citra berukuran 512x512 nilai SSIM menjadi 0.99992825, dan terus meningkat pada citra 1024x1024 piksel menjadi 0.99996575.

Berdasarkan hasil pengujian pesan yang dirahasiakan dengan menggunakan skema kriptografi RSA dan skema steganografi LSB mampu direkonstruksi dengan baik. Pesan rahasia di acak menggunakan algoritma RSA menghasilkan *ciphertext* yang kemudian disisipkan dalam *cover* citra. Bentuk penyandian pada steganografi menggunakan algoritma Least Significant Bit (LSB) di mana pesan berupa *ciphertext* diubah menjadi bentuk biner dan disisipkan ke dalam citra digital dengan mengganti bit terkecil tiap piksel citra tersebut dengan nilai bit pesan. Dalam skema yang digunakan pada penelitian ini pesan yang disisipkan ke dalam citra digital dapat direkonstruksi dengan baik.

Proses enkripsi-*embedding* maupun ekstraksi-dekripsi menggunakan kriptografi dan steganografi membuktikan variable citra seperti format dan ukuran memiliki pengaruh. Citra berukuran kecil memiliki batas muatan untuk penyisipan pesan. Dari 4 macam ukuran yang digunakan, citra berukuran 64x64 piksel tidak dapat melakukan proses enkripsi-dekripsi pada skema steganografi menggunakan pesan rahasia text3 dan text4. Pada citra ukuran 128x128 proses enkripsi-dekripsi juga tidak dapat dilakukan pada pesan rahasia text4. Sedangkan citra berukuran 512x512 dan 1024x1024 proses enkripsi-dekripsi berhasil dilakukan dengan baik. Pada format citra digunakan 4 macam tipe data, berdasarkan pengujian format tiff dengan ukuran 64x64 dan 128x128 tidak dapat melakukan enkripsi-dekripsi pada skema steganografi. Hal ini membuktikan variabel ukuran dan format pada citra berpengaruh pada proses enkripsi-*embedding* maupun ekstraksi-dekripsi.

Hasil pengukuran kualitas citra antara citra asli dan *stego* citra diketahui bahwa nilai rata-rata MSE terbesar terdapat pada ukuran citra 128x128 dengan nilai *error* 0.034150413 dan terkecil pada citra 1024x1024 dengan *error* 0.004282579. Pengukuran berdasarkan nilai rata-rata PSNR citra 64x64 dan 128x128 memiliki nilai dibawah 40 dB. Sedangkan citra berukuran 512x512 dan 1024 memiliki nilai kebalikannya yaitu lebih dari 40 dB dengan masing-masing nilai sebesar 71.61805 dB 79.96560625 dB. Pada pengukuran NCC terlihat ukuran citra 64x64 menghasilkan nilai rata-rata terjauh dari nilai 1 yaitu sebesar 0.374883563. Citra ukuran 512x512 dan 1024x1024 memiliki nilai yang mendekati 1 yaitu sebesar 0.99992825 dan 0.99996575. Berdasarkan pengukuran menggunakan SSIM citra ukuran 64x64 memiliki nilai rata-rata terendah sebesar 0.374938125 dan nilai rata-rata mendekati 1 terdapat pada citra 1024x1024 sebesar 0.99996575.

5. KESIMPULAN

Dari hasil penelitian dan pembahasan yang sudah dijabarkan dalam bab sebeumnya, dapat disimpulkan bahwa proses enkripsi-*embedding* maupun ekstraksi-dekripsi menggunakan teknik kriptografi RSA dan steganografi LSB memiliki pengaruh variabel citra. Hal ini dibuktikan citra berukuran kecil pada format tiff gagal saat proses penyisipan dan selain format tiff hanya gagal saat disisipkan pesan rahasia yang panjang. Sedangkan citra berukuran besar dengan semua format berhasil melakukan penyisipan. Pengukuran kualitas citra antara *cover image* dan *stego image* tidak memiliki distorsi yang terlihat (seperti yang terlihat dengan mata telanjang), dengan hasil tingkat kemiripan yang kuat untuk citra berukuran besar, hal ini dibuktikan dengan nilai PSNR, MSE, NCC dan SSIM yang relatif sangat baik dengan berbagai penyisipan panjang pesan.

Diketahui bahwa dalam penelitian yang dilakukan ini masih terdapat kekurangan dan diperlukan penelitian lebih lanjut guna menghasilkan penelitian yang lebih baik lagi. Oleh karena itu pada penelitian selanjutnya diharapkan dapat menggunakan parameter pengujian yang lebih banyak lagi. Faktor keamanan dengan menggunakan aplikasi *steganalysis* merupakan parameter perbandingan yang dapat dilakukan pada penelitian selanjutnya**.**

DAFTAR PUSTAKA

ABDELWAHAB, O.F., HUSSEIN, A.I., HAMED, H.F.A., KELASH, H.M. & KHALAF, A.A.M., 2021. Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data. Procedia Computer Science, 182, hal.5–12.

AL-SHAABY, A.A. & ALKHAROBI, T., 2017. Cryptography and Steganography: New Approach. Transactions on Networks and Communications, 5(6).

ARUN, C. & MURUGAN, S., 2018. Design of image steganography using LSB XOR substitution method. Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017, 2018-Janua, hal.674–677.

DARWIS, D., 2017. Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma GIFSHUFFLE. Jurnal Teknoinfo, 11(1), hal.19.

GARG, D. & SHARMA, G., 2016. Applications of Steganography in Information Hiding. , 3(1), hal.3–5.

HANDOYO, A.E., SETIADI, D.R.I.M., RACHMAWANTO, E.H., SARI, C.A. & SUSANTO, A., 2018. Teknik Penyembunyian

dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. Jurnal Teknologi dan Sistem Komputer, 6(1), hal.37–43.

HERMANSA, UMAR, R. & YUDHANA, A., 2019. Analisis Sistem Keamanan Teknik Kriptografi Dan Steganografi Pada Citra Digital (Bitmap). Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana, hal.1–9.

JANI ANBARASI, L., PRASSANNA, J., MD, A.Q., CHRISTY JACKSON, J., MANIKANDAN, R., RAHIM, R. & SUSEENDRAN, G., 2020. Visual secret sharing: A review. Journal of Critical Reviews, 7(9), hal.1212–1216.

JATMOKO, C., HANDOKO, L.B., SARI, C.A. & SETIADI, D.R.I.M., 2018. Uji Performa Penyisipan Pesan Dengan Metode Lsb Dan Msb. Dinamika Rekayasa, 14(1), hal.47–56.

KASAPBASI, M.C., 2019. A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption with Post-Quantum Security. IEEE Access, 7, hal.148495–148510.

KUNCORO, T.R. & ADITAMA, R., 2019. Analisis Kombinasi Algoritma Kriptografi Rsa Dan Algoritma Steganografi Least Significant Bit (Lsb) Dalam Pengamanan Pesan Digital. Statmat : Jurnal Statistika Dan Matematika, 1(2), hal.60–82.

NURFITRI, K. & SUYANTO, M., 2016. Penilaian Kualitas Pemampatan Citra Pada Aplikasi-Aplikasi Instant Messenger. Jurnal Ilmiah Multitek Indonesia, 10(2), hal.78–90.

REHMAN, A., SABA, T., MAHMOOD, T., MEHMOOD, Z., SHAH, M. & ANJUM, A., 2019. Data hiding technique in steganography for information security using number theory. Journal of Information Science, 45(6), hal.767–778.

REJANI, R., MURUGAN, D. & KRISHNAN, D. V, 2016. Digital Data Protection Using Steganography. ICTACT Journal on Communication Technology, 7(1), hal.1245–1254.

SALEH, A., HARAHAP, M. & INDRA, E., 2020. Kombinasi Jaringan Learning Vector Quantization Dan Normalized Cross Correlation Pada Pengenalan Wajah. JUSIKOM PRIMA (Junal Sistem Informasi Ilmu Komputer Prima), 3(2).

SARA, U., AKTER, M. & UDDIN, M.S., 2019. Image Quality Assessment through FSIM , SSIM , MSE and PSNR — A Comparative Study. Journal of Computer and Communications, (7), hal.8–18.

SEKARWATI, K.A. & BUDIMAN, A., 2017. Implementasi Algoritma Rivest-Shamir-Adleman (Rsa) Dan Metode Least Significant Bit(Lsb) Untuk Keamanan File Teks Dan Dokumen Menggunakan Visual C#. Jurnal Teknologi Rekayasa, 22(1), hal.54–62.

SETIADI, D.R.I.M., RACHMAWANTO, E.H. & SARI, C.A., 2017. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System, 2(1), hal.1–11.

SINGH, N., 2019. High PSNR based Image Steganography. International Journal of Advanced Engineering Research and Science, 6(1), hal.109–115.

SINGH, N., 2017. Survey Paper on Steganography. International Refereed Journal of Engineering and Science (IRJES), 6(1), hal.68–71.

SULISTIYORINI & PRIHANTO, A., 2019. Perbandingan Efisiensi Algoritma RSA dan RSA-CRT dengan Data Teks Berukuran Besar. Journal of Informatics and Computer Science, 01(02), hal.84–90.

ZULFIKAR, M.I., ABDILLAH, G. & KOMARUDIN, A., 2019. Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). Seminar Nasional Aplikasi Teknologi Informasi (SNATi) 2019, 2(1), hal.19–26.