IMPERCEPTIBLE KRIPTOGRAFI CITRA BERWARNA MENGGUNAKAN RIVEST SHAMIR ADLEMAN

Christy Atika Sari[1], Wellia Shinta Sari[2], Bambang Sugiarto[3]
[1,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[2]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]christy.atika.sari@dsn.dinus.ac.id, [2]wellia.shinta.sari@dsn.dinus.ac.id, [3]bambangsugiarto2427@gmail.com

ABSTRAK

Algoritma Rivest Shamir Adleman (RSA) adalah algoritma unggul yang memanfaatkan teknik asimetris dengan 2 buah kunci berbeda yaitu privat dan public. Proses dekripsi RSA dengan memfaktorkan nilai bilangan prima yang begitu besar dan perhitungan operasi matematika yang rumit. Penelitian ini bertujuan untuk melalukan enkripsi dekripsicitra digital berwarna. Pengujian kemiripan antara citra asli dengan citra yang telah terenkripsi menggunakan nilai Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) serta pengujian lain seperti Bit Error Rate (BER) dan Entropy. Dari hasil MSE dan PSNR antara citra asli dengan citra hasil enkripsi hasil menunjukkan bahwa untuk nilai MSE lebih dari 0, dan nilai PSNR kurang dari 30dB. Hal ini menunjukkan bahwa kedua gambar antara gambar asli dan gambar setelah terenkripsi memiliki perbedaan yang signifikan.

***Kata Kunci**: RSA, citra, MSE, PSNR, BER, entropy*

PENDAHULUAN

Dengan berkembangnya teknologi informasi pada masa ini membuat pertukaran data menjadi semakin praktis dan efisien, namun juga berbanding lurus dengan tingkat kejahatan *cyber* yang semakin canggih sehingga membutuhkan keamanan berlapis untuk perlindungan data. Media digital seperti gambar atau foto adalah media digital yang seringkali tidak terlalu diperhatikan dampak negatifnya, jika dimanfaatkan oleh pihak yang tidak berkepentingan [1]. Terdapat banyak manipulasi pada gambar digital yang sering disalahgunakan hanya untuk kepentingan pribadi sehingga membuat pemilik asli dari gambar tersebut merasa dirugikan karena gambar yang dimanipulasi dapat menunjukkan citra yang buruk. Adapun permasalahan yang lainya adalah adanya citra yang diubah dan digunakan oleh pihak tertentu tanpa sepengetahuan pemilik dari citra tersebut. Dari permasalahan tersebut merupakan indikasi dari tindakan pencurian [2]. Hal ini disebabkan kurangnya perhatian terhadap masalah keamanan dari para perancang atau pengelola sistem informasi sehingga berakibat buruk bagi pengguna. Dengan demikian dibutuhkan teknik untuk mengatasi masalah kerahasiaan data. Suatu metode yang dianggap paling efektif untuk mengatasi masalah tersebut adalah metode kriptografi.

Teknik kriptografi merupakan studi tentang keamanan data yang digunakan untuk mengamankan proses komunikasi antara pengirim dan penerima agar terhindar dari pihak ketiga. Kriptografi itu sendiri mempunyai banyak definisi, salah atunya yaitu kriptografi dapat digunakan untuk mengubah data atau informasi kedalam bentuk yang berbeda dengan data aslinya, sehingga data tersebut tidak dapat dikenali [3]–[5]. Pada dasarnya teknik kriptografi digunakan untuk mengenkripsi dan mendekripsi informasi dalam bentuk data berupa teks, gambar, video, suara, dan sebagainya. Tujuan dari kriptografi yaitu mengamankan data dengan bentuk lain yang tidak dikenali orang awam serta dapat dikirimkan menggunakan jaringan tanpa ada yang mengetahui dan terhindar dari pihak-pihak yang tidak berwenang. Kriptografi dapat dikategorikan menjadi beberapa kelas. Kelas pada kriptografi adalah algoritma asimetris, algoritma simetris, dan fungsi hash [6], [7]. Algoritma yang sering digunakan pada kriptografi dan cukup terkenal, salah satu metode yang dianggap efektif untuk enkripsi dan digital signature yaitu Rivest Shamir Adleman (RSA) [8].

Rivest Shamir Adleman (RSA) merupakan bagian dari kriptografi modern 2 kunci yang dikenal dengan kunci publik dan kunci privat. Kesulitan dari algoritma ini terletak pada sulitnya untuk menemukan kunci privat, meskipun ada beberapa serangan yang mungkin terjadi pada algoritma ini tapi tidak mengurangi kegunaan dan fungsinya [3]. Algoritma RSA dikembangkan pada tahun 1977 dan mulai dipublikasikan pada tahun 1978. Metode RSA dapat menyembunyikan informasi dari gambar sehingga tidak dapat dikenali menggunakan kunci publik dan mengembalikan gambar seperti semula dengan menggunakan kunci privat. Keunggulan dari algoritma RSA terletak pada tingkat kesulitan untuk menentukan hasil dari faktor bilangan prima yang sangat besar [5], [9]. Dari hasil pemfaktoran tersebut kemudian akan digunakan untuk mendapatkan nilai dari kunci privat. Apabila nilai dari pemfaktoran bilangan prima belum ditemukan, maka bisa dikatakan bahwa tingkat keamanan dari algoritma Rivest Shamir Adleman (RSA) masih tetap aman. Metode RSA dipilih untuk proses enkripsi dan dekripsi pada gambar karena mempunyai tingkat keamanan yang sangat tinggi.

Dalam penelitian yang dilakukan oleh Shankar [10], menggunakan dua metode yaitu Rivest Shamir Adleman (RSA) dan Particle Swarm Optimazation(PSO). Proses enkripsi dekripsi dilakukan degan RSA, kemudian algoritma PSO digunakan untuk melakukan proses optimasi kunci publik pada algoritma RSA. Nilai NPCR mendekati 100 sednagkan UACI antara 25 sampai 30 sedangkan PSNR menghasilkan nilai kurang dari 10 dB. Kemudian penelitian terkait lainnya yang dilakukan oleh Eko Budi Setiawan dan Yogie Setiawan Nugraha, menggunakan algoritma RSA untuk mengenkripsi dan mendekripsi gambar [11]. Hasil menunjukkan bahwa gambar yang telah terenkripsi tidak dapat dikenali data yang sebenarnya, namun belum ada proses pengujian secara empiris misalnya MSE PSNR dari citra hasil.

Berdasarkan uraian keunggulan RSA dan beberapa penelitian yang sudah dilakukan. Terdapat beberapa ide untuk menggunakan media kriptografi berupa citra digital dan proses pembuktian proses kriptografi. Urgensi penelitian ini adalah melakukan enkripsi dekripsi file gambar dengan menggunakan algoritma kriptografi RSA dan melakukan uji analisa hasil menggunakan MSE, PSNR, BER, entropy.

TINJAUAN PUSTAKA

Konsep Kriptografi

Kriptografi menurut istilah adalah teknik untuk mengamankan pesan rahasia pada saat dikirm dari tempat satu ke tempat lain melalui jaringan. Semakin berkembangnya teknologi, kegunaan kriptografi juga semakin bertambah. Kriptografi bisa juga digunakan untuk mengidentifikasi pengirim pesan, kriptografi juga dapat digunakan untuk menguji tingkat keaslian pada tanda tangan digital dan sidik jari digital [12], [13]. Tingkat keamanan pada algoritma kriptografi terdapat pada bagaimana algoritma kriptografi bekerja. Cara menyembunyikan kunci pada kritografi merupakan letak keamanan dari algoritma kriptografi, tanpa menyerahkan kerahasiaan tersebut pada pihak lain [14]. Kunci pada algoritma kriptografi sama halnya seperti kata sandi yang kita miliki, jika kata sandi tersebut berhasil dianalisa dan diberitahukan kepada pihak yang tidak berwenang maka algoritma tersebut dikategorikan mempunyai tingkat keamanan yang rendah. Kriptografi memberikan keamanan yang baik untuk menjamin privasi agar tetap terlindungi dari pihak yang tidak berkepentingan. Pada saat ini kriptografi masih banyak digunakan karena memiliki keamanan yang baik. Ada beberapa tujuan dari kriptografi, antara lain [15] :

1. Tingkat Kerahasiaan

   Informasi yang telah dirahasiakan harus dijaga dan dilindungi dan tidak boleh dibocorkan sehingga data tidak bocor ke pihak lain, kecuali kepada pihak yang mempunyai wewenang akan informasi tersebut.
2. Autentifikasi

   Autentifikasi merupakan berhubungan dengan pengenalan pada informasi. Hubungan antara penerima dan pengirim harus dikenali dengan baik, selama proses pengiriman informasi dipastikan tidak adanya pengintai atau penyusup.
3. Integritas data

   Sistem yang akan digunakan dapat mendeteksi tidak terjadi adanya manipulasi data oleh pihak lain.
4. Non-repudiasi

   Pencegahan terjadinya penyangkalan selama proses mengirim ataupun menerima pesan.

Proses enkripsi merupakan proses dimana pesan asli yang nantinya akan diubah menjadi chiperteks atau pesan setelah dienkripsi, sedangkan untuk pengertian dekripsi adalah proses dimana pesan yang telah terenkripsi diubah menjadi bentuk semula atau pesan asli. Pada teknik kriptografi istilah enkripsi digunakan untuk melindungi data yang bersifat rahasia yang nantinya diubah kedalam bentuk yang tidak dapat dikenali sehingga terhidar dari pihak yang tidak berwenang. Apabila ditinjau secara matematika konsep kriptografi memiliki dua buah himpunan, yaitu himpunan yang memiliki plainteks dan himpunan yang memiliki chiperteks. Proses pada enkripsi dan dekripsi adalah elemen yang memetakan dari kedua himpunan tersebut. Misalnya symbol P dinyatakan dengan plainteks dan symbol C dinyatakan dengan chiperteks. Sehingga fungsi perhitungan enkripsi yang dinyatakan dengan symbol E memetakan P ke C seperti pada persamaan (1) dan persamaan (2) sedangkan dekripsi yang disimbolkan dengan D memetakan fungsi C ke P.

$$E(P) = C \quad (1)$$

$$D(C) = P \quad (2)$$

Rivest Shamir Adleman (RSA)

Pembentukan kunci RSA ini merupakan langkah awal sebelum dilakukanya proses enkripsi dan dekripsi. Ada beberapa tahapan dalam pembentukan kunci algoritma RSA:

1. Memilih 2 buah nilai prima yaitu p dan q secara acak. Dimana $p \neq q$
2. Menghitung nilai p serta q menggunakan persamaan (3) dan persamaan (4).

$$n = p \; x \; q \quad (3)$$

$$\emptyset(n) = (p-1)(q-1) \quad (4)$$

3. Cari nilai kunci publik e dengan ketentuan nilai e harus relative prima terhadap $\emptyset(n)$.
4. Hitung nilai kunci privat d sesuai persamaan (5).

$$d = \frac{1+(k \; x \; \emptyset(n))}{e} \quad (5)$$

5. Apabila $ed \; mod \; \emptyset(n) = 1$, maka nilai e dan d dapat digunakan.

3. METODE PENELITIAN

Sumber Data

Dataset yang digunakan adalah Lena, Tiffany, Jet dan Sailboat dengan ukuran 512x512 piksel dengan totoal bytes sebanyak 768000. Gambar tersebut bisa diakses melalui link https://www.na.icar.cnr.it/~maddalena.l/DFRLab/GC06BlueScratches.html seperti tampak pada Gambar 1 berikut.

Lena.tif Jet.tif Tiffany.tif Sailboat.tif

Gambar 1. Dataset penelitian

Proses Enkripsi

Setelah mengetahui nilai *[e,n]* dan *[d,n]* pada tahap pembentukan kunci. Langkah selanjutnya adalah melakukan enkripsi. Enkripsi adalah proses pengubahan plainteks menjadi chiperteks. Berikut adalah langkah-langkah dalam melakukan enkripsi sesuai Gambar 2 (a).

1. Citra host harus digunakan sebagai input.
2. Citra host diubah menjadi angka.
3. Buat kunci RSA sesuai teori pada sub bab 2.1pilih 2 nilai prima acak untuk menentukan nilai p dan q. dalam makalah ini nilai p dan q yang digunakan adalah p = 13, q = 31 dan p = 23, q = 67.
4. Lakukan proses enkripsi menggunakan algoritma RSA sesuai persamaan (6), dinana C adalah chipertext, sedangkan M adalah pesan atau plaintext yang akan dilakukan proses enkripsi.

$$C = M^e mod \; n \quad (6)$$

5. Setelah melakukan proses enkripsi, chiperteks berhasil didapatkan.

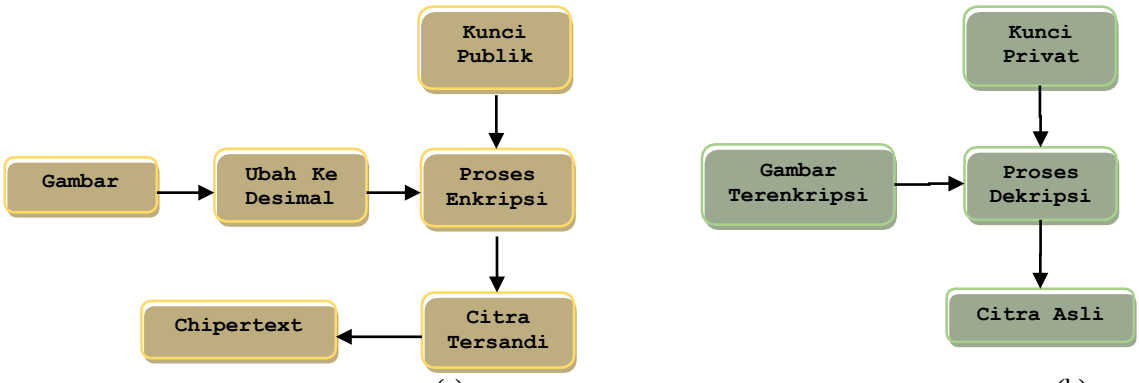
Proses Dekripsi

Dekripsi digunakan untuk mengubah chipertext menjadi plaintext atau proses pengubahan gambar yang telah dienkripsi menjadi gambar asli atau data awal. Adapun langkah-langkah dari dekripsi sebagai berikut:

1. Gambar yang telah diproses enkripsi dijadikan sebagai input.
2. Kemudian lakukan proses dekripsi melalui persamaan (7), dimana M adalah pesan awal, dan C adalah chipertext atau pesan yang telah terenkripsi.

$$M = C^d mod \; n \quad (7)$$

3. Setelah gambar berhasil didekripsi, plainteks berhasil didapatkan.



(a) (b)

Gambar 2. Skema Penelitian : (a) Enkripsi, (b) Dekripsi

Teknik Analisis Data

MSE untuk melihat kesalahan kuadrat rata-rata antara gambar sebelum dan sesudah dienkripsi. Semakin tinggi nilai MSE yang dihasilkan maka akan semakin jauh pula persamaan antara gambar sebelum dan sesudah dienkripsi dan begitu juga dengan sebaliknya. Adapun rumus perhitungan MSE dapat dilihat apda persamaan (8), dimana S adalah plain-image dan C adalah chiper-image, nilai M dan N menunjukan ukuran dari kedua gambar, sedangkan x dan y adalah nilai dari koordinat piksel.

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[S_{xy} - C_{xy}\right]^2 \quad (8)$$

PSNR digunakan untuk mengetahui perbandingan kualitas dan kuantitas antara kedua gambar. Apabila nilai PSNR diatas 30dB maka bisa dikatakan bahwa nilai tersebut sudah ideal, yang artinya persamaan antara kedua gambar hampir sama atau mirip, begitu juga dengan sebaliknya [10]. Adapun rumus perhitungan PSNR sesuai persamaan (9), dimana xy^2_{max} adalah nilai maksimum pada suatu citra, citra dengan 8 bit biasanya maksimal 255 piksel.

$$PSNR = 10 \log 10 \left(\frac{xy^2_{max}}{MSE}\right) \quad (9)$$

Entropy digunakan untuk mengetahui ketidakteraturan pada suatu citra. Nilai entropy dikatakan bagus apabila mendekati angka 8. Adapun rumus perhitungan entropy sesuai persamaan (10), dengan G adalah jumlah nilai k, sedangkan P(k) adalah kemungkina kemunculan nilai dari k, dan log adalah logaritma basis 2.

$$H_e = -\sum_{k=0}^{G-1} P(k) log_2 (P(k)) \quad (10)$$

BER digunakan untuk mengetahui jumlah bit yanf berbeda pada citra sebelum dan sesudah dienkripsi. Apabila nilai BER semakin rendah maka bisa dikatakan nilai tersebut ideal atau bagus. Nilai BER dikatakan ideal apabila nilainya sama dengan 0. E adalah nilai bit yang error sedangkan T adalah jumlah keseluruhan bit yang dikirimkan sesuai pada persamaan (11).

$$BER = \frac{E}{T} \quad (11)$$

4. HASIL DAN PEMBAHASAN

Pembentukan Kunci RSA

Tahapan pembentukan RSA sesuai pada kajian pada point 2.2 sebelumnya.

1. Pilih 2 bilangan prima secara acak yaitu p = 13 dan q = 31. Untuk perhitungan pada nilai p = 23 dan q = 67 disesuaikan saja dengan langkah-langkahnya.
2. Hitung nilai n yaitu dengan menggunakan persamaan berikut:
   $n = 13 \; x \; 31 = 403$
   Hitung $\emptyset(n) = (13 - 1)(31 - 1) = 12 \; x \; 30 = 360$
3. Cari nilai kunci publik e, dimana nilai e harus relative prima terhadap $\emptyset(n)$.
4. Ambil nilai e = 7, nilai tersebut tidak harus 7. Bisa menggunakan angka lain, yang terpenting nilai e harus relative prima terhadap $\emptyset(n)$. Karena 7 relative prima terhadap 360 jadi nilai 7 bisa digunakan.

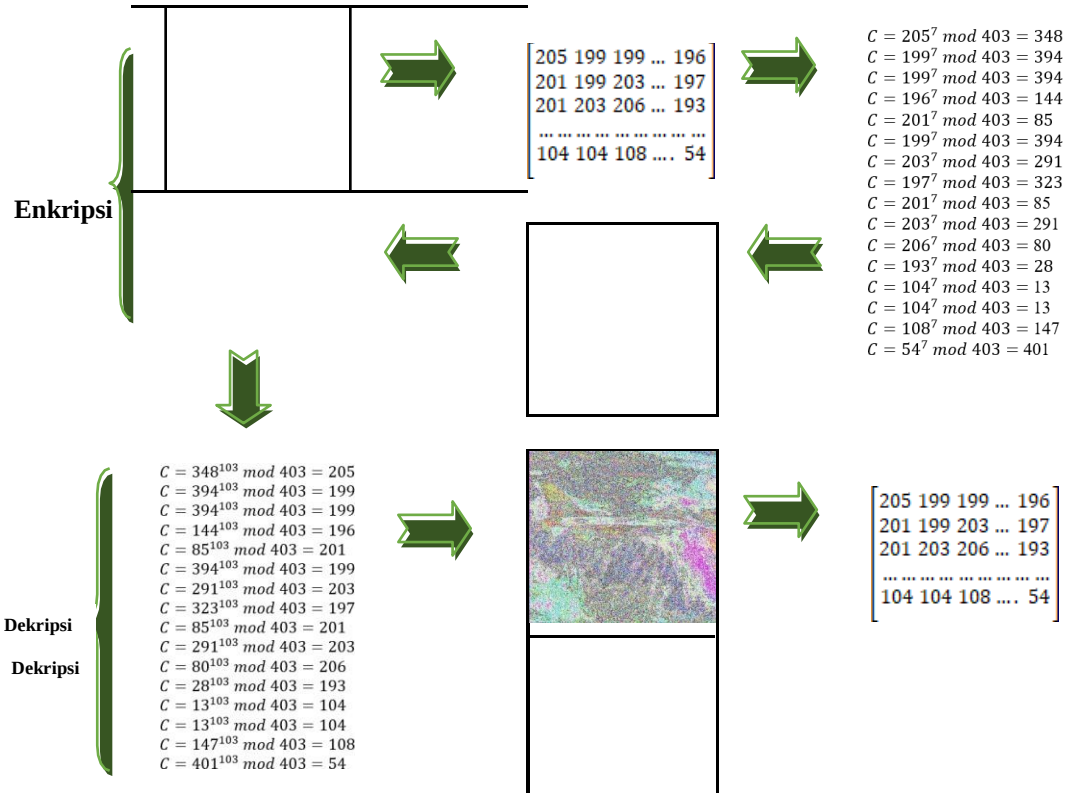
5. Hitung nilai kunci privat d (nilai d harus desimal tidak boleh pecahan) sebagai berikut:

$$d1 = \frac{1 + (1\ x\ 360)}{7} = 51{,}57 \quad \text{dan} \quad d2 = \frac{1 + (2\ x\ 360)}{7} = 103$$

Karena pada iterasi ke-2 nilai d sudah desimal maka pencarian nilai d dihentikan dan dihasilkan $ed\ mod\ \emptyset(n) = 7x\ 103\ mod\ 360 = 721\ mod\ 360 = 1$ karena $ed\ mod\ \emptyset(n) = 1$ maka nilai e dan d bisa digunakan.

Enkripsi Citra

Citra harus dijadikan sebagai inputan kemudian ubah ke dalam bentuk desimal, kemudian lakukan proses enkripsi pada semua nilai M. Setelah berhasil dienkripsi maka dihasilkan gambar dan matriks yang telah terenkripsi sesuai Gambar 3.

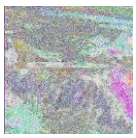
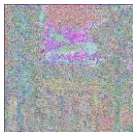


Gambar 3. Proses Enkripsi dan Dekripsi

Berdasarkan Gambar 3, berikut ini merupakan hasil dari gambar yang telah dilakukan proses enkripsi menggunakan algoritma RSA. Untuk lebih jelasnya perhatikan Tabel 1 dimana telah dilakukan uji coba menggunakan dua buah nilai p dan 1 yang berbeda. Tujuan dua nilai ini hanya sebagai pembanding saja. Pada Tabel 1, hasil enkripsi pada gambar menggunakan algortima RSA dengan nilai p = 13, q = 31 dan p = 23, q = 67. Hasil menunjukan bahwa kedua gambar sudah berhasil dilakukan enkripsi, namun untuk gambar dengan nilai p = 13, q =

31 menunjukan hasil gambar yang cukup jelas atau hampir bisa dikenali dikarenakan masih ada pola yang membentuk gambar asli tersebut. Sedangkan pada gambar dengan nilai p = 23, q = 67 menunjukan hasil gambar yang sudah tidak bisa dikenali lagi bahkan sudah sangat berbeda dan tidak ada pola yang mirip dengan gambar asli.

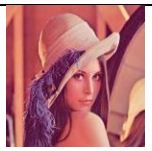
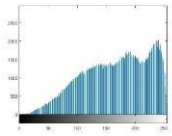
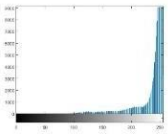
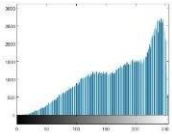
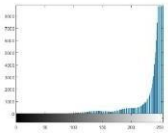
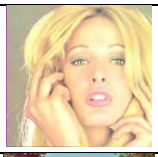
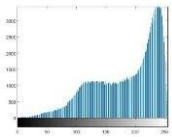
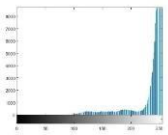
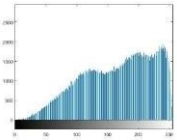
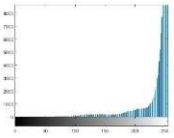
Tabel 1. Citra hasil enkripsi

Citra Asli	Enkripsi	
	p=13 dan q=31	p=23 dan q=67
		
		
		
		

Histogram Cipher

Tabel 2 merupakan perbandingan histogram pada gambar yang telah terenkripsi dengan nilai p=13, q=31dan p=23, q=67. Hasil menunjukan bahwa gambar dengan nilai p=13 dan q=31 mempunyai pola yang lebih rendah dibandingkan dengan gambar histogram dengan nilai p=23 dan q=67.

Tabel 2. Citra hasil enkripsi

Citra Asli	Enkripsi	
	p=13 dan q=31	p=23 dan q=67
		
		
		
		

MSE, PNSR, dan BER

Penelitian ini menggunakan alat ukur atau pengujian menggunakan MSE, PSNR, BER, dan Entropy sesuai Tabel 3 dan Tabel 4.

Tabel 3. Analisa MSE, PSNR, dan BER

Citra	MSE		PSNR		BER	
	p=13, q=31	p=23, q=67	p=13, q=31	p=23, q=67	p=13, q=31	p=23, q=67
Lena.tif	19212.8	697364	-42.8359	-58.4346	0	0
Tiffany.tif	16204.1	494611	-42.0963	-56.9426	0	0
Jet.tif	15254.1	654309	-41.8339	-58.1578	0	0
Sailboat.tif	21790.6	664377	-43.3827	-58.2241	0	0
Rata-rata	**18115.4**	**627665.3**	**-42.5372**	**-57.9398**	**0**	**0**

Berdasarkan Tabel 3 di atas, telah dipaparkan hasil perbandingan nilai MSE, PSNR dan BER dengan nilai p dan q yang semakin besar. Hasil menunjukan bahwa nilai p=23 dan q=67 meghasilkan PSNR lebih tinggi di banding nilai p=13 dan q=31. Hal ini disebabkan oleh pengaruh dari bilangan prima yang dipilih, dimana semakin besar bilangan prima yang di pilih maka akan semakin bagus pula hasil dari enkripsi pada gambar. Namun untuk hasil BER antara nilai p=13, q=31 dan p=23, q=67 mempunyai hasil yang sama yaitu 0. Hal ini menandakan bahwa semua gambar berhasil didekripsi dengan sempurna dan tidak ada bit yang hilang.

Entropy

Berikut ini adalah Tabel 4 yang berisi perbandingan entropy pada chiper-image dengan nilai p=13, q=31 dan p=23, q=67.

Tabel 4. Nilai Entropy

Citra	Entropy	
	p=13, q=31	p=23, q=67
Lena.tif	5.69311	0.94812
Tiffany.tif	4.22182	0.905759
Jet.tif	4.52213	1.06017
Sailboat.tif	5.55035	1.10706
Rata-rata	**4.996853**	**1.005277**

Tabel 4 menunjukkan bahwa untuk nilai bilangan prima p=13, q=31 lebih unggul dibandingkan dengan nilai entropy pada bilangan prima p=23, q=67. Nilai tersebut jauh dari nilai ideal pada nilai entropy. Nilai entropy dikatakan bagus apabila mendekati nilai 8. Sehingga hasil implementasi algoritma masih kurang sempurna jika di lihat dari perhitungan entropy.

5. KESIMPULAN

RSA telah digunakan untuk melakukan enkripsi dekripsi pada citra berwarna. Bilangan prima yang digunakan pada penelitian ini yaitu p=13, q=31 dan p=23, q=67. Hasil menunjukkan bahwa prose enkripsi dan dekripsi berhasil dilakukan menggunakn algoritma RSA. Keteracakan hasil enkripsi dapat dilihat dariMSE dan PSNR dengan hasil mendekati 0, dimana nilai MSE sangat tinggi yaitu lebih dari 0 dan nilai PSNR sangat rendah yaitu kurang dari 30 dB. Yang artinya kedua gambar sebelum dan sesudah di enkripsi sangat berbeda atau tidak memiliki kesamaan. Untuk bilangan prima yang lebih besar memiliki hasil enkripsi yang lebih bagus dari pada bilangan prima yang lebih kecil. Proses dekripsi berhasil dilakukan tanpa adanya bit atau piksel yang hilang. Sedangkan untuk nilai entropy pada bilangan prima yang lebih rendah yaitu p = 13 dan q = 31 lebih unggul dari pada p = 23 dan q = 67.

DAFTAR PUSTAKA

[1] S. S. Putra, P. S. Sasongko, and N. Bahtiar, “Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermarking,” *J. Sains dan Mat.*, vol. 19, no. 3, pp. 75–81, 2011.

[2] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *J. Appl. Intell. Syst.*, vol. 3, no. 1, pp. 28–38, 2018.

[3] R. Mathur, S. Agarwal, and V. Sharma, "Solving security issues in mobile computing using cryptography techniques — A Survey," in *International Conference on Computing, Communication & Automation*, 2015, pp. 492–497.

[4] A. D. Alrehily, A. F. Alotaibi, S. B. Almutairy, M. S. Alqhtani, and J. Kar, "Conventional and Improved Digital Signature Scheme: A Comparative Study," *J. Inf. Secur.*, vol. 06, no. 01, pp. 59–67, 2015.

[5] N. Sharma, Prabhjot, and H. Kaur, "A Review of Information Security using Cryptography Technique.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 323–326, 2017.

[6] C. Sari, E. Rachmawanto, Y. Astuti, and L. Umaroh, "Optimasi penyandian file menggunakan kriptografi shift cipher," in *Seminar Multi Disiplin Ilmu Unisbank (SENDI_U) ke-2 Semarang*, 2016.

[7] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper Dan End of File," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.

[8] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. Ignatius, and M. Setiadi, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in *International Conference on Smart Cities, Automation & Intelligent Computing Systems*, 2017, pp. 1–6.

[9] M. Vanitha and R. Mangayarkarasi, "Comparative study of different cryptographic algorithms," *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 26433–26438, 2016.

[10] S. K, "An Optimal RSA Encryption Algorithm for Secret Images," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2491–2500, 2018.

[11] E. B. Setiawan and Y. S. Nugraha, "Kriptografi Citra Menggunakan Metode Rivest-Shamir-Adleman Chinese Remainder Theorem Di Konsultan XYZ," *J. Ultim.*, vol. 7, no. 2, pp. 82–90, 2016.

[12] S. Goyal, M. Ramaiya, and D. Dubey, "Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images," in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015, pp. 1120–1124.

[13] J. Weir, W. Q. Yan, and M. S. Kankanhalli, "Image Hatching for Visual Cryptography," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 8, no. S2, 2012.

[14] C. A. Sari and E. H. Rachmawanto, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[15] P. A. Nani, "PENERAPAN ENKRIPSI ALGORITMA BLOWFISH PADA PROSES STEGANOGRAFI METODE EOF," *Penerapan Enkripsi Algoritm. Blowfish Pada Proses Steganografi Metod. Eof*, pp. 1–6, 2011.