Jurnal Masyarakat Informatika *ISSN: 2086-4930*
Vol. 13, No. 1, 2022 *e-ISSN: 2777-0648*

Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna

Christy Atika Sari[*1)], Wellia Shinta Sari[2)]**

[*]Program Studi Teknik Informatika, Universitas Dian Nuswantoro
[**]Program Studi Sistem Informasi, Universitas Dian Nuswantoro
[1)]christy.atika.sari@dsn.dinus.ac.id, [2)]wellia.shinta.sari@dsn.dinus.ac.id

Abstrak

Semakin berkembangnya internet dan aplikasi jaringan, membuat seseorang dapat bertukar pesan, informasi maupun data tanpa dibatasi oleh waktu dan jarak. Dengan adanya itu maka aspek keamanan dari data yang ditukarkan melalui internet dan aplikasi jaringan juga meningkat. Salah satu kategori keamanan komputer utama yang mengkonversi informasi dari bentuk normal ke bentuk yang tidak terbaca adalah kriptografi. Algoritma kriptografi yang popular saat ini adalah Chiper Block Chaining (CBC), algoritma ini merupakan metode kriptografi yang cukup handal dan stabil Algoritma ini paling umum digunakan pada protocol internet TLS dan IPsec. Teknik steganografi juga bisa digunakan untuk menjaga keamanan dan kerahasiaan pesan. Salah satu konsep steganografi adalah LSB. Perlunya digunakan metode pendeteksian tepi untuk memperbesar kapasitas penyisipan lebih banyak pada piksel tepi sehingga dapat menampung pesan lebih banyak tanpa terdeteksi, karena konsep LSB masih lemah. Metode Sobel adalah pendeteksian tepi yang paling umum dan merupakan metode yang terbaik untuk mendeteksi tepi pada grey-level. Setelah dilakukan pengujian menggunakan PSNR dan MSE. hasil penggabungan metode CBC dan LSB-Sobel ini dapat merahasiakan pesan dengan baik dan memiliki kualitas stego-image yang cukup tinggi.

Kata kunci : *Kriptografi , LSB-1, RSA, Steganografi*

Abstract

The development of the internet and network applications, allows a person to exchange messages, information and data without being limited by time and distance. With this, the security aspect of the data exchanged via the internet and network applications also increases. One of the main categories of computer security that converts information from normal to unreadable form is cryptography. The popular cryptographic algorithm today is Cipher Block Chaining (CBC), this algorithm is a fairly reliable and stable cryptographic method. This algorithm is most commonly used in TLS and IPsec internet protocols. Steganography techniques can also be used to maintain the security and confidentiality of messages. One of the concepts of steganography is LSB. It is necessary to use an edge detection method to increase the embedding capacity of more edge pixels so that it can accommodate more messages without being detected, because the LSB concept is still weak. The Sobel method is the most common edge detection and is the best method for detecting gray-level edges. After testing using PSNR and MSE. The result of combining the CBC and LSB-Sobel methods can keep messages secret and has a high enough stego-image quality.

Keywords : *Cryptography, LSB-1, RSA, Steganography*

1 PENDAHULUAN

Jaringan komunikasi yang terhubung antara satu dengan lain merupakan penerapan dari media internet. Pada era sekarang internet merupakan salah satu kebutuhan bagi para penggunanya karena dapat menyampaikan informasi serta bertukar informasi secara cepat tanpa batasan ruang maupun waktu. Dalam penyampaian informasi dibutuhkan akses yang cepat untuk mempermudah penyampaian informasi tersebut. namun di sisi lain terdapat dampak yang sering terjadi berkaitan dengan keamanan data dalam penukaran informasi di dunia maya, seperti halnya *hacking* dan *cracking* [1]. Kebutuhan dalam mengamankan pesan informasi pada gambar sangat dibutuhkan sekali contohnya dalam bidang fotografi [2]. Dibutuhkan suatu teknik penyembunyian atau penyandian dengan kode tertentu untuk seperti untuk seorang pemilik karya seni dalam bentuk citra digital dalam pendistribusian konten mereka yang bersifat rahasia dan terjaga, agar nantinya pesan yang diterima oleh client gambar yang di terima tetep terjaga keasliannya. Metode dalam penyembunyian pesan dengan media lain yang dikenal yaitu steganografi dan kriptografi [1]. Penyembunyian dengan teknik steganografi ditunjukan agar pesan yang disembunyikan dapat memanipulasi pesan sehingga tidak mudah terdeteksi terjadinya perubahan menurut indra penglihatan manusia yang sifatnya terbatas [3].

Salah satu metode steganografi yang diusulkan oleh [1] adalah metode *Least Significant Bit*, pada metode LSB menggunakan teknik substitusi dengan menggantikan nilai piksel pada bit terakhir dengan bit pesan hasil dari steganografi ini sering disebut stegano image. Tapi sayangnya metode LSB dinilai sederhana dan mudah diimplementasikan rentan terjadinya serangan. Uapaya memperbaiki metode ini dilakukan oleh oleh [4]-[5] dengan cara inverted bit LSB yaitu salah satunya metode LSB-1 adalah modifikasi dari metode LSB konvensional dengan menukarkan bit ke 8-1 (bit ke-7) dengan cara subtitusikan nilai bit piksel penampung dengan nilai bit piksel pesan. Menurut [4] modifikasi dengan cara inverted bit LSB dapat menghasilkan nilai *imperceptibilitas* yang tinggi yang nantinya menghasilkan gambar stegano image yang menyerupai gambar sampul.

Kriptografi merupakan teknik penyandian dengan pembuatan pesan dengan teknik enkripsi dan dekripsi dengan kode acak berbeda dengan steganografi [6]. Letak perbedaan kriptografi dan steganografi yaitu pada proses penyandiannya dengan menggunakan algoritma kunci [7]. Algoritma kunci yang dimaksud adalah kunci simetris dan asimetris.

Salah satu algoritma asimetris yaitu adalah algoritma RSA. Proses penyandian algoritma ini menggunakan dua kunci public dalam proses enkripsi dan kunci private proses dekripsinya. Algoritma RSA yang ditemukan pada tahun 1977 oleh peneliti Ron Rivest, Adi Shamir, dan Leonard Adleman penamaan dari algoritma RSA diambil dari 3 nama depan peneliti tersebut. Pada [8] telah dilakukan penelitian dengan menggabungkan algoritma LSB dan RSA dengan hasil stegano image ditunjukan dengan nilai PSNR 56.513.

Dari pemaparan latar belakang, dalam penelitian ini penulis menggunakan skema algoritma kombinasi LSB-1 dan RSA sebagai metode penelitiannya untuk diimplemantasikan dalam pengamanan data citra digital agar hasil citra enkripsi dapat menyimpan pesan asli tanpa mengurangi keaslian data sehingga hanya orang yang berhak yang dapat memulihkan informasi dengan benar pada proses deskripsi untuk melihat hasil evaluasi perhitungan perubahan citra sebelum dilakukan enkripsi dan setelah dilakukan dekripsi dapat diukur dengan MSR, PSNR dan Entropy.

2 TINJAUAN PUSTAKA

2.1 CITRA DIGITAL

Merepresantikan sebuah citra agar bisa diolah secara komputasi adalah pengertian dari citra digital. Citra digital adalah sebuah matriks dua dimensi yang terdiri dari *M* kolom dan *N* baris [9], yang dimana potongan antara kolom dan baris disebut juga piksel atau berupa potongan terkecil dari sebuah citra. Besarnya intensitas atau perubahan warna dari piksel dinyatakan pada nilai koordinat $f(x, y)$, menurut [10] terdapat jenis citra berdasarkan warnanya sebagai berikut :

a.) Citra keabuan atau *grayscale*, merupakan sebuah matriks yang memiliki derajat keabuan atau warna putih [9]-[11]. Kumpulan dari angka matriks di dalam citra disebut piksel. Piksel dalam citra keabuan ini mempunyai kedalaman warna 8 bit dan jarak antar 0 sampai 255 [9].
b.) Citra *true color* atau citra warna adalah suatu citra yang merepresentasikan warna tertentu. RGB dikenal dengan 3 unsur komponen warma yaitu *Red, Green,* dan B*lue* [10], [12]. Tiga komponen tersebut digunakan untuk representasi dan kecerahan tiap piksel dalam citra.
c.) Citra CMYK sering disebut juga warna subjektif printer karena pada proses seblum pencetakan citra RGB dilakukan konversi ke CMYK adalah suatu citra yang mempunyai komponen *Cyan, Magenta*, *Yellow* dan *Black* [13]

2.2 STEGANOGRAFI

Steganogafi adalah salah satu teknik penyembunyian pesan informasi. Pesan informasi tersebut dapat berupa text, gambar, audio maupun video. Steganografi ini merupakan perkembangan dari kriptografi yang memiliki peran untuk menyimpan suatu pesan informasi kedalam media tertentu agar pesan yang tersimpan tidak mudah diketahui keberadaan sekaligus dengan mata penglihatan manusia [14].

2.3 LEAST SIGNIFICANT BIT

Salah satu metode paling umum yang digunakan dalam penyembunyian pesan informasi menggunakan teknik substitusi dan merubah nilai bit dengan bit pesan rahasia adalah metode *Least Significant Bit* (LSB) [5]. Terdapat 2 teknik pada penyisipan pesan yang cukup terkenal yaitu penyisipan bit paling kanan (*Least Significant Bit*) dan penyisipan bit paling kiri (*Most Significant Bit*). Dimisalkan terdapat citra 24 bit, yang terdiri atas 3 byte merepresentasikan panel *Red, Green,* dan *Blue,* dengan ukuran 256 x 256 pixel, maka memperoleh bit yang dapat disisipkan sebanyak 256 x 256 x 3 = 196608 bit dan selanjutnya untuk nilai byte yang akan disembunyikan pada citra maksimum mencapai 196608 / 8 = 24576 byte.

2.4 METODE LEAST SIGNIFICANT BIT-1

Metode LSB-1 menyusun dengan merubah posisi yang akan ditukarkan dengan bit pesan yang akan disembunyikan. Pada umumnya LSB dilakukan mengubah nilai bit terakhir (bit ke-

8) maka untuk LSB-1 akan mengubah nilai bit terakhir ke-8 dikurangi dengan 1 (nilai LSB – 1) atau posisi sama dengan bit ke-7.

Berikut adalah contoh tahapan encode dengan LSB-1 pada citra dengan ukuran 3 x 3 [15] :

10110101	01111001	10101010
00001010	11010100	00000010
11101011	11111011	11111100

Kemudian, disisipkan pesan dengan diketahui biner 01010100 , sehingga dihasilkan hasil biner stegano citra sebagai berikut :

10110101	01111001	10101010
00001010	11010100	00000010
11101011	11111001	11111110

Contoh diatas merupakan penerapan dari memodifiksi metode *Least Significat Bit-1*, disimpulkan bahwa penukaran bit dilakukan tidak lagi pada bit terakhir *byte pixel*, maka stegano citra yang dihasilkan dapat memanipulasi pesan rahasia didalam medium pesan.

2.5 KRIPTOGRAFI

Kriptografi diambil dari bahasa Yunani *kryptos* berarti tersembunyi dan *graphien* berarti tulisan secara etimologi. Kriptografi diartikan sebagai disiplin ilmu yang mempelajari teknik penyandian pesan dengan aspek keamanan data [1] seperti kerahasian, keaslian, autentikasi data dan non-repudiasi [2], [7]. Teknik kriptografi telah ada sejak zaman romawi kuno, masa itu bangsa Yunani dalam menyampaikan pesan rahasia menggunakan alat yang bernama *scytale*. *Scytale* adalah alat berbentuk kayu yang digulung dengan kertas. Prinsip kerja alat *scytale* apabila kertas dibuka akan menghasilkan sandi yang sulit diterjemahkan.

2.6 RIVEST SHAMIR ADLEMAN

Pertama diperkenalkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Algoritma RSA sering dikenal sebagai algoritma asimetris karena menggunakan dua kunci dalam proses penyandian, yaitu kunci publik untuk proses enkripsi pesan *plaintext* menjadi *chipertext*, sedangkan kunci privat dirahasikan untuk proses dekripsi *chipertext* menjadi *plaintext* [16]. Algoritma RSA menjadi aman karena terdapat kesulitan pada pemfaktoran bilangan besar yang menjadi faktor bilangan prima [7], [17], [18]. Pemfaktoran yang dilakukan untuk memperoleh kunci pribadi. Pendapat juga disampaikan oleh AlSabti et al [16], keamanan algoritma RSA bergantung pada faktorisasi bilangan bulat untuk menemukan kunci privat.

Dalam algoritma RSA terdapat 3 proses yaitu : Pembangkitan kunci, proses enkripsi, dan proses dekripsi yang dijelaskan sebagai berikut ini [6] [16]. Proses pertama adalah pembangkitan kunci dengan Langkah sebagai berikut:

1. Ambil bilangan prima p dan q , dimana nilai $p \neq q$
2. Kemudian, hitung nilai $(Ø)n = p \cdot q$
3. Hitung fungsi Euler totient dengan rumus $n = (p - 1) \cdot (q - 1)$

4. Pilih bilangan prima acak dan tentukan nilai e sebagai kunci publik untuk enkripsi yang relative prima terhadap (Ø (*n*), e) = 1; dimana 1 < e <Ø (*n*)
5. Hitung dengan kunci dekripsi, d = e-1 (mod Ø (*n*)).
6. Diperoleh pasangan kunci, yaitu kunci publik (e, *n*) dan kunci privat (d, *n*)

Proses selanjutnya adalah enkripsi untuk mendapatkan chipertext dibutuhan persamaan rumus sebagi berikut :

$$C(M) = M^e \ mod \ n \quad (1)$$

dimana *C* adalah *Chipertext* , *M* adalah *Message* atau pesan yang akan disisipkan dan e adalah nilai kunci publik yang tidak dirahasikan.

Proses terakhir adalah dekripsi yang dilakukan dengan rumus persamaan

$$M(C) = C^d \ mod \ n \quad (2)$$

dimana d adalah kunci publik yang dibutuhkan untuk mengubah chipertext ke pesan asli.

2.7 MEAN SQUARE ERROR (MSE)

Nilai kesalahan kuadrat rata-rata dengan membandingkan selisih jarak antara piksel dari citra asli dengan nilai piksel citra yang sudah disisipkan pesan merupakan pengertian dari *Mean Square Error,* jumlah piksel antara kedua citra harus sama [19]. Metode ini dapat diterapkan pada *plain image* yang telah disisipkan gambar pesan atau *chiper image*. Rumus MSE dapat dilihat pada persamaan (3) sebagai berikut :

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} (C_i - S_i)^2 \quad (3)$$

Ci dan Si mewakili jumlah pixel i dari gambar asli dan gambar pesan, N untuk jumlah total piksel. Dikatakan kualitas citra yang baik jika menunjukan nilai MSE kecil [20], jadi semakin kecil nilai yang dihasilkan semakin bagus kualitas citra.

2.8 PEAK SIGNAL TO NOISE ROTION (PSNR)

Peak Signal to Noise Rotion adalah hasil hitung dari perbandingan nilai maksimal gambar hasil dengan nilai MSE, hasil dari nilai PSNR dinyatakan dengan desibel (dB). Metode ini berguna untuk mengukur kualitas citra yang sudah terkontruksi pada teknik steganografi. Jika, nilai PSNR besar menunjukan bahwa sedikit adanya perubahan pada *plain image* dengan *chiper image* atau gambar terenkripsi [21], sehingga dapat diartikan bahwa kualitas citra yang dihasilkan semakin baik [20]. Menurut [1], standart kualitas citra yang baik ditunjukan pada nilai 40 dB dan kualitas citra sangat baik tanpa drau ditunjukan pada nilai 60 dB. PSNR dapat dihitung dengan persamaan (4)

$$\text{PSNR} = 10 \log 10 \frac{\text{MAXi}^2}{\sqrt{\text{MSE}}} \quad (4)$$

Keterangan:
MAXi = Nilai maksimum, satuan piksel

MSE = nilai dari MSE

Pendapat lain juga disampaikan oleh [19] pada penelitiannya dengan menggunakan teknik kriptografi, bahwa kualitas yang baik dalam hasil enkripsi ditunjukan pada nilai PSNR yang lebih kecil dan nilai MSE yang lebih besar.

2.9 ENTROPY

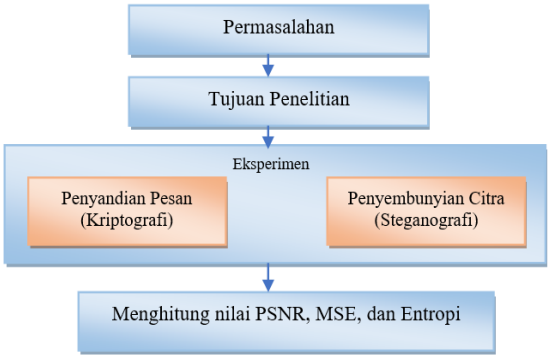
Parameter yang penting dalam menetukan informasi kemungkinan dari gambar yang dienkripsi mengandung pesan informasi tersembunyi adalah pengertian dari entropi [22] sehingga gambar mudah dienkripsi dan didekripsi secara matematis [19]. Persamaan (5) digunakan untuk menghitung nilai entropi

$$H(m) = -\sum_{i=0}^{2^n-1} P(m_i) log_2 P(m_i) \quad (5)$$

Dimana $P(m_i)$ adalah probabilitas keberadaan nilai level abu-abu dari piksel mi pada gambar dan log diambil untuk mewakili bit piksel. Dikarenakan nilai-nilai piksel gambar skala abu-abu adalah 256 tingkat abu-abu maka itu mengandung 8 bit, sehingga dengan perolehan nilai mendekati 8 dapat disimpulkan hasil gambar yang bagus [19].

3 METODE PENELITIAN

Fokus penulis pada metode penelitian ini adalah mengamankan pesan rahasia berupa citra dengan mengkombinasi teknik kriptografi dan steganografi. Algoritma RSA digunakan untuk menggabungkan citra pada proses enkripsi dan dekripsi berupa gambar cover. Selanjutnya metode steganografi digunakan pada penyisipan citra. Metode steganografi yang digunakan yakni metode *Least Significant Bit-1* (LSB-1).



Gambar 3. 1 Flowchart Penelitian

3.1 KEY GENERATE RSA

1. Memilih nilai p dan q yang merupakan bilangan prima.
2. Memilih nilai e yang relatif bilangan prima φ(n), dimana 1 < e < φ(n)
3. Program akan menghasilkan nilai n = pq dan φ(n) = (p–1)(q–1)
4. Program menghasilkan pasangan kunci (n,e) sebagai kunci publik.
5. Menghitung nilai d dengan aturan 1 < d < φ(n) seperti ed ≡ 1 mod φ(n)
6. Program telah menghasilkan pasangan kunci (n,d) sebagai kunci peivate kunci ini digunakan untuk menghasilkan citra pesan pada peoses dekripsi.

3.2 PROSES ENKRIPSI

1. Mengambil citra pesan informasi.
2. Memperoleh nilai matriks piksel elemen RGB citra pesan sebagai *plainimage m.*
3. Reshape perolehan nilai *plainimage m* menjadi vektor N x 1.
4. Lakukan penyandian menggunakan kunci yang dihasilkan sebelumnya yaitu kunci publik atau (n,e) selanjutnya lakukan perhitungan dengan rumus enkripsi ditunjukan pada Persamaan (2) sesuai urutan vektor.
5. Simpan citra pesan yang baru berupa citra chiper.

3.3 PROSES PENYISIPAN LSB

1. Mengambil citra pesan berupa citra chiper dan citra cover
2. Memperoleh nilai integer dari citra chiper.
3. Lakukan konversi menjadi biner 16 bit pada citra chiper.
4. Lakukan metode penyisipan citra chiper pada citra cover dengan metode LSB-1
5. Simpan citra cover baru berupa citra steganochiper yang telah berisikan pesan informasi.

3.4 PROSES EKSTRAKSI

1. Mengambil citra steganochiper
2. Memperoleh matriks tiap elemen RGB citra berupa bilangan integer
3. Lakukan transformasi menjadi bentuk vektor N x 1
4. Lakukan konversi bilangan menjadi biner 8 bit
5. Memisahkan citra cover dengan citra chiper
6. Proses ekstrasi berhasil dengan menampilkan citra chiper yang manghasilkan nilai biner 16 bit

3.5 PROSES DEKRIPSI

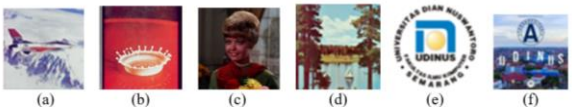
1. Mengambil citra pesan berupa citra chiper.
2. Memperoleh nilai biner 16 bit pada citra pesan.
3. Lakukan konversi bilangan biner menjadi desimal.
4. Lakukan penyandian menggunakan kunci privat (n,d) dan lakukan perhitungan dengan rumus Persamaan (3)
5. Proses dekripsi berhasil jika menghasilkan nilai *Plainimage m* berupa vektor selanjutnya ubah menjadi matriks kembali.
6. Simpan citra pesan

4 HASIL DAN PEMBAHASAN

Eksperimen pada penelitian ini dilakukan dengan menggunakan objek citra RGB sejumlah 5 data citra *cover* berukuran 256 x 256 dan 6 data citra pesan berukuran 64 x 64 dengan format bmp yang mana citra pesan akan disembunyikan dalam citra *cover*. Implementasi dilakukan pada program MATLAB dengan menggunakan metode yang diusulkan peneliti dan telah dijelaskan pada bab sebelumnya. Pada penerapan algoritma RSA citra pesan yang akan dilakukan penyandian ditunjukan pada Gmabar 2 dengan menggunakan

5 pasangan kunci publik dan privat yang berbeda-beda, mulai dari kunci yang pendek dengan kunci yang panjang, skema selanjutnya adalah melakukan penyisipan dengan menggunakan metode LSB-1 dengan menyisipan citra pesan ke dalam citra *cover* yang ditunjukan pada Gambar 1.

Gambar 1 Citra Cover Tree. bmp(1), Babbon.bmp(2), House.bmp(3), Female(4), Papper(5)



Gambar 2 Citra Pesan

Berikut adalah hasil perolehan dari proses enkripsi pada citra pesan dengan menggunakan algoritma RSA ditunjukan pada Tabel 1 sampai dengan Tabel 5 mengungkapkan bahwa gambar yang telah dilakukan penyandian berhasil mengelabuhi mata penglihatan manusia dimana citra pesan tidak terbaca secara baik. Hasil gambar dari proses enkripsi ini juga ditunjukan dengan perolehen nilai entropy ditunjukan pada Tabel 8.

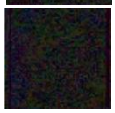
Selain itu, perolehan dari teknik penyisipan dengan menggunakan metode steganografi LSB ditujukan dengan hasil citra stegano baru sangat mirip dengan citra cover. Ini menunjukan bahwa skema yang diusulkan peneliti efektif sesuai dengan tujuan awal penelitian hasil dari proses penyisipan dapat dilihat dapa Tabel 2.

Tabel 1 Hasil Enkripsi pada Citra Pesan Cover 1

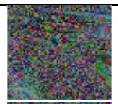
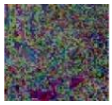
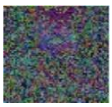
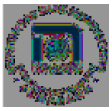
Kunci RSA	Inputan Pesan	Hasil
p=19 q=23 e=17	Chiperimage (a)	
	Chiperimage (b)	
	Chiperimage (c)	
	Chiperimage (d)	
	Chiperimage (e)	
	Chiperimage (f)	

Karena pada hasil stegano menunjukan kemiripan yang sama dengan citra cover, pengujian lain dilakukan dengan cara membandingkan perubahan nilai piksel dari kedua citra tersebut. Pengujian ini sering digunakan pada proses enkripsi untuk menguji analisis keamanan seperti hasil keseragaman histogram yang ditunjukan pada Tabel 7 dengan menghitung nilai MSE dan PSNR.

Tabel 2 Hasil Enkripsi pada Citra Pesan Cover 2

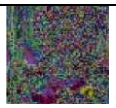
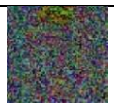
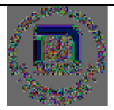
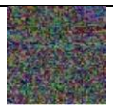
Kunci RSA	Inputan Pesan	Hasil
p=107 q=131 e=409	Chiperimage (a)	
	Chiperimage (b)	
	Chiperimage (c)	
	Chiperimage (d)	
	Chiperimage (e)	
	Chiperimage (f)	

Tabel 3 Hasil Enkripsi pada Citra Pesan Cover 3

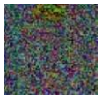
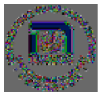
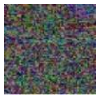
Kunci RSA	Inputan Pesan	Hasil
p=241 q=173 e=769	Chiperimage (a)	
	Chiperimage (b)	
	Chiperimage (c)	
	Chiperimage (d)	
	Chiperimage (e)	
	Chiperimage (f)	

Berdasarkan hasil dari percobaan yang dilakukan peneliti perolehan nilai PSNR yang ditunjukan dalam bentuk grafik seperti Gambar 4. Nilai PSNR tertinggi mencapai 45,1778 dB dengan hasil perolehan ini maka citra stegano yang dihasilkan memiliki kualitas citra yang baik dimana nilai PSNR mencapai lebih dari 40 dB.

Tabel 4 Hasil Enkripsi pada Citra Pesan Cover 4

Kunci RSA	Inputan Pesan	Hasil
p=191 q=229 e=823	Chiperimage (a)	
	Chiperimage (b)	
	Chiperimage (c)	
	Chiperimage (d)	
	Chiperimage (e)	
	Chiperimage (f)	

Tabel 5 Hasil Enkripsi pada Citra Pesan Cover 5

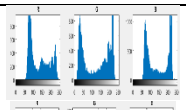
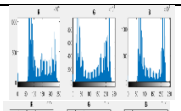
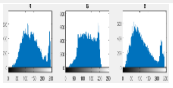
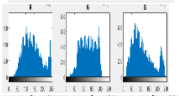
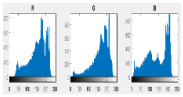
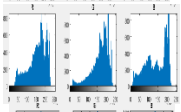
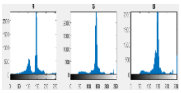
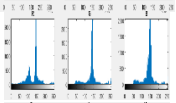
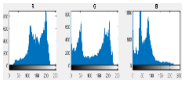
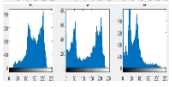
Kunci RSA	Inputan Pesan	Hasil
p=191 q=229 e=823	Chiperimage (a)	
	Chiperimage (b)	
	Chiperimage €	
	Chiperimage (d)	
	Chiperimage €	
	Chiperimage (f)	

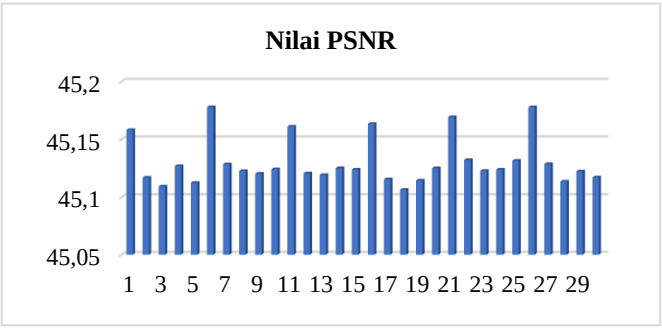
ISSN: 2086-4930
e-ISSN: 2777-0648

Tabel 6 Hasil Stegano dengan menggunakan Chiperimage (a) dan (b)

Kunci RSA	Citra Cover	Stegano	
		(a)	(b)
p=19 q=23 e=17	(1)		
p=107 q=131 e=409	(2)		
p=241 q=173 e=769	(3)		
p=191 q=229 e=823	(4)		
p=223 q=241 e=997	(5)		

Tabel 7 Perbandingan hasil histogram citra cover dan citra stegano dengan Chiperimage (a)

Kunci RSA	Citra Cover	Histogram Citra Cover	Histogram Citra Steganografi (a)
p=19 q=23 e=17	(1)		
p=107 q=131 e=409	(2)		
p=241 q=173 e=769	(3)		
p=191 q=229 e=823	(4)		
p=223 q=241 e=997	(5)		



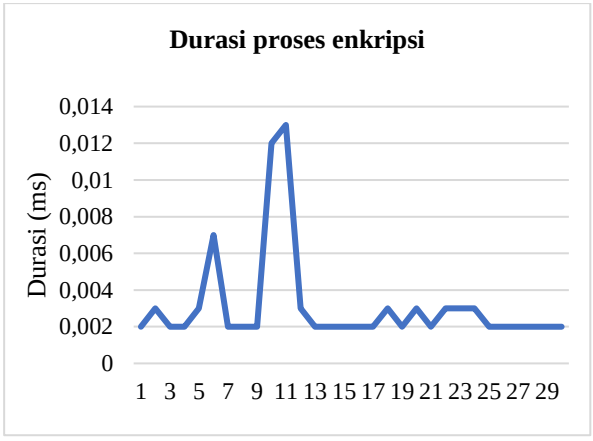
Gambar 3 Grafik perolehan nilai PSNR (dB)

Sebelum menghitung nilai PSNR, perolehan MSE menunjukan hasil 2,0066 dengan pencapaian tertinggi selama percobaan, sehingga hasil dari perbandingan nilai tersebut mempengaruhi kualitas citra *stegano.* Citra stegano dikatakan baik karena nilai MSE lebih rendah dari nilai PSNR.

Tabel 8 Tabel hasil perolehan nilai entropy

Citra Cover	Entropy
Tree.bmp	7,3103
Babbon.bmp	7,2223
House.bmp	7,2085
Female.bmp	5,5939
Papper.bmp	7,5694

Dari Tabel 8, dapat disimpulkan terdapat pesan informasi pada citra yang telah dilakukan proses enkripsi. Hasil yang didapat menunjukan terdapat sedikit perubahan pada citra tersebut dengan perolehan nilai tertinggi sebesar 7,5694 ditunjukan pada citra Papper.bmp yang mana nilai tersebut mendekati nilai standart entropi yaitu 8. Adapun untuk melihat hasil perolehan lamanya waktu proses enkripsi ditunjukan pada Gambar 4.



Gambar 4 Grafik perolehan waktu proses enkripsi

Pada gambar yang ditunjukan pada Gambar 4, dimana perolehan merupakan grafik fluktiatif yang mana keadaan grafik yang tidak stabil atau tidak tetap. Perubahan dengan pencapaian durasi terlama ditunjukan pada pecobaan ke-11 dengan perolehan waktu 0,0013 detik sedangkan pada perolehan durasi terpendek memperoleh durasi rata-rata 0,002 – 0,003 detik.

Menurut hasil yang ditunjukan pada Tabel 9 metode yang diusulkan oleh peneliti berbeda dibandingkan dengan metode lain yang telah ada sebelumnya baik dari hasil dengan meliputi parameter objek gambar yang digunakan pada metode [8] dimana citra pesan yang disisipkan berupa citra 8 bit atau citra keabuan. Metode lain [23] menggunakan penyisipan pesan LSB dengan metode konvensional hal ini menunjukan perbedaan pada skema yang kami usulkan dengan memodifikasi pengeseran satu bit menjadi ke bit-7 terakhir disetiap piksel citra. Selain itu, terdapat faktor yang mempengaruhi perolehan nilai perbandingan piksel adalah ukuran pesan rahasia. Jika ukuran pesan rahasia besar, maka jumlah perolehan bit berubah juga

semakin bertambah, hal ini dapat meningkatkan perolehan dalam penyembunyian secara efektif dengan memberikan pesan informasi tersembunyi ke dalam citra *cover.*

Tabel 9 Komparasi hasil implementasi dengan penelitian sebelumnya

Metode	Metode yang diusulkan	Metode dari R. Apau dan C. Adomako [23]	Metode X. Zhou, W. Gong, W. Fu, dan L. Jin [8]
Ukuran citra cover	256 x 256	512 x 512	256 x 256
Jenis citra cover	RGB	RGB	RGB
Jenis pesan yang disispkan	RGB (24 bit)	Teks	*Grayscale* (8 bit)
Ukuran pesan yang disisipkan	64 x 64	1500 chars	90 x 90
PSNR (dB)	45.1778	63.3886	56.513
MSE	1.9739	0.0298	-

5 KESIMPULAN

Kombinasi antara metode kriptografi dan steganografi yang diusulkan peneliti untuk penyisipan pesan informasi berupa pesan citra digital telah berhasil diterapkan pada penelitian ini. Pada tahapan enkripsi memggunakan RSA menghasilkan kualitas citra berupa pesan citra *chiper* sehingga sangat sulit untuk memulihkan informasi yang tersembunyi untuk pihak ketiga tanpa mengetahui kunci rahasianya dan faktor keamanan pada proses enkripsi ditunjukan dengan nilai entropi terbaik sebesar 7,5694 sedangkan untuk penyisipan dengan menggunakan modifikasi dari LSB-1 berhasil mendapatkan citra *stegano* dengan kualitas yang baik karena tampak dari citra *stegano* yang dihasilkam tidak terlihat perubahan yang signifikan adapun bukti lain dengan menghitung nilai PSNR dan MSE untuk mengetahaui perubahan dengan membandingkan piksel pada citra *cover*. Dari hasil tiap percobaan memperoleh nilai PSNR lebih dari 40 dB. Nilai PSNR terbaik dihasilkan mencapai 45,1778 dB dengan nilai MSE sebesar 1,9739.

DAFTAR PUSTAKA

[1] A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *J. Teknol. dan Sist. Komput.*, vol. 6, no. November 2017, pp. 37–43, 2018, doi: 10.14710/jtsiskom.6.1.2018.37-43.

[2] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, M. Mamat, and P. K. An, "Secure Image Steganography Using Encryption Algorithm," in *Internasional Conference on Intelligent Computing, Computer Science & Information System*, 2016, pp. 43–46.

[3] M. R. Rambe, E. V. Haryanto, and A. Setiawan, "Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android," in *Konferensi NAsional Sistem Informasi 2018*, 2018, pp. 8–9.
[4] E. J. Kusuma, C. A. Sari, and E. H. Rachmawanto, "A Combination of Inverted LSB , RSA , and Arnold Transformation to get Secure and Imperceptible Image Steganography," *ITB J.*, vol. 12, no. 2, pp. 103–122, 2018, doi: 10.5614/itbj.ict.res.appl.2018.12.2.1.
[5] P. Informatika, B. Darma, T. Zebua, and A. A. Kriptografi, "PENERAPAN METODE LSB-2 UNTUK MENYEMBUNYIKAN," *Pelita Inform. Budi Darma*, vol. X, 2015.
[6] S. Chepuri, "An RGB Image Encryption using RSA Algorithm," *Int. J. Curr. Trends Eng. Res.*, vol. 3, no. 3, pp. 1–7, 2017.
[7] C. Himawan, T. Wibowo, B. Sulityo, R. Roestam, Y. Wahyu, and R. B. Wahyu, "Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal," *Semin. Nas. APTIKOM*, vol. 6, no. 1, pp. 28–29, 2016.
[8] X. Zhou, W. Gong, W. Fu, and L. Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography," *IEEE ICIS*, pp. 4–7, 2016.
[9] D. I. S. Saputra, T. B. Pranata, and S. W. Handani, "Prototype Aplikasi Pengolah Citra Invert Sebagai Media Pengolah Klise Foto," in *Conference on Information Technology*, 2016, pp. 23–24.
[10] T. Zebua and E. Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 4, pp. 275–282, 2017, doi: 10.25126/jtiik.201744474.
[11] N. Nafi'iyah, "Algoritma Kohonen dalam Mengubah Citra Graylevel Menjadi Citra Biner," *J. Ilm. Teknol. Teknol. dan Informasia ASIA*, vol. 9, no. 2, pp. 49–55, 2015.
[12] Siswanto, A. Shofian, and M. Anif, "Aplikasi Kriptografi Video Menggunakan Algoritma Rivest Shamir Adleman (RSA)," in *Prosiding SENTIA*, 2015, vol. 7, pp. 53–58.
[13] L. Golben, "CMYK VS. RGB: WHAT'S THE DIFFERENCE?," 2013. .
[14] B. Damanik, "Penerapan steganografi pada sebuah citra," *J. Mahajana Inf.*, vol. 1, no. 2, pp. 1–7, 2016.
[15] T. Zebua, "PENGAMANAN DATA TEKS DENGAN KOMBINASI CIPHER BLOCK CHANING DAN LSB-1," in *Seminar Nasional Inovasi dan Teknologi Informasi 2015 (SNITI)*, 2015, no. September, pp. 85–89.
[16] K. D. M. AlSabti and H. R. Hashim, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB," *J. Pure Appl. Math.*, vol. 12, no. 4, pp. 3631–3640, 2016.
[17] H. J. Yakubu, T. Aboiyar, and P. B. Zirra, "An improved RSA image encryption algorithm using 1-D logistic map," *Int. J. Commun. Comput. Techonologies*, vol. 6, no. 1, pp. 1–6, 2018.
[18] A. H. Mansour, "Analysis of RSA Digital Signature Key Generation using Strong Prime," *Int. J. Comput.*, vol. 21, no. 1, pp. 28–36, 2017.
[19] A. Setyono, D. R. I. M. Setiadi, and M. Muljono, "Dual Encryption Techniques for Secure Image Transmission," *J. Telecommun. Electron. Comput. Enginnering*, vol. 10, no. 3, pp. 41–46, 2018.
[20] M. G. Gumelar, I. Fibriani, D. Setiabudi, and B. Supeno, "Analisis Sistem Pengenalan dan Keamanan Kriptografi Hill Cipher pada Plat Nomor Kendaraan Menggunakan Metode Template Matching," in *Prosiding Seminar Nasional XI "Rekayasa Teknologi Indrustri dan Informasi 2016 Sekolah Tinggi Teknologi NAsional Yogyakarta*, 2016, pp. 29–38.
[21] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," *Int. Conf. Smart Cities, Autom. Intell. Comput. Syst. (ICON-SONICS). IEEE*, no. November, pp. 87–92, 2017, doi: 10.1109/ICON-SONICS.2017.8267827.
[22] M. T. Gatta and S. T. A. Al-Latief, "Medical image security using modified chaos-based cryptography approach," *J. Phys. IOP Conf. Ser. 1003*, 2018.
[23] R. Apau and C. Adomako, "Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones," *Int. J. Comput. Appl.*, vol. 164, no. 1, pp. 13–22, 2017.