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

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

[1,2,3] *Jurusan Teknik Elektro Fakultas Sains dan Teknik Undana,*
Jl. Adisucipto Penfui-Kupang-NTT Telp (0380) 881557.
Email: arul.win1@gmail.com
Email: siltena@staf.undana.ac.id
Email: sarlince_manu@staf.undana.ac.id

ABSTRACT

The digital image is a medium that can be stored on storage media or transmitted over a network. However, in transmission, data theft and misuse may occur that are detrimental to interested parties. Therefore, to protect and maintain the confidentiality of a digital image, cryptographic methods are used. In this study, a comparison of two algorithms was used, namely Rivest Shamir Adleman (RSA) and Rivest Code 6 (RC6). RSA is an asymmetric algorithm where the encryption and decryption keys are different, while RC6 is a symmetric algorithm where the keys are the same. The test shows that the operating time of the RC6 algorithm is faster than the RSA algorithm. On the other hand, the noise test carried out by RSA is more durable than RC6. For Gaussian noise with a mean value of 0.00001 and a variant of 0.000001, the MSE value is 1252.98 and PSNR 43.85 dB, while RC6 cannot stand this noise. Then for salt & pepper noise, RSA can survive at a density value of 0.05 with MSE values 1256.66 and PSNR 42.71 dB, while RC6 can survive at density values 0.01 with MSE values 1108.85 and PSNR 40.72. dB. Both algorithms are equally resistant to lossy compression based on the compression test, while for lossless compression, both algorithms can still survive. The results of the decryption are the same as the original image.

Keywords: *Kriptografi, RSA, RC6, Noise*

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, Noise*

1. PENDAHULUAN

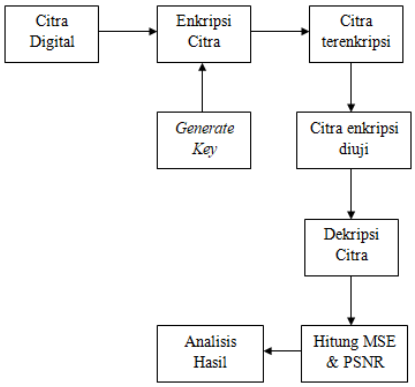
Komunikasi data merupakan proses pengiriman dan penerimaan data/informasi dari dua atau lebih perangkat yang terhubung dalam sebuah jaringan. Proses pengiriman data dengan memanfaatkan jaringan seperti internet cukup efisien, cepat, dan murah. Namun terdapat juga beberapa kekurangan yang memungkinkan 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* [1].
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 [2]. 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 [3]. Kelebihan algoritma ini terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor primanya [4]. Selain metode algoritma RSA ada metode *kriptografi* lain yang dapat digunakan dalam keamanan citra digital yaitu Algoritma *Rivest Code* 6 (RC6) [5, 6]. 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 [7].

2. METODE PENELITIAN

2.1. Diagram Alir Sistem

Berikut adalah perancangan dan desain sistem keamanan citra menggunakan algoritma RSA dan 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 dekripsi citra menggunakan algoritma RSA dan RC6 [8]. Gambaran umum dari sistem ini dapat dilihat pada Gambar 1.

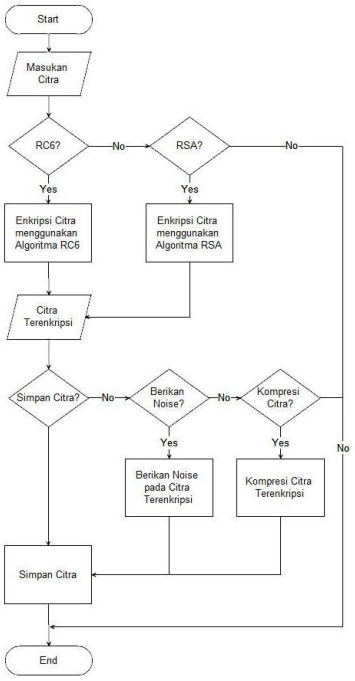


Gambar 1 Gambaran Umum Sistem Keamanan Citra

Dari gambaran umum proses di atas proses enkripsi dan deskripsi dapat dijelaskan sebagai berikut :
1. Citra digital dienkripsi terlebih dahulu menggunakan algoritma RSA dan 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 dan PSNR dari citra tersebut.
4. Hasil yang didapatkan menunjukkan algoritma yang lebih baik.

2.2. *Flowchart* Proses Enkripsi

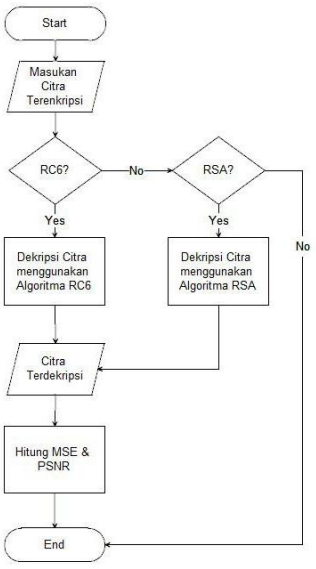
Untuk *flowchart* proses enkripsi yang diteliti dapat dilihat pada Gambar 2. Algoritma proses enkripsi yang ditunjukan pada Gambar 2 yaitu:
1. Masukan citra yang akan dienkripsi.
2. Kemudian jika citra ingin dienkripsi menggunakan algoritma RC6, maka program akan mengenkripsi citra masukan menggunakan 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 dekripsi menggunakan algoritma RC6, maka program ingin mendekripsi citra masukan menggunakan algoritma RC6. Jika citra ingin dekripsi menggunakan algoritma RSA, maka program akan mendekripsi citra masukan menggunakan algoritma RSA.
3. Keluarkan dari proses dekripsi adalah citra terdeskripsi
4. Citra yang sudah didekripsi dihitung MSE dan PSNRnya untuk mendapatkan hasil algoritma mana yang lebih baik antara RSA dan RC6 dalam keamanan citra digital.



Gambar 3 *Flowchart* Proses Dekripsi

3. HASIL DAN PEMBAHASAN

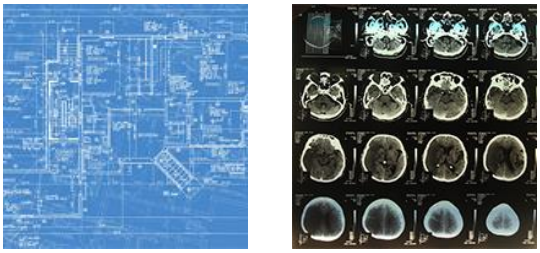
3.1. Pengujian *Black Box*

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.

3.2. 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 *ct scan* dengan citra deskripsinya. 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 dilihat 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

3.3. 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

3.3.1. 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 deskripsinya 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 ct scan.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 deskripsinya 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 ct scan.bmp yang ditambahkan *noise salt & pepper* dengan nilai *density* 1 dimana menghasilkan nilai MSE 31283,9 dan nilai PSNR 7,32 dB.

3.3.2. 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 ct scan.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 *densitas* 0,03 pada gambar ct scan.bmp berada pada kriteria *inferior* (sangat buruk, tetapi masih bisa diamati) dikarenakan pada hasil deskripsinya 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 ct scan.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.

3.4. Pengujian Kompresi

Pengujian kompresi dilakukan dengan cara menyimpan citra enkripsi dengan format terkompresi yaitu format JPG dan PNG. Hasil deskripsi 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

4. 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.

DAFTAR PUSTAKA

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

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

[3] Shahana, T., "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, KMCT College of Engineering. India, 2013.

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

[5] Mardiana, "Pengembangan Algoritma Block Cipher RC6 pada Citra Digital," *Skripsi,* Universitas Sumatera Utara. Medan, 2013.

[6] Phakira, Malay, "Digital Image Processing and Pattern Recognition. *College Kalyani*. West Bengal, 2014.

[7] Rudianto, "Analisis Keamanan Algoritma Kriptografi RC6," Institut Teknologi Bandung. Bandung, 2007.

[8] Schneier, B., "Applied Cryptography 2nd, *John Wiley & Sons*, 1996.