ANALISIS PERBANDINGAN ALGORITMA *RIVEST SHAMIR ADLEMAN (RSA)* & *RIVEST CODE* 6 *(RC6)* DALAM KEAMANAN CITRA DIGITAL

Syahrul[1], Silvester Tena[2], Sarlince O. Manu[3]

1 Jurusan Teknik Elektro Fakultas Sains dan Teknik Undana, Jl. Adisucipto Penfui, Kupang.
email : arul.win1@gmail.com
2 Jurusan Teknik Elektro Fakultas Sains dan Teknik Undana, Jl. Adisucipto Penfui, Kupang
email: siltena@staf.undana.ac.id
3 Jurusan Teknik Elektro Fakultas Sains dan Teknik Undana, Jl. Adisucipto Penfui, Kupang
email: sarlince_manu@staf.undana.ac.id

ABSTRAK

Citra digital merupakan satu media yang dapat disimpan pada media penyimpanan atau ditransmisikan melalui jaringan. Namun dalam transmisi dapat terjadi tindakan pencurian dan penyalahgunaan data yang merugikan pihak berkepentingan terhadap data tersebut. Untuk melindungi dan menjaga kerahasiaan sebuah citra digital digunakan metode *kriptografi.*

Pada penelitian ini dibandingkan dua algoritma yaitu *Rivest Shamir Adleman* (RSA) dan *Rivest Code* 6 (RC6). RSA merupakan salah satu algoritma asimetris dimana kunci enkripsi dan dekripsi yang digunakan berbeda, sedangkan RC6 merupakan algoritma simetris dimana kunci yang digunakan sama.

Berdasarkan pengujian,waktu operasi algoritma RC6 lebih cepat dari algoritma RSA. Untuk pengujian *noise* yang dilakukan RSA lebih dapat bertahan daripada RC6. Hasil pengujian RSA dapat bertahan pada *noise gaussian* dengan nilai mean 0,00001 dan varian 0,000001 mendapatkan nilai MSE 1252,98 dan PSNR 43,85 dB, sedangkan RC6 tidak dapat bertahan dengan *noise* ini. Kemudian untuk *noise salt & pepper*, RSA dapat bertahan pada nilai *density* 0,05 dengan nilai MSE 1256,66 dan PSNR 42,71 dB, sedangkan RC6 dapat bertahan pada nilai *density* 0,01 dengan nilai MSE 1108,85 dan PSNR 40,72 dB. Berdasarkan pengujian kompresi kedua algoritma ini sama-sama tidak tahan terhadap *lossy compression*, sedangkan untuk *lossless compression* kedua algoritma masih bisa bertahan yakni hasil dekripsi sama dengan citra asli.

Kata Kunci : *Kriptografi*, RSA, RC6, n*oise*

1. PENDAHULUAN

Komunikasi data merupakan proses pengiriman dan penerimaan data/informasi dari dua atau lebih perangkat yang terhubung dalam sebuah jaringan. Proses pengiriman data dengan memanfaatkan jaringan seperti internet cukup efisien, cepat, dan murah. Namun terdapat juga beberapa kekurangan yang memungkinkan terhambatnya proses pengiriman dan penerimaan data. Salah satunya adalah tindakan pencurian dan penyalahgunaan informasi melalui internet yang masih menjadi ancaman dalam melakukan aktivitas pengiriman dan penerimaan informasi atau data. Tindakan pencurian dan penyalahgunaan data melalui internet tentunya dapat merugikan berbagai pihak yang memiliki kepentingan dengan data tersebut.

Kegiatan pencurian dan penyalahgunaan data melalui internet (dunia maya) disebut *cybercrime*. *Cybercrime* merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Salah satunya adalah penyadapan dan penyalahgunaan data citra digital untuk menjatuhkan seseorang maupun kelompok.

Citra merupakan sebuah media informasi yang lebih akurat dibandingkan dengan pesan teks maupun suara. Orang beranggapan bahwa jika tidak ada gambar sebagai media informasi, maka informasi tersebut akan dianggap bohong, sehingga informasi termuat dalam citra haruslah dijaga kerahasiaannya agar tidak digunakan secara ilegal. Oleh karena itu, keamanan citra digital menjadi bagian yang penting dalam penyimpanan dan transmisi untuk menghindari pencurian dan penyalahgunaan data oleh pihak yang tidak berwenang. Misalnya pencurian dan penyalahgunaan citra-citra dalam bidang militer seperti pencurian citra markas besar militer sebuah negara. Salah satu metode yang digunakan menjaga kerahasiaan sebuah data citra digital adalah *kriptografi.*

Kriptografi merupakan salah satu ilmu yang mempelajari keamanan dalam proses komunikasi data. Sistem *kriptografi* dapat digunakan untuk memenuhi aspek kerahasiaan pesan yang dikirim, yaitu pesan yang dikirim hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut dengan menggunakan kunci rahasia karena pesan tersebut dienkripsi. Walau demikian, enkripsi tidak dapat mencegah intersepsi dan modifikasi data pada saluran komunikasi. Oleh karena itu dibutuhkan algoritma enkripsi yang kuat untuk mengenkripsi data rahasia tersebut.

Penelitian mengenai *kriptografi* citra digital yang pernah dilakukan sebelumnya yaitu penelitian oleh Komba tentang *kriptografi* pada citra digital menggunakan algoritma *Rivest, Shamir, Adleman (*RSA). RSA merupakan salah satu algoritma asimetris dimana kunci enkripsi dan dekripsi yang digunakan berbeda. Kelebihan algoritma ini terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor primanya (Komba, 2014). Selain metode algortima RSA ada metode *kriptografi* lain yang dapat digunakan dalam keamanan citra digital yaitu Algoritma *Rivest Code* 6 (RC6) (El-samie, 2014). RC6 merupakan salah satu algoritma simetris dimana kunci enkripsi dan dekripsi yang digunakan sama. Tingkat keamanan pada algoritma ini terletak pada kekuatan rotasi yang berdasarkan data, penggunaan eksklusif OR yang bergantian, fungsi modulo dan fungsi persamaan yang menggunakan rotasi tetap (Rudianto, 2007).

2. DASAR TEORI

2.1. Citra

Citra adalah suatu representasi, kemiripan, atau imitasi dari suatu objek. Citra terbagi menjadi dua, yaitu citra analog dan citra digital. Citra analog adalah citra yang bersifat kontinu, seperti gambar pada foto sinar-X, foto yang tercetak di kertas foto, lukisan, pemandangan alam, hasil *CTscan*, dan sebagainya. Citra digital adalah citra yang dapat diolah dengan bantuan komputer.

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari *m* baris dan *n* kolom, di mana perpotongan antara baris dan kolom disebut piksel atau *pixel* (*picture element*), yaitu elemen terkecil dari sebuah citra. Setiap piksel diwakili oleh bilangan bulat (integer). Piksel mempunyai dua parameter, yaitu koordinat (menunjukkan lokasi dalam bidang citra) dan intensitas (menunjukkan cahaya atau keadaan terang gelap). Nilai yang terdapat pada koordinat (*x,y*) adalah *f(x,y)*, yaitu besar intensitas atau warna dari piksel di titik itu. Sebuah citra digital dapat ditulis dalam bentuk matriks berukuran *m*×*n*.

2.2. Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan) (Ariyus, 2008). *Kriptografi* adalah seni untuk mengacak informasi atau data yang memiliki arti menjadi sesuatu yang tidak dapat dimengerti atau seakan-akan tidak berarti sehingga pesan yang dikirim dapat disampaikan kepada penerima dengan aman.

Menurut Menezes (Ariyus, 2008), ada empat tujuan mendasar dari ilmu *kriptografi* yang merupakan aspek keamanan informasi, yaitu:

1. *Confidentiality* (kerahasiaan) adalah suatu layanan yang digunakan untuk menjaga isi informasi dari pihak yang tidak berwenang untuk memilikinya.
2. *Data integrity* (integritas data) adalah suatu layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. *Authentication* (otentikasi) adalah suatu layanan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan mengidentifikasi kebenaran sumber pesan *(data origin authentication).*
4. *Non-repudiation* (penyangkalan) adalah suatu layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal telah melakukan pengiriman pesan atau penerima pesan menyangkal telah menerima pesan.

Algoritma *kriptografi* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi (Schneier, 1996). Algoritma *kriptografi* merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi merupakan hal yang sangat penting dalam *kriptografi*, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode.
2. Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan.
3. Kunci merupakan kunci untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Algoritma *kriptografi* dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya (Ariyus, 2008) yakni :

1. Algoritma simetri.
   Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi
2. Algoritma asimetri.
   Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu kunci umum (*public key*) dan kunci rahasia (*private key*).
3. *Hash function*.
   Fungsi *hash* sering disebut dengan fungsi *hash* satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompresi dan *Message Authentication Code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.

2.2.1. Algoritma *Rivest Shamir Adleman* (RSA)

Algoritma RSA merupakan penerapan dari *kriptografi* asimetri, yakni jenis *kriptografi* yang menggunakan dua kunci yang berbeda yaitu kunci publik (*public key*) dan kunci pribadi (*private key*). RSA mendasarkan proses enkripsi dan deskripsinya pada konsep bilangan prima dan aritmatika modulo. Baik kunci enkripsi maupun kunci deskripsi keduanya berupa bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk deskripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci deskripsi, orang harus memfaktorkan suatu bilangan non prima menjadi faktor primanya.

2.2.2. Algoritma *Rivest Code* 6 (RC6)

RC6 merupakan *block cipher* turunan dari RC5. Didesain oleh Ron Rivest, Matt Robshaw, Ray Sidney, dan Yigun Lisa Yin untuk memenuhi persyaratan dari kompetisi *Advanced Encryption Standard* (AES). RC6 mempunyai *block size* 128 *bit* dan mendukung panjang kunci 128, 192, dan 256 *bit*. Seperti halnya RC5 maka RC6 dapat diparameter untuk mendukung panjang kata yang lebih besar dan bervariasi, *key size*, dan jumlah *round* yang dapat ditentukan. RC6 sangat mirip dengan RC5 dalam strukturnya. Menggunakan data *dependent rotation*, penjumlahan *modular* dan operasi XOR. Pada kenyataannya RC6 dapat dilihat sebagai proses enkripsi RC5 dengan dua *parallel interweaving*. RC6 menggunakan operasi perkalian ekstra yang tidak terdapat dalam RC5 dengan maksud membuat *rotation dependent* pada setiap *bit*, jadi tidak hanya beberapa *least significant bit* saja.

Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-*w/r/b*. Parameter *w* merupakan ukuran kata dalam satuan bit, parameter *r* merupakan bilangan bukan negatif yang menunjukkan banyaknya iterasi selama proses enkripsi dan parameter *b* menunjukkan ukuran kunci enkripsi dalam *byte*. Setelah algoritma ini masuk ke dalam AES, maka ditetapkan bahwa nilai $w = 32$, $r = 20$, dan *b* bervariasi antara 16, 24, dan 32 byte (Mardiana, 2013).

2.3. *Noise*

Noise atau derau didefinisikan sebagai gangguan pada sinyal citra yang disebabkan oleh gangguan fisis (optik) pada alat akuisisi maupun secara disengaja akibat proses pengolahan yang tidak sesuai. Jika suatu citra dikirim secara elektronik dari suatu tempat ke tempat yang lain melalui sebuah jaringan, maka kemungkinan besar *error* akan terjadi. *Error* ini muncul atau tampak pada citra keluaran tergantung dari tipe gangguan pada sinyal

2.3.1. *Noise Gaussian*

Noise gaussian merupakan model *noise* yang mengikuti distribusi *normal standard* dengan rata-rata nol dan *standard deviasi* 1. Efek dari *gaussian noise* ini, pada gambar muncul titik-titik berwarna yang jumlahnya sama dengan prosentase *noise* (Sigit, 2013).

2.3.2. *Noise Salt & Papper*

Noise Salt & Papper memberikan *noise* seperti halnya taburan garam, akan memberikan warna putih pada titik yang terkena noise. Pada citra akan nampak seperti titik-titik. Untuk citra RGB titik-titik muncul dalam tiga warna yakni merah (*red*), hijau (*green*), dan biru (*blue*), sedangkan pada citra *grayscale, noise* akan muncul dalam dua warna yakni hitam (*black*) dan putih (*white*).

2.4. Kompresi

Kompresi citra atau pemampatan citra bertujuan meminimalkan kebutuhan memori untuk merepresentasikan citra digital dengan mengurangi duplikasi data dalam citra sehingga memori yang dibutuhkan menjadi lebih sedikit, jadi citra dapat disimpan atau ditransmisikan secara efisien. Ada dua jenik teknik pemampatan citra yaitu *loseless compression* yang merupakan teknik kompresi citra dimana tidak ada satupun informasi citra yang dihilangkan dan *lossy compression* yang merupakan tipe kompresi dimana terdapat data yang hilang selama proses kompresi, akibatnya kualitas data yang dihasilkan lebih rendah daripada kualitas data asli.

Beberapa format kompresi citra antara lain yaitu format *JPG.* JPG adalah jenis data yang dikembangkan oleh *Joint Photographic Experts Group* (JPEG) yang dijadikan standar untuk para fotografer *profesional*. File JPG menggunakan teknik kompresi yang menyebabkan turunnya kualitas gambar (*lossy compression*). Setiap kali menyimpan ke tipe JPG dari tipe lain, ukuran gambar biasanya mengecil, dan penurunan kualitasnya tidak dapat dikembalikan. Meskipun dengan penurunan kualitas gambar, pada gambar-gambar tertentu (misalnya pemandangan), penurunan kualitas gambar hampir tidak terlihat mata.

Selain format JPG ada format lain yaitu format PNG. PNG adalah kepanjangan dari *Portable Network Graphics* dan format ini mendukung transparansi. Tipe file PNG merupakan solusi kompresi yang powerful dengan warna yang lebih banyak (24-bit RGB + *alpha*). Berbeda dengan JPG yang menggunakan teknik kompresi yang menghilangkan data, file PNG menggunakan kompresi yang tidak menghilangkan data (loseless compression).

2.5. Kriteria Keandalan Kriptosistem

Kriteria kehandalan kriptosistem terletak pada kerahasiaan kunci (bukan pada kerahasiaan algoritma yang digunakan), menghasilkan *ciphertext* yang terlihat acak dalam seluruh tes statistik yang

dilakukan terhadapnya dan mampu menahan serangan yang diberikan.

2.5.1. Kriteria Objektif (Kuantitatif)

Ada beberapa parameter kuantitatif dalam pengukuran kesalahan atau error dalam pemrosesan citra. Dua parameter yang paling umum digunakan adalah *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR). Walaupun tidak selalu berkorelasi dengan persepsi visual manusia, MSE merupakan ukuran yang baik untuk mengukur kesamaan dua buah citra. MSE antara keduanya didefinisikan persamaan berikut :

$$M = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left[B_1(i,j) - B_2(i,j) \right]^2 \quad (1)$$

Dimana B_1 dan B_2 adalah dua buah citra yang dibandingkan, sedangkan $m \times n$ adalah ukuran dimensi baris × kolom dari citra yang dibandingkan.. Semakin besar nilai MSE, maka semakin besar perbedaan antara dua buah citra yang dibandingkan. Nilai MSE yang baik yaitu jika nilai MSE dari citra tersebut mendekati nol (MSE ≈ 0).

Satu lagi parameter pengukuran kesalahan yang sama baiknya adalah PSNR. Untuk dua buah citra *grayscale* 8-*bit* dengan dimensi yang sama dan dengan menggunakan nilai MSE dari kedua citra tersebut maka PSNR antara keduanya didefinisikan :

$$P = 10 \log_1 \left(\frac{255^2}{M} \right) \quad (2)$$

Nilai 255^2 merepresentasikan nilai MSE terbesar yang mungkin antara dua citra digital 8-bit. Nilai PSNR yang lebih besar mengindikasikan aproksimasi yang lebih dekat dari B_1 dan B_2. Satuan yang digunakan PSNR adalah *desibel* (dB). Untuk kualitas citra berdasarkan jangkauan PSNR dapat dilihat pada Tabel 1.

Tabel 1
Kualitas citra berdasarkan jangkauan PSNR

PSNR (dB)	Kualitas Citra
60	Sangat baik (tanpa derau)
50	Baik (terdapat sejumlah derau tapi kualitas citra masih bagus
40	Cukup baik (terdapat butiran halus atau seperti salju di dalam citra)
30	Kurang baik (terdapat banyak derau)
20	Tidak baik (tidak dapat digunakan)

(Sumber : Shahana, 2013)

2.5.2. Kriteria Subjektif (Kualitatif)

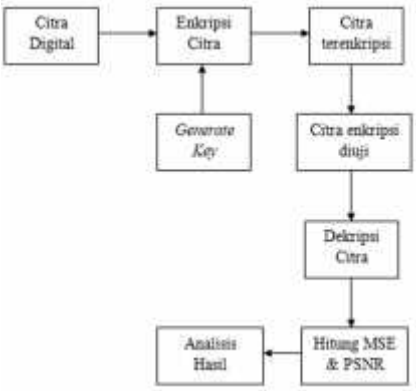
Kriteria kualitatif diberikan kepada hasil dekripsi citra cipher dibandingkan dengan citra asli. Penilaian dengan cara pengamatan visual ini lebih bersifat subjektif karena penerimaan dan penilaian setiap orang berbeda. Penilaian subjektif ini dapat dibagi menjadi (Pakhira, 2014) :

- *Excellent* (kualitas terbaik, seperti aslinya)
- *Fine* (kualitas tinggi, dapat dinikmati)
- *Passable* (kualitas cukup baik, masih dapat diterima)
- *Marginal* (kualitas buruk, masih bisa diperbaiki)
- *Inferior* (kualitas sangat buruk, namun masih bisa diamati)
- *Unusable* (sudah tidak dapat diamati lagi).

3. PERANCANGAN SISTEM

3.1. Diagram Alir Sistem

Berikut adalah perancangan dan desain sistem keamanan citra menggunakan algoritma RSA & RC6. Sistem keamanan yang dibuat diharapkan dapat menganalisis algoritma manakah yang lebih baik dalam keamanan citra digital. Sistem ini diimplementasikan menggunakan *Graphical User Interface* (GUI) pada *Matlab 2016* dan *Java*. Dalam sistem ini dilakukan proses enkripsi dan deksripsi citra menggunakan algoritma RSA & RC6. Gambaran umum dari sistem ini dapat dilihat pada Gambar 1.



Gambar 1 Gambaran umum sistem keamanan citra

Dari gambaran umum proses di atas proses enkripsi dan deskripsi dapat dijelaskan sebagai berikut :

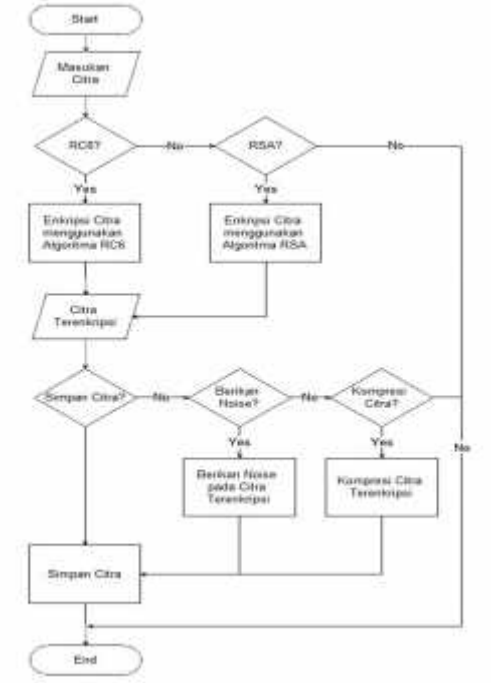
1. Citra digital dienkripsi terlebih dahulu menggunakan algoritma RSA & RC6 menjadi sebuah citra terenkripsi.
2. Saat menjadi citra terenkripsi, citra diuji untuk membandingkan algoritma mana yang lebih baik dalam keamanan citra digital. Untuk lebih lengkapnya tentang pengujian ini dibahas pada pengujian sistem.
3. Citra terenkripsi yang telah diuji didekripsi kembali menjadi citra asli sehingga dapat dihitung MSE & PSNR dari citra tersebut.
4. Hasil yang didapatkan menunjukkan algoritma yang lebih baik.

3.2. *Flowchart* Proses Enkripsi

Untuk *flowchart* proses enkripsi yang diteliti dapat dilihat pada Gambar 2. Algoritma proses enkripsi yang ditunjukan pada Gambar 2 yaitu :

1. Masukan citra yang akan dienkripsi.
2. Kemudian jika citra ingin dienkripsi menggunakan algoritma RC6, maka program akan mengenkripsi citra masukan menggunakan algoritma RC6. Jika citra ingin dienkripsi menggunakan algoritma RSA, maka program

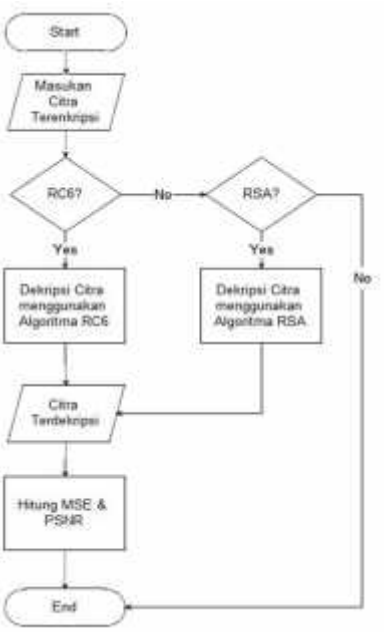
akan mengenkripsi citra masukan menggunakan algoritma RSA.
3. Keluaran dari proses enkripsi adalah citra terenkripsi.
4. Citra terenkripsi dapat diberi noise ataupun dikompresi untuk menguji ketahanan dari algoritma RC6 dan RSA.



Gambar 2 *Flowchart* proses enkripsi

Untuk Algoritma proses dekripsi yang ditunjukan pada Gambar 3 yaitu :

1. Masukan citra yang telah dienkripsi
2. Kemudian jika citra ingin didekripsi menggunakan algoritma RC6, maka program ingin mendekripsi citra masukan menggunakan algoritma RC6. Jika citra ingin didekripsi menggunakan algoritma RSA, maka program akan mendekripsi citra masukan menggunakan algoritma RSA.
3. Keluarkan dari proses dekripsi adalah citra terdekripsi
4. Citra yang sudah didekripsi dihitung MSE dan PSNRnya untuk mendapatkan hasil algoritma mana yang lebih baik diantara RSA atau RC6 dalam keamanan citra digital.



Gambar 3 *Flowchart* proses dekripsi

4. HASIL DAN PEMBAHASAN

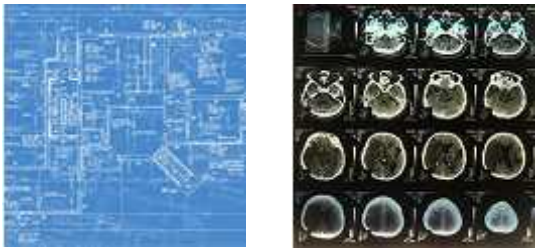
4.1. Pengujian *Black Box*

Pengujian *black box* berguna untuk menguji fungsi-fungsi dari sistem yang telah dirancang. Metode ini digunakan untuk mengetahui apakah sistem telah berfungsi dengan baik atau belum. Kebenaran pengujian dilihat dari keluaran yang dihasilkan dan data/kondisi masukan yang diberikan tanpa melihat bagaimana proses untuk mendapatkan keluaran tersebut. Dari keluaran yang dihasilkan sistem dapat dilihat kemampuan program dalam memenuhi kebutuhan *user* serta dapat diketahui kesalahannya.

Dari pengujian *black box* dilakukan pada 14 tampilan sistem yang ada dan seluruh tindakan yang dilakukan pada pengujian ini mendapatkan hasil yang diharapkan. Hasil pengujian pada setiap *push button*, *text field*, dan *axes* yang dilakukan pada setiap tampilan seluruhnya berhasil, sehingga dapat disimpulkan bahwa seluruh fungsi dari sistem yang dirancang untuk menganalisis perbandingan algoritma RSA dan RC6 dalam keamanan citra digital dapat berjalan dengan baik.

4.2. Pengujian Enkripsi dan Dekripsi

Pengujian ini dilakukan dengan menggunakan dua citra uji yang dapat dilihat pada Gambar 4.



Gambar 4 Citra uji

Dari hasil dekripsi Algoritma RSA dan RC6 nilai MSE dan PSNR dari perbandingan citra asli *blue* dan *ctscan* dengan citra dekripsinya. Nilai MSE yang didapatkan bernilai 0 dan nilai PSNR menunjukkan nilai tak terhingga. Sehingga dapat disimpulkan bahwa kriptosistem ini dapat mengembalikan citra dekripsi yang ada menjadi citra aslinya.

Rata-rata waktu yang dibutuhkan dalam proses enkripsi dan dekripsi diperoleh dengan melakukan lima kali percobaan. Untuk rata-rata waktu proses enkripsi dan dekripsi algoritma RSA dan RC6 dapat di lihat pada Tabel 2 dan Tabel 3.

Tabel 2
Rata-rata waktu enkripsi dan dekripsi RSA

No	Citra Uji	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	blue.bmp 150×150 *pixel*	0,60	0,56
2	ctscan.bmp 200×200 *pixel*	0,77	0,70

Tabel 3
Rata-rata waktu enkripsi dan dekripsi RC6

No	Citra Uji	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	blue.bmp 150×150 *pixel*	0,55	0,58
2	ctscan.bmp 200×200 *pixel*	0,58	0,58

4.3. Pengujian Noise

Pengujian *noise* dilakukan dengan menambahkan dua jenis *noise* yaitu *noise gaussian* dan *noise salt & pepper* pada citra terenkripsi sebelum didekripsi kembali. Penambahan *noise* dilakukan dengan nilai *mean*, *varian* dan *density* yang bervariasi. Variasi nilai *mean*, *varian* dan *density* dapat dilihat pada Tabel 4 dan Tabel 5.

Tabel 4
Variasi nilai *mean* dan *varian* untuk *noise gaussian*

Percobaan Ke -	*Mean*	*Varian*
1	0,000001	0,000001
2	0,00001	0,000001
3	0,001	0,000001
4	0,000001	0,00001
5	0,00001	0,00001
6	0,01	0,01
7	0,1	0,01
8	0,01	0,1
9	0,1	0,1
10	1	1

Tabel 5
Variasi nilai *density* untuk *noise salt & pepper*

Percobaan Ke -	*Density*
1	0,01
2	0,03
3	0,05
4	0,07
5	0,1
6	0,3
7	0,5
8	0,7
9	0,9
10	1

4.3.1. Pengujian Noise pada Algoritma RSA

Hasil dekripsi citra terenkripsi dengan algoritma RSA yang telah ditambahkan *noise gaussian* secara kualitatif dengan nilai *mean* 0,000001 dan 0,000001 serta nilai *varian* 0,000001 berada pada kriteria *passable* (cukup baik, masih bisa diterima). Untuk citra terenkripsi yang dinaikan nilai *varian* menjadi 0,00001 berada pada kriteria *unusable* (sudah tidak dapat dikenali lagi), sedangkan untuk citra yang dinaikan nilai *mean* sampai 0,001 berada pada kriteria *inferior* (sangat buruk, tetapi masih bisa diamati) dikarenakan pada hasil dekripsinya masih bisa dilihat pola dari citra.

Secara kuantitatif hasil citra dekripsi RSA dari citra terenkripsi yang ditambahkan *noise gaussian* dapat dilihat pada Tabel 6.

Tabel 6
Penilaian kuantitatif citra dekripsi RSA dari citra terenkripsi yang ditambahkan *noise gaussian*

(*Mean, Varian*)	MSE		PSNR (dB)	
	blue.bmp	ctscan.bmp	blue.bmp	ctscan.bmp
(0,000001 , 0,000001)	1289,11	3739,8	43,37	28,56
(0,00001 , 0,000001)	1252,98	3697,23	43,85	28,67
(0,001 , 0,000001)	4085,98	12226,6	31,93	16,71
(0,000001 , 0,00001)	10072,2	30537,5	22,71	7,56
(0,00001 , 0,00001)	10018,1	30422	22,76	7,60
(0,01 , 0,01)	13161,2	39289,4	19,01	5,04
(0,1 , 0,01)	12955,7	40011,7	19,79	4,86
(0,01 , 0,1)	13691,7	38240,7	17,47	5,31
(0,1 , 0,1)	13403,3	39147,9	18,40	5,08
(1 , 1)	11212,1	36343,8	21,45	5,82

Dari Tabel 6 terlihat bahwa nilai MSE terkecil terdapat pada citra blue.bmp yang ditambahkan *noise gaussian* dengan nilai *mean* 0,00001 dan *varian* 0,000001 dimana menghasilkan nilai MSE 1252,98 dan nilai PSNRnya 43,85 dB, sedangkan nilai MSE terbesar terdapat pada citra ctscan.bmp yang ditambahkan *noise gaussian* dengan nilai *mean* 0,1 dan *varian* 0,01 dimana menghasilkan nilai MSE 40011,7 dan nilai PSNR 4,86 dB.

Untuk hasil dekripsi citra terenkripsi dengan algoritma RSA yang telah ditambahkan *noise salt & pepper* secara kualitatif dengan nilai *density* 0,01, 0,03, dan 0,05 berada pada kriteria *passable* (cukup baik, masih bisa diterima*)*. Untuk citra dekripsi dari citra terenkripsi dengan nilai *density* 0,1 berada pada kriteria *inferior* (sangat buruk, tetapi masih bisa diamati) dikarenakan pada hasil dekripsinya masih bisa dilihat pola dari citra aslinya, sedangkan citra dekripsi dari citra terenkripsi dengan nilai *density* 0,3 berada pada kriteria *unusable* (sudah tidak dapat dikenali lagi).

Secara kuantitatif hasil citra dekripsi dari citra terenkripsi yang ditambahkan *noise salt & pepper* dapat dilihat pada Tabel 7.

Tabel 7
Penilaian kuantitatif citra dekripsi RSA dari citra terenkripsi yang ditambahkan *noise salt & pepper*

Density	MSE		PSNR (dB)	
	blue.bmp	ctscan.bmp	blue.bmp	ctscan.bmp
0,01	257,79	783,55	58,95	44,19
0,03	787,61	2312,39	47,18	33,37
0,05	1256,66	3767,06	42,71	28,49
0,07	1773,5	5154,82	39,02	25,35
0,1	2501,04	7160,13	35,42	22,07
0,3	6771,54	18935,2	24,71	12,34
0,5	10171,6	26961,6	20,07	8,81
0,7	12792,1	31013,6	17,20	7,41
0,9	14452,6	31283,9	15,49	7,32
1	14909,5	30170,6	14,99	7,68

Dari Tabel 7 dapat dilihat bahwa nilai MSE terkecil terdapat pada citra blue.bmp yang ditambahkan *noise salt & pepper* dengan nilai *density* 0,01 dimana menghasilkan nilai MSE 257,79 dan nilai PSNR 58,95 dB, sedangkan nilai MSE terbesar terdapat pada citra ctscan.bmp yang ditambahkan *noise salt & pepper* dengan nilai *density* 1 dimana menghasilkan nilai MSE 31283,9 dan nilai PSNR 7,32 dB.

4.3.2. Pengujian Noise pada Algoritma RC6

Hasil dekripsi citra terenkripsi dengan algoritma RC6 yang telah ditambahkan *noise gaussian* secara kualitatif dengan variasi nilai *mean* dan *varian* pada pengujian berada pada kriteria *unusable* (sudah tidak dapat dikenali lagi).

Secara kuantitatif hasil citra dekripsi dari citra terenkripsi yang ditambahkan *noise gaussian* dapat dilihat pada Tabel 8.

Tabel 8
Penilaian kuantitatif citra dekripsi RC6 dari citra terenkripsi yang ditambahkan *noise gaussian*

(*Mean, Varian*)	MSE		PSNR (dB)	
	blue.bmp	ctscan.bmp	blue.bmp	ctscan.bmp
(0,000001 , 0,000001)	7651,92	4133,06	23,24	27,56
(0,00001 , 0,000001)	7767,37	4137,24	22,84	27,55
(0,001 , 0,000001)	12992,1	7097,07	17,88	22,16
(0,000001 , 0,00001)	13705,5	5962,43	17,19	23,90
(0,00001 , 0,00001)	13685,4	7398,76	17,32	21.74
(0,01 , 0,01)	13562,2	7406,36	17,47	21,73
(0,1 , 0,01)	13724	7401,46	17,32	21,74
(0,01 , 0,1)	13596,3	7425,32	17,40	21,70
(0,1 , 0,1)	13647,9	7406,45	17,37	21,73
(1 , 1)	13641,2	7395,93	17,30	21,74

Dari Tabel 8 dapat dilihat bahwa nilai MSE terkecil terdapat pada citra ctscan.bmp yang ditambahkan *noise gaussian* dengan nilai *mean* 0,000001 dan *varian* 0,000001 dimana menghasilkan nilai MSE 4133,06 dan nilai PSNRnya 27,56 dB, sedangkan nilai MSE terbesar terdapat pada citra blue.bmp yang ditambahkan *noise gaussian* dengan nilai *mean* 0,000001 dan *varian* 0,00001 dimana menghasilkan nilai MSE 13705,5 dan nilai PSNR 17,19 dB.

Untuk hasil dekripsi citra terenkripsi dengan algoritma RC6 yang telah ditambahkan *noise salt & pepper* secara kualitatif dengan nilai *density* 0,01 berada pada kriteria *passable* (cukup baik, masih bisa diterima). Untuk citra dekripsi dari citra terenkripsi dengan nilai *density* 0,03 pada gambar ctscan.bmp berada pada kriteria *inferior* (sangat buruk, tetapi masih bisa diamati) dikarenakan pada hasil dekripsinya masih bisa dilihat pola dari citra aslinya, sedangkan pada citra dekripsi dari citra terenkripsi lainnya berada pada kriteria *unusable* (sudah tidak dapat dikenali lagi).

Secara kuantitatif hasil citra dekripsi dari citra terenkripsi yang ditambahkan *noise salt & pepper* dapat dilihat pada Tabel 9.

Tabel 9
Penilaian kuantitatif citra dekripsi RC6 dari citra terenkripsi yang ditambahkan *noise salt & pepper*

Density	MSE		PSNR (dB)	
	blue.bmp	ctscan.bmp	blue.bmp	ctscan.bmp
0,01	2019,41	1108,85	36,24	40,72
0,03	5428,85	2836,68	26,50	31,33
0,05	7500,29	4155,14	23,28	27,51
0,07	9257,64	5021,3	21,14	25,62
0,1	11008,1	5962,43	19,43	23,90
0,3	13725,7	7393,19	17,36	21,74
0,5	13664,3	7420,91	17,37	21,71
0,7	13646,2	7426,77	17,42	21,70
0,9	13667,8	7431,23	17,36	21,70
1	13663,6	7443,58	17,37	21,68

Dari Tabel 9 dapat dilihat bahwa nilai MSE terkecil terdapat pada citra ctscan.bmp yang ditambahkan *noise salt & pepper* dengan nilai *density* 0,01 dimana menghasilkan nilai MSE 1108,85 dan nilai PSNR 40,72 dB, sedangkan nilai MSE terbesar terdapat pada citra blue.bmp yang ditambahkan *noise salt & pepper* dengan nilai *density* 0,3 dimana menghasilkan nilai MSE 13725,7 dan nilai PSNR 17,37 dB.

4.4. Pengujian Kompresi

Pengujian kompresi dilakukan dengan cara menyimpan citra enkripsi dengan format terkompresi yaitu format JPG dan PNG. Hasil dekripsi dari citra terenkripsi yang telah dikompresi ke format JPG secara kualitatif berada pada kriteria *unusable* (sudah tidak dapat dikenali lagi), sedangkan untuk citra dekripsi dari citra terenkripsi yang telah dikompresi ke format PNG berada pada kriteria e*xcellent* (kualitas terbaik, seperti aslinya).

Secara kuantitatif hasil citra dekripsi dari citra terenkripsi menggunakan algoritma RSA dan RC6 yang telah dikompresi terdapat pada Tabel 10.

Tabel 10
Penilaian kuantitatif citra dekripsi dari citra terenkripsi yang dikompresi

Algoritma	Citra	MSE	PSNR (dB)
RSA	decryptedRSA_blue.jpg	12918,8	19,76
	decryptedRSA_blue.png	0	Inf
	decryptedRSA_ctscan.jpg	39453,6	5,00
	decryptedRSA_ctscan.png	0	Inf
RC6	decryptedRC6_blue.jpg	13629,4	17,28
	decryptedRC6_blue.png	0	Inf
	decryptedRC6_ctscan.jpg	7424,28	21,70
	decryptedRC6_ctscan.png	0	Inf

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil pengujian dan analisis didapatkan beberapa kesimpulan sebagai berikut :

1. Algoritma RC6 memiliki waktu proses enkripsi dan dekripsi yang lebih cepat dari algoritma RSA.
2. Algoritma RSA memiliki ketahanan terhadap *noise* lebih baik dibandingkan algoritma RC6. Berdasarkan uji serangan *noise* yang dilakukan algoritma RSA dapat menerima variasi *noise* yang lebih besar dari algoritma RC6. Hal tersebut dibuktikan dengan hasil penilaian citra dekripsi secara kualitatif dan kuantitatif yang dilakukan. Dari hasil pengujian algoritma RSA dapat bertahan terhadap *noise gaussian* dengan nilai *mean* 0,00001 dan *varian* 0,000001 mendapatkan nilai MSE 1252,98 dan PSNR 43,85 dB, sedangkan RC6 tidak dapat bertahan dengan nilai *mean* dan *varian* yang sangat kecil sekalipun. Kemudian terhadap *noise salt & pepper* algoritma RSA dapat bertahan terhadap *noise* dengan nilai *density* 0,05 mendapatkan nilai MSE 1256,66 dan PSNR 42,71 dB, sedangkan algoritma RC6 hanya dapat bertahan pada nilai *density* 0,01 dengan nilai MSE 1108,85 dan PSNR 40,72 dB.
3. Kedua algoritma ini sama-sama tidak tahan terhadap pengujian *lossy compression* sedangkan untuk *lossless compression* masih bisa bertahan terhadap uji kompresi yang dilakukan.

5.2. Saran

Beberapa saran yang dapat diberikan antara lain:

1. Aplikasi dapat dikembangkan menggunakan program aplikasi lain untuk memperbesar nilai kunci RSA.
2. Penggunaan algoritma kriptografi lainnya yang lebih tahan terhadap serangan *noise*.
3. Melakukan uji serangan lainnya seperti *cropping*, *rotate*, atau menambahkan *noise* lain.
4. Melakukan keamanan pada kunci yang digunakan untuk menjaga kerahasiaannya pada saat pengiriman kunci ke penerima pesan.
5. Melakukan pengujian dengan mengirim data citra menggunakan kanal.

DAFTAR PUSTAKA

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

[2] El-shame, F., Ahmed. H., dkk. 2014. *Image Encryption : A Communication Perspective.* CRC Press. London.

[3] Komba, K. 2014. *Kriptografi Pada Citra Digital Menggunakan Algoritma RSA (Rivest, Shamir, Adleman).* Jurusan Teknik Elektro. Universitas Nusa Cendana. Kupang.

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

[5] Phakira, Malay. 2014. *Digital Image Processing and Pattern Recognition.* Collage Kalyani. West Bengal.

[6] Rudianto. 2007. *Analisis Keamanan Algoritma Kriptografi RC6.* Institut Teknologi Bandung. Bandung.

[7] Schneier, B. 1996. *Aplied Cryptography 2nd*. John Wiley & Sons.

[8] 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. KMCT College of Engineering. India.