# IMPLEMENTASI ALGORITMA *RIVEST CODE* 6 (RC6) DAN *STEGANOGRAFI LEAST SIGNIFICANT BIT* (LSB) UNTUK KEAMANAN DATA CITRA DIGITAL

**Silvester Tena[1], Stephanie I. Pella[2], Brian J. Mooy[3]**

[1,2,3]*Program Studi Teknik Elektro, Fakultas Sains dan Teknik Universitas Nusa Cendana*
*Jl Adisucipto Penfui, Kupang, Indonesia 85000*
*Email: silvertena_unc@yahoo.com*

## *ABSTRACT*

*This study incorporates the Rivest Code 6 algorithm (RC6) and the Least Significant Bit (LSB) method. RC6 is an asymmetric cryptographic algorithm where locks on both the sender and receiver sides are the same. LSB is a method that inserts every bit of information into 1 byte of an image. The test results showed that the system went well by generating compute time that was affected by the image size. The bigger the image size than the longer the computation time. The original image and the output image are the same (MSE = 0). The container Citra before and after the insertion got the largest MSE 0.0488 and the smallest Psnr 141,021 DB. The combination of THE RC6 algorithm AND LSB method can withstand salt and pepper noise at a range of density 0.01-0.1 with MSE 7.904, 28-24.614, 1 AND PSNR 9, 89dB-21, 50dB.* The *Successful percentage of the extraction and decryption process is at a range of 24%-96%. The difference in MSE value, PSNR and the efficacy percentage of the extraction process are determined by data image characteristics. Pixel density is directly proportional to noise-resistance levels.*

**Keywords:** *cryptography, steganography, RC6, LSB, digital imagery*

## *ABSTRAK*

*Penelitian ini menggabungkan algoritma Rivest Code 6 (RC6) dan metode Least Significant Bit (LSB). RC6 merupakan algoritma kriptografi asimetris dimana kunci pada sisi pengirim maupun penerima sama. LSB merupakan metode yang menyisipkan setiap bit informasi ke dalam 1 byte gambar. Hasil pengujian menunjukkan bahwa sistem berjalan baik dengan menghasilkan waktu komputasi yang dipengaruhi oleh ukuran citra. Semakin besar ukuran citra maka semakin lama waktu komputasinya. Citra asli dan citra keluaran yang didapatkan sama (MSE=0). Citra wadah sebelum dan sesudah penyisipan mendapat MSE terbesar 0.0488 dan PSNR terkecil 141.021 dB. Kombinasi algoritma RC6 dan metode LSB dapat bertahan terhadap noise salt and pepper pada rentang density 0.01-0.1 dengan MSE 7.904,28-24.614,1 dan PSNR 9,89dB- 21,50dB. Persentase keberhasilan proses ekstraksi dan dekripsi berada pada rentang 24%-96%. Perbedaan nilai MSE, PSNR dan persentase keberhasilan proses ekstraksi ditentukan oleh karakteristik citra data. Kerapatan piksel berbanding lurus dengan tingkat ketahanannya terhadap noise.*

**Kata kunci:** *Kriptografi, Steganografi, RC6, LSB, citra digital*

## 1. PENDAHULUAN

Informasi berupa citra/gambar digital merupakan bentuk informasi yang cukup akurat dan terpercaya untuk mendeskripsikan sesuatu, sehingga tingkat keaslian dari informasi ini perlu dijaga. Untuk menjaga keamanan dan kerahasiaan informasi citra/gambar digital perlu adanya sebuah teknik yang disebut kriptografi.

Kriptografi merupakan teknik atau algoritma untuk mengubah sebuah data atau informasi menjadi berbeda dengan informasi aslinya. Teknik ini dikembangkan pertama kali oleh Julius Caesar untuk mengirimkan informasi kepada tentaranya di medan perang. Dalam algoritma kriptografi terdapat dua proses yaitu proses enkripsi dimana informasi asli (*plain)* akan diubah sedemikian rupa sehingga menghasilkan informasi (*chiper)* yang tampak berbeda dari pesan aslinya. Kemudian proses dekripsi untuk mengembalikan informasi hasil enkripsi (*chiper*) menjadi informasi asli (*plain*) sehingga dapat dilihat oleh penerima.

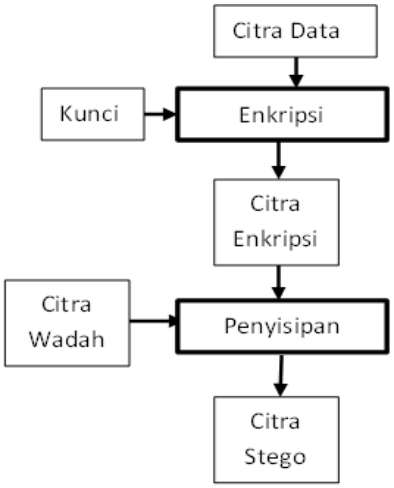
Salah satu metode yang dapat digunakan untuk melakukan kriptografi adalah metode *Rivest Code 6* (RC6). Algoritma RC6 merupakan salah satu

kandidat *Advanced Encryption Standard* (AES) yang diajukan oleh RSA Laboratoriest kepada *National Institute of Standards and Technology* (NIST). Dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin. Algoritma ini merupakan algoritma asimetris pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST.

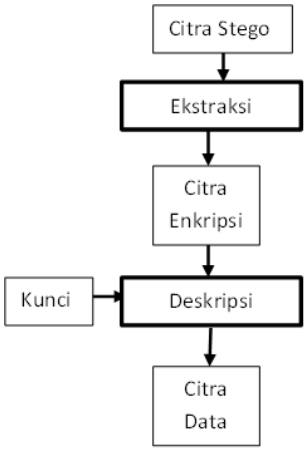
Namun kriptografi masih memiliki kelemahan, yaitu bentuk dari informasi hasil enkripsi (*chiper*) yang terlihat acak dan mencolok serta menarik perhatian orang lain. Oleh karena itu dibutuhkan teknik *steganografi* agar pesan dapat disamarkan dengan menyisipkannya kedalam sebuah media. Salah satu teknik *steganografi* adalah *Least Significant Bit* (LSB). Cara kerja LSB yaitu mengubah pemborosan bit pada *cover image* yang tidak terpengaruh secara siginifikan dengan bit dari pesan rahasia. Misalkan pada sebuah media gambar berbasis *pixel* dengan nilai 8 bit. Setiap *pixel* yang terdiri dari 8 bit dibagi menjadi 2 bagian yaitu 4 bit MSB (*Most Significant Bit*) dan 4 bit LSB (*Least Significant Bit*). Bagian LSB kemudian diubah menjadi nilai dari pesan yang akan disisipkan. Setelah itu, setiap *pixel* dibangun ulang menjadi gambar utuh yang menyerupai media gambar semula.

## 2. METODE PENELITIAN

Sistem diimplementasikan menggunakan GUI pada Matlab R2010b. Dalam sistem ini akan dilakukan proses enkripsi dan deksripsi citra menggunakan algoritma RC6 dan proses *steganografi* dengan menggunakan metode LSB. Gambaran umum dari sistem ini dapat dilihat pada Gambar 6 dan 7.




Gambar 6 Gambaran umum sistem kerja enkripsi – penyisipan




Gambar 7 Gambaran umum sistem kerja ekstraksi – dekripsi

Dari gambaran umum sistem kerja di atas dapat dijelaskan sebagai berikut :

1. Citra data akan dienkripsi terlebih dahulu menggunakan algoritma RC6 dengan memanfaatkan *key* menjadi sebuah citra terenkripsi.
2. Citra terenkripsi kemudian disisipkan menggunakan metode LSB kedalam sebuah citra wadah menjadi sebuah *stego image*.
3. *Stego image* kemudian diuji secara kualitatif dan kuantitatif, kemudian hasilnya dianalisa.
4. Selanjutnya *stego image* akan diekstraksi untuk untuk mendapatkan kembali citra terenkripsi.

Citra terenkripsi hasil ekstraksi kemudian didekripsi untuk mendapatkan citra dekripsi yang sama dengan citra data. Selanjutnya diuji secara kualitatif dan kuantitatif, kemudian hasilnya dianalisa.

Algoritma Enkripsi RC6 :

1. Dilakukan proses *whitening* awal, nilai $B$ akan dijumlahkan dengan $S[0]$ dan nilai $D$ dijumlahkan dengan $S[i]$.
2. Dilakukan iterasi dari $i = 0$ meningkat iterasi $i = i+1$ sampai iterasi $i = r$.
3. Kemudian setiap iterasi mengikuti aturan sebagai berikut, nilai $B$ dimasukan ke dalam fungsi $f$, yang didefinisikan sebagai $f(x) = x(2x+1)$, kemudian diputar kekiri sejauh $lg$-$w$ atau 5 *bit*. Hasil yang didapat pada proses ini dimisalkan sebagai $q$. Nilai $q$ kemudian di XOR dengan $C$ dan hasilnya menjadi nilai $C$. Nilai $p$ juga digunakan sebagai acuan bagi $C$ untuk memutar nilainya kekiri. Begitu pula dengan nilai $q$, juga digunakan sebagai acuan bagi nilai $A$ untuk melakukan proses pemutaran kekiri.
4. Dilakukan proses *whitening* akhir dimana nilai $A$ dijumlahkan dengan $S[42]$ dan nilai $C$ dijumlahkan dengan $S[43]$.

5. Kemudian sub kunci *S*[2*i*] pada iterasi dijumlahkan dengan *A*, dan sub kunci *S*[2*i*+1] dijumlahkan dengan *C*. Keempat bagian dari blok kemudian akan saling bertukar tempat dengan mengikuti aturan, bahwa nilai *A* ditempatkan pada *D*, nilai *B* ditempatkan pada *A*, nilai *C* ditempatkan pada *B*, dan nilai (asli) *D* ditempatkan pada *C*. Demikian iterasi tersebut akan terus berlangsung hingga *r* kali.

Sedangkan untuk algoritma dekripsi RC6 merupakan pembalikan dari proses enkripsi.

Implentasi algoritma RC6 dilakukan dengan menggunakan bahasa pemograman *java* yang kemudian dibuat *class* agar matlab dapat membaca *file java* yang sudah dibuat.

Algoritma penyisipan LSB :

1. Inisialisasi citra *cover* sebagai A dan citra data sebagai B.
2. Ambil informasi mengenai *row, column,* dan *channel* dari citra A dan B.
3. Pengecekan apakah *row* A berukuran delapan kali lebih besar dari citra A dengan tambahan 3 *row* untuk menyimpan informasi nilai *row, column,* dan *channel* citra B. Jika *Yes* lanjut ke langkah selanjutnya, jika *No* maka proses berakhir.
4. Untuk nilai x = 1 sampai x <= 16. Simpan pada citra A *row* pertama, *column* x, dan *channel* pertama nilai *row* citra B, simpan pada citra A *row* kedua, *column* x, dan *channel* pertama nilai *column* citra B dan simpan pada citra A *row* ketiga, *column* x, dan *channel* pertama nilai *channel* citra B.
5. Lakukan penyisipan setiap 1 *bit* citra B ke dalam setiap *byte* citra A.

Algoritma ekstraksi LSB :

1. Inisialisasi citra *stego* sebagai A dan citra data sebagai B.
2. Mengambil informasi nilai *row* B dari *row* pertama *column* pertama sampai keenam belas *channel* pertama A, nilai *column* B dari *row* kedua *column* pertama sampai keenam belas *channel* pertama A dan nilai *channel* B dari *row* ketiga *column* pertama sampai keenam belas *channel* pertama A.
3. Membuat matriks B dengan informasi yang didapatkan dari langkah sebelumnya dan membuat tambahan matriks untuk nilai *alpha.*
4. Logika pengulangan untuk *col* = 1 sampai nilai *column* B dan *row* = 1 sampai nilai *row* B.
5. Inisialisasi nilai *i* = ((*col*-1)*1)+1 dan nilai *j* = ((*col*-1)*1)+8. Mengambil nilai dari A kemudian diubah dan ditempatkan di matriks B.

## 3. HASIL DAN PEMBAHASAN

### 4.1 Metode Pengujian Sistem

Dalam penelitian ini digunakan 2 macam metode pengujia sebagai berikut

**1. *Blackbox***

*Black Box* Testing adalah metode pengujian yang berfokus pada persyaratan fungsional perangkat lunak. Pengujian ini berusaha menemukan kesalahan dalam kategori sebagai berikut :

- Fungsi – fungsi yang tidak benar atau hilang,
- Kesalahan *interface*,
- Kesalahan dalam struktur data atau akses *database* eksternal,
- Kesalahan kinerja.

**2. Secara Kualitatif**

Pengujian secara kualitatif dilakukan dengan cara membandingkan citra asli dan citra yang sudah didekripsi secara visual. Penilaian citra secara kualitatif dapat dilihat pada Tabel 6.

Tabel 6 Tabel penilaian secara kualitatif

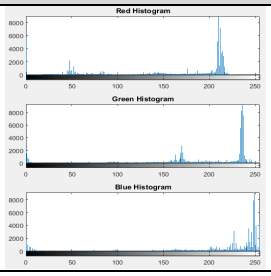
| No | Tingkatan | Keterangan |
|---|---|---|
| 1 | *Excellent* | Kualitas terbaik, seperti aslinya |
| 2 | *Fine* | Kualitas tinggi, dapat diamati |
| 3 | *Passable* | Kualitas cukup baik, masih dapat diterima |
| 4 | *Marginal* | Kualitas buruk, masih bisa diperbaiki |
| 5 | *Inferior* | Kualitas sangat buruk, namun masih bisa diamati |
| 6 | *Unusable* | Sudah tidak dapat diamati lagi |

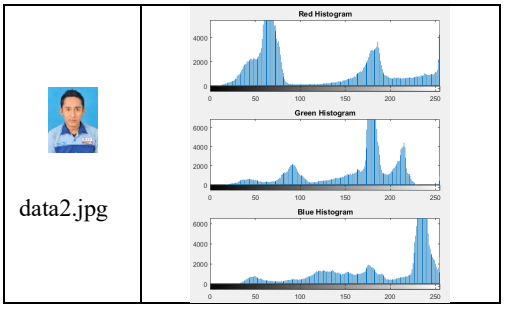
(Sumber : [11])

### 4.2 Pengujian Waktu Enktipsi dan Dekripsi

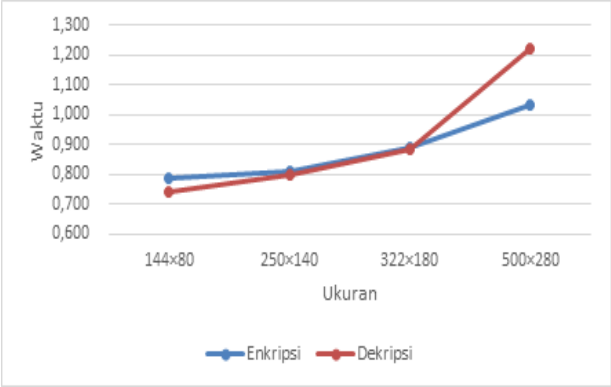
Citra yang digunakan untuk algoritma enkripsi dan dekripsi RC6 yakni 2 buah citra berekstensi *.JPG dan bertipe RGB dengan ukuran untuk lebar dan tinggi citra adalah genap. Algoritma RC6 dilengkapi dengan beberapa parameter *w/r/b* dengan *w* = 32, *r*=20 dan *b* sebesar 16 *byte*. Penggunaan 2 buah citra dikarenakan masing – masing dari citra ini memiliki ciri kerapatan piksel yang berbeda, *file* data1.jpg merupakan data citra teks sedangkan data2.jpg merupakan data citra gambar.

Tabel 7 Informasi Histogram dari 2 data citra

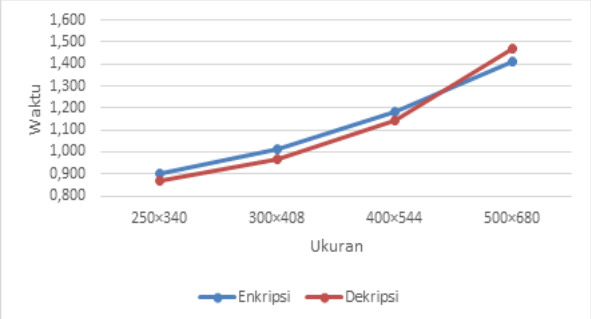
| Data | Informasi Histogram |
|---|---|
|  data1.jpg |   |




Dari dua buah citra percobaan enkripsi dan dekripsi dibuat masing–masing 4 buah variasi ukuran citra untuk melihat pengaruh ukuran citra terhadap waktu komputasi. Dapat dilihat pada Gambar 8 dan 9 perubahan ukuran citra dalam hal ini besar nilai piksel dari citra yang diproses oleh algoritma RC6 berpengaruh pada waktu komputasi yang diperlukan. Semakin besar ukuran citra maka semakin banyak pula waktu komputasi yang diperlukan.



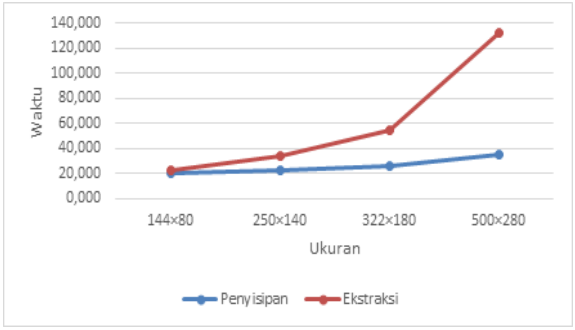

Gambar 8 Grafik perubahan waktu enkripsi dan dekripsi file data1.jpg terhadap perubahan ukuran



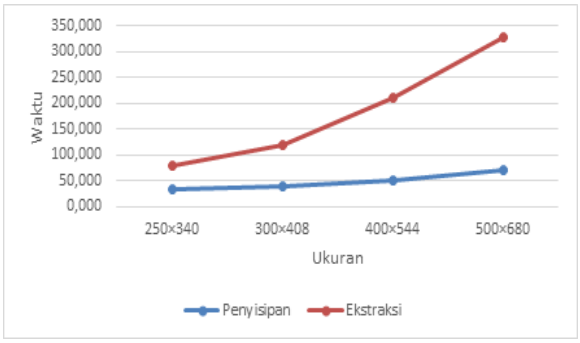

Gambar 9 Grafik perubahan waktu enkripsi dan dekripsi file data2.jpg terhadap perubahan ukuran

Citra yang digunakan pada proses *steganografi* dengan metode LSB terdiri atas 2 buah citra. Citra pertama yaitu citra data yang merupakan citra hasil enkripsi dengan algoritma RC6 dan citra kedua adalah citra wadah.

Pada metode ini citra data akan disisipkan ke dalam citra wadah. Dengan menggunakan LSB setiap 1 *bit* citra data akan disisipkan ke dalam 1 *byte* citra wadah sehingga citra wadah harus berukuran delapan kali lebih besar dari citra data. Selain itu terdapat 3 buah baris data dari citra wadah yang juga akan dipakai untuk menyimpan informasi berupa panjang lebar dan jumlah kanal dari citra data.




Gambar 10 Grafik perubahan waktu penyisipan dan ekstraksi *file* encrypted_data1.jpg terhadap perubahan ukuran

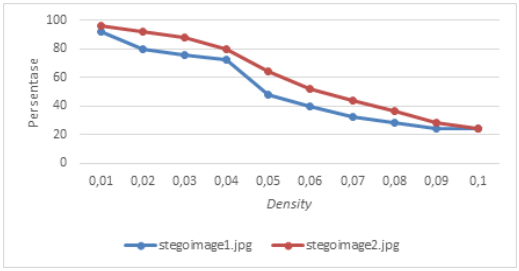



Gambar 11 Grafik perubahan waktu penyisipan dan ekstraksi *file* encrypted_data2.jpg terhadap perubahan ukuran

Dari Gambar 10 dan 11 perubahan ukuran citra dalam hal ini besar nilai piksel dari citra yang dalam proses penyisipan dan ekstraksi dengan metode LSB berpengaruh pada waktu komputasi yang diperlukan. Semakin besar ukuran citra maka semakin banyak pula waktu komputasi yang diperlukan. Perbedaan waktu penyisipan dan ekstraksi disebabkan karena pada waktu ekstraksi proses yang terjadi didalam pengambilan file lebih rinci yaitu mulai dari pelacakan *bit* yang disisipkan kemudian mengambil *bit-bit* file yang disisipkan lalu menyatukan kembali *bit-bit* file menjadi sebuah data file yang sempurna.

Pada pengujian berikutnya digunakan jenis *noise salt and pepper*. Proses pengujiannya yaitu citra hasil penyisipan akan diberikan *noise salt and pepper* kemudian akan diekstrak dan didekripsi dengan algoritma RC6 untuk melihat dampak dari *noise* yang diberikan. Terdapat variasi nilai *noise* (*density*) yang

diberikan dalam pengujian ini dengan variasi 0,01 – 0,1.




Gambar 12 Grafik persentase keberhasilan ekstraksi dan dekripsi *file* stegoimage1.jpg dan stegoimage2.jpg

Pada pengujian ketahanan *noise* selain dibuat variasi nilai *density*, pada setiap nilai *density* dilakukan percobaan sebanyak 25 kali untuk mendapatkan persentase keberhasilan pengembalian data baik proses enkripsi maupun dekripsi. Dari gambar 12 dapat dilihat bahwa persentase keberhasilan menurun seiring ditingkatkannya nilai *density noise* yang diberikan. Hal ini dapat terjadi karena semakin besar nilai *density* maka semakin besar kemungkinan kerusakan data baik untuk *file* stegoimage1.jpg maupun stegoimage2.jpg. Kegagalan dalam proses ekstraksi dapat terjadi karena piksel penting dari stegoimage1.jpg dan stegoimage2.jpg yaitu piksel pada baris 1, 2 dan 3 yang berisi informasi kolom, baris dan kanal dari citra data berubah akibat terkena *noise* yang diberikan. Data pada gambar 12 juga menunjukan bahwa stegoimage2.jpg memiliki persentase keberhasilan yang lebih baik dari pada stegoimage1.jpg, hal ini dapat terjadi karena informasi yang ada pada stegoimage2.jpg berbeda dengan informasi pada stegoimage1.jpg dimana informasi di stegoimage2.jpg lebih tahan terhadap serangan.

### 4.3. Pengujian Error

Perhitungan MSE dan PSNR yang dilakukan, yaitu pada citra data awal terhadap citra akhir hasil proses kriptografi dan *steganografi*, citra hasil penyisipan terhadap citra *cover* dan citra awal terhadap citra hasil ekstraksi dan dekripsi yang telah diberikan *noise*.

Tabel 8 Hasil perhitungan MSE dan PSNR citra data awal terhadap citra akhir hasil proses kriptografi dan *steganografi*

| *File* | | Waktu (detik) | |
|---|---|---|---|
| Citra Data | Citra Hasil | MSE | PSNR |
| data1.jpg (500×280 piksel) | encrypted_ data1.jpg | 35,474 | 132,258 |
| | | 25,851 | 54,474 |
| | | 22,774 | 34,275 |
| | | 20,618 | 22,854 |
| data2.jpg (500×680 piksel) | encrypted_ data2.jpg | 69,319 | 327,061 |
| | | 50,718 | 210,451 |
| | | 38,719 | 119,239 |
| | | 33,635 | 79,841 |

Tabel 9 Hasil perhitungan MSE dan PSNR citra wadah awal terhadap citra hasil proses penyisipan

| *File* | | Waktu (detik) | |
|---|---|---|---|
| Citra Data | Citra Hasil | MSE | PSNR |
| data1.jpg (500×280 piksel) | decrypted_extractedLsb1.png (500×280 piksel) | 0 | *Inf* |
| data1.jpg (500×680 piksel) | decrypted_extractedLsb2.png (500×680 piksel) | 0 | *Inf* |

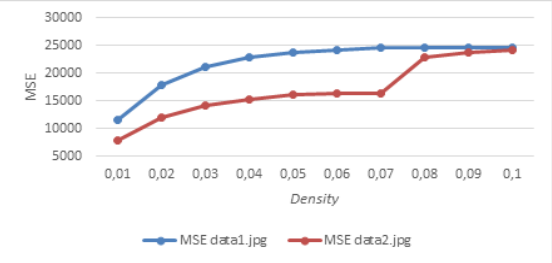
Tabel 10 Hasil perhitungan MSE dan PSNR citra wadah awal terhadap citra hasil proses penyisipan

| *File* | | Waktu (detik) | |
|---|---|---|---|
| Citra Wadah | Citra Hasil Penyisipan | MSE | PSNR |
| wadah.png (4448×6264 piksel) | stegoimage1.png (4448×6264 piksel) | 0,0201 | 149,896 |
| | Stegoimage2.png (4448×6264 piksel) | 0,0488 | 141,021 |

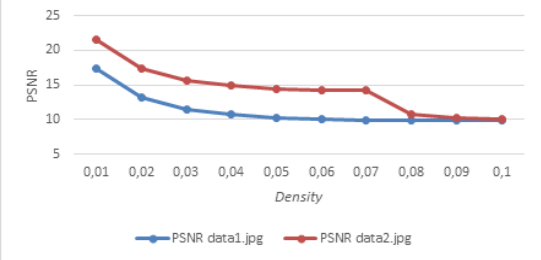
Tabel 11 Hasil perhitungan MSE dan PSNR citra data awal terhadap citra akhir hasil proses kriptografi dan *steganografi* yang telah diberi *noise*

| Nama *File* | Nilai *Density* | Waktu (detik) | |
|---|---|---|---|
| | | Ekstraksi | Dekripsi |
| data1.jpg | 0,01 | 11.626,9 | 17,39 |
| | 0,02 | 17.807,5 | 13,13 |
| | 0,03 | 21.075,6 | 11,45 |
| | 0,04 | 22.745,8 | 10,68 |
| | 0,05 | 23.693,2 | 10,26 |
| | 0,06 | 24.116,7 | 10,09 |
| | 0,07 | 24.602.6 | 9,90 |
| | 0,08 | 24.615,2 | 9,89 |
| | 0,09 | 24.610,6 | 9,89 |
| | 0,1 | 24.614,1 | 9,89 |
| data2.jpg | 0,01 | 7.904,28 | 21,50 |
| | 0,02 | 11,957,1 | 17,37 |
| | 0,03 | 14.243,4 | 15,61 |
| | 0,04 | 15.311,4 | 14,89 |
| | 0,05 | 15.999,4 | 14,46 |
| | 0,06 | 16.236,5 | 14,31 |
| | 0,07 | 16.425,7 | 14,19 |

| | | | |
|---|---|---|---|
| | 0,08 | 22.745,8 | 10,68 |
| | 0,09 | 23.693,2 | 10,26 |
| | 0,1 | 24.116,7 | 10,09 |




Gambar 13 Grafik hasil perhitungan MSE citra data awal terhadap citra akhir hasil proses kriptografi dan *steganografi* yang telah diberi *noise*




Gambar 14 Grafik hasil perhitungan MSE citra data awal terhadap citra akhir hasil proses kriptografi dan *steganografi* yang telah diberi *noise*

Berdasarkan grafik pada gambar 19 dan gambar 20 niSemakin besar *density* maka semakin buruk nilai MSE dan PSNR yang didapatkan dalam hal ini MSE semakin besar dan PSNR semakin kecil. Nilai MSE dan PSNR untuk data2.jpg mengalami penurunan yang drastis pada nilai *density* dari 0,07 menuju 0,08 dan cenderung stabil dari 0,08 hingga 0,1 yang menunjukan pengaruh maksimal *noise salt and pepper* pada data2.jpg mulai bekerja pada rentan *noise* 0,08 hingga 0,1 sedangkan data1.jpg cenderung stabil pada titik terendah dari nilai *density* 0,05 hingga 0,1. Hal ini menunjukan bahwa data2.jpg memiliki tingkat ketahanan yang lebih baik dari pada data1.jpg.

### 4.4. Pengujian Secara Kualitatif

Secara kualitatif pengujian dilakukan dengan mengumpulkan pendapat dari 5 orang responden untuk setiap citra uji. Pengujian citra keluaran sistem dengan citra data untuk data1.jpg dan data2.jpg mendapat penilaian *excellent* atau kualitas citra keluaran masih sama seperti kualitas citra asli. Kemudian dilakukan juga pengujian terhadap citra wadah sebelum dan sesudah proses penyisipan dan mendapatkan penilaian *excellent* dari responden.

Selain pengujian diatas, dilakukan pula pengujian kualitatif terhapat citra yang sudah diberikan *noise* berupa *noise salt and pepper* dengan intensitas (*density*) 0,01 – 0,1. Dari setiap *density noise* yang diberikan, responden memberikan penilaian *marginal* untuk file data1.jpg dengan *density* 0,01 dan 0,02, *inferior* untuk 0,03, dan *unusable* untuk 0,04 – 0,1. Untuk file data2.jpg responden memberikan penilaian marginal untuk density 0,01 dan 0,02, inferior untuk 0,03 dan 0,04, dan unusable untuk 0,05 – 0,1.

## 4. KESIMPULAN

Kombinasi algoritma RC6 dan metode LSB dapat digunakan untuk meningkatkan keamanan data citra digital dengan tidak adanya perbedaan antara citra asli dan citra keluaran (MSE 0) dan penilaian kualitatif *excellent.* Demikian juga untuk citra wadah sebelum dan sesudah penyisipan yang mendapat MSE terbesar 0,0488 dan PSNR terkecil 141,021 dB dengan penilaian kualitatif *excellent*.

Kombinasi algoritma RC6 dan metode LSB dapat bertahan terhadap *noise salt and pepper* dengan rentang *density* 0,01 - 0,1 dengan MSE 7.904,28 - 24.614,1 dan PSNR 9,89 dB - 21,50 dB. Persentase keberhasilan proses ekstraksi dan dekripsi berada pada rentang 24% - 96%. Kegagalan terjadi karena *noise* mengenai bagian vital yaitu baris 1, 2 dan 3 citra stegoimage1.jpg maupun stegoimage2.jpg yang berisi informasi mengenai ukuran dan jumlah kanal dari citra data. Perbedaan nilai PSNR, MSE dan persentase yang didapatkan besar dipengaruhi oleh karakteristik dari citra data.

Waktu komputasi yang dibutuhkan algoritma RC6 dan metode LSB sangat dipengaruhi oleh ukuran citra, Citra dengan ukuran terbesar yakni 500×680 membutuhkan waktu 1.412 detik untuk dienkripsi dan 1,472 detik untuk didekripsi serta 69,319 detik untuk disisipkan dan 327,061 detik untuk diekstraksi, sedangkan citra dengan ukuran terkecil yakni 144×80 membutuhkan waktu 0,787 detik untuk dienkripsi dan 0,739 detik untuk didekripsi serta 20,618 detik untuk disisipkan dan 12,854 detik untuk diekstraksi. Semakin besar ukuran citra maka semakin lama waktu komputasinya.

## DAFTAR PUSTAKA

[1] Aji, I. 2015. ***Implementasi Metode Huffman untuk Kompresi Citra Hasil dari Steganografi Discrete Cosine Transform (DCT)***. Universitas Dian Nuswantoro. Semarang.

[2] Ariyus, D. 2008. ***Pengantar Ilmu Kriptografi***. Penerbit Andi. Yogyakarta.

[3] A, Ganesha Dwi dkk. 2015. ***Implementasi Kriptografi dan Steganografi Pada Media Gambar Menggunakan Algoritma Blowfish dan Metode Least Significant Bit***. e-Proceeding of Engineering : Vol.2 ISSN : 2355-9365. Bandung

[4] Maulana, Ahmad Mansur dkk. 2013. ***Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit***. Institut Teknologi Sepuluh Nopember. Surabaya

[5] Mardiana. 2013. ***Pengembangan Algoritma Block Chiper RC6 pada Citra Digital***. Universitas Sumatera Utara. Medan.

[6] Muharini, A. 2012. ***Aplikasi Algoritma Rivest Code 6 Dalam Pengamanan Citra Digital***. Universitas Indonesia. Jakarta

[7] Munir, R. 2004. ***Pengolahan Citra Digital dengan Pendekatan Algoritma***. Bandung: Informatika

[8] Munir, R. 2015. ***Bahan Kuliah IF4020 Kriptografi***. Program Studi Informatika STEI-ITB. Bandung

[9] Shahana, T. 2013. ***A Secure DCT Image Steganography based on Public-Key Cryptography***, International Journal of Computer Trends and Technology (IJCTT), vol. 4, no. 3, pp. 2039-2043, 2013.

[10] Tena, S. 2010. ***Bahan Ajar Modul Pengolahan Citra***. Universitas Nusa Cendana. Kupang.

[11] Yonata, Y. 2001. ***Kompresi Video, pemampatan data video untuk aplikasi videophone dan multimedia over IP***. PT Elex Media Komputindo. Jakarta.

[12] Yusuf, K. 2004. ***Kriptografi Keamanan Internet dan Jaringan Komunikasi***. Informatika. Bandung.

[13] Zakariah, M. 2013. ***Dasar-Dasar Operasi Matlab***. Universitas Negeri Yogyakarta. Yogyakarta