Analisis Integritas Data pada Kriptografi Citra Digital Menggunakan Penggabungan Arnold's Cat Map dan Bernoulli Map

Ruddy J Suhatril dan Rama Dian Syah

Fakultas Ilmu Komputer dan Teknologi Informasi
Universitas Gunadarma, Jl. Margonda Raya No. 100, Depok
E-mail: ruddyjs@staff.gunadarma.ac.id, rama_ds@staff.gunadarma.ac.id

Abstrak

Kriptografi merupakan teknik untuk keamanan data. Perubahan data terenkripsi mungkin terjadi pada saat pengiriman data melalui internet oleh pihak lain. Integritas data diperlukan untuk menghindari hal tersebut. Analisis integritas data diterapkan pada kriptografi citra digital untuk menguji keamanan suatu algoritma kritptografi. Metode kriptografi pada penelitian ini yaitu mengimplementasikan penggabungan algoritma Arnold's Cat Map dan Bernoulli Map. Pengujian integritas data dilakukan dengan melihat hasil proses dekripsi dari sebuah citra terenkripsi yang sebelumnya sudah mengalami perubahan data. Hasil dari penelitian ini adalah algoritma tidak menjamin integritas data.

Kata Kunci: Integritas Data, Kriptografi, Arnold's Cat Map, Bernoulli Map.

Pendahuluan

Keamanan pada data dan informasi sangat penting pada perkembangan teknologi informasi saat ini. Data yang ditransmisikan pada jaringan internet harus terjaga keamanannya. Metode untuk keamanan diperlukan agar privasi data tidak tersebar ke publik. Kriptografi merupakan cabang ilmu matematika untuk keamanan data dan informasi seperti kerahasiaan, keutuhan data dan otentikasi. Kriptografi menggunakan berbagai metode matematika untuk menjaga isi pesan terenkripsi [1].

Kriptografi memiliki beberapa aspek keamanan. Integritas data merupakan salah satu aspek keamanan kriptografi untuk menjaga pengubahan data dari pihak yang tidak berwenang. Integritas data harus memastikan bahwa hanya pihak yang berwenang yang dapat melakukan modifikasi data dan informasi yang dikirimkan. Modifikasi data tersebut yaitu menulis, mengubah, menghapus, menunda atau memutar ulang pesan yang dikirim [2].

Kriptografi dapat diimpelementasikan pada citra digital. Enkripsi pada citra adalah teknik kriptografi untuk menjaga informasi pada pesan citra dari pengaksesan tanpa izin. Enkripsi pada citra harus dilakukan pada waktu yang cepat dengan tingkat keamanan yang tinggi [3]. Peningkatan keamanan pada kriptografi dapat dilakukan dengan menggabungkan dua algoritma yaitu metode Arnold's Cat Map dan Bernoulli Map.

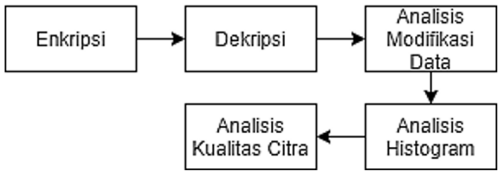
Kedua metode tersebut memiliki karakter yang berbeda. Karakter pada Arnold's Cat Map yaitu mengacak posisi piksel citra tanpa mengubah nilai piksel, sedangkan karakter pada Bernoulli Map yaitu membangkitkan nilai bilangan acak untuk mengubah nilai piksel menggunakan operasi XOR. Pengujian metode kriptografi dapat dilakukan dengan analisis integritas data. Pengujian dilakukan dengan cara memodifikasi citra terenkripsi dan melihat hasil dari proses dekripsi dari citra tersebut.

Pada penelitian ini disajikan analisis integritas data pada kriptografi citra digital menggunakan penggabungan Arnold's cat map dan Bernoulli Map. Analisis akan meliputi analisis hasil proses enkripsi dan dekripsi, analisis perubahan data, analisis histogram dan analisis psnr.

Metode Penelitian

Penelitian ini dilakukan dengan 5 tahapan yaitu: (1) enkripsi; (2) dekripsi; (3) analisis perubahan data; (4) analisis histogram; (5) analisis kualitas citra. Berikut Diagram alur tahapan penelitian dapat dilihat pada Gambar 1.

DOI : http://dx.doi.org/10.32409/jikstik.19.1.2778



Gambar 1: Kerangka Kerja Penelitian

Proses enkripsi dan dekripsi dilakukan pada citra digital berdimensi persegi dengan tipe warna grayscale dan RGB. Hasil dari proses enkripsi dan dekripsi akan dianalisis.

Enkripsi

Enkripsi dilakukan dengan mengacak posisi piksel menggunakan Arnold's Cat Map dengan persamaan berikut [4].

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \qquad (1)$$

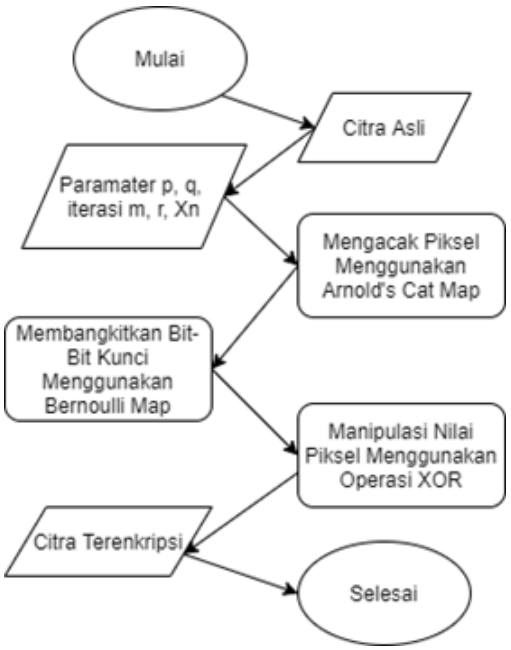
Nilai p dan q merupakan kunci rahasia dengan angka bilangan positif yang mempunyai panjang kunci tak terbatas. Nilai x dan y merupakan posisi piksel citra asli. N merupakan ukuran citra asli N × N. Kemudian bit-bit kunci dibangkitkan menggunakan fungsi Bernoulli Map dengan persamaan berikut [5].

$$x_{n+1} = r \times x_n \bmod 1 \qquad (2)$$

Nilai Xn merupakan kunci rahasia dengan rentang Xn ∈ [0, 1] dengan nilai awal dimulai dari 0.1 sedangkan r ∈ [1, ∞]. Kedua kunci merupakan angka bilangan desimal. Kemudian nilai piksel dirubah oleh operasi XOR dengan persamaan sebagai berikut [6].

$$I_C = I_P \oplus I_K \qquad (3)$$

Nilai Ic merupakan piksel citra terenkripsi, Nilai Ip merupakan piksel citra asli dan Ik merupakan bit-bit kunci yang dibangkitkan dengan fungsi Bernoulli Map. Diagram alur enkripsi menggunakan gabungan Arnold's Cat Map dan Bernoulli Map terdapat pada Gambar 2.



Gambar 2: Diagram Alur Enkripsi

Dekripsi

Dekripsi dilakukan dengan membangkitkan bit-bit kunci menggunakan Bernoulli Map yang terdapat pada persamaan 2. Kemudian mengembalikan nilai piksel menggunakan operasi XOR seperti pada persamaan berikut [6].

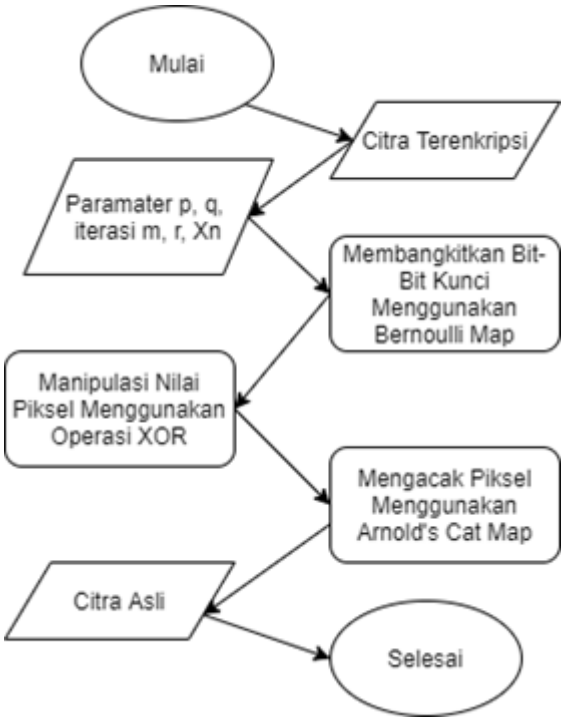
$$I_P = I_C \oplus I_K \qquad (4)$$

Kemudian posisi piksel dikembalikan menggunakan persaman dekripsi Arnold's Cat Map seperti persaman berikut [2].

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} \frac{pq+1}{pq+1-pq} & \frac{-p}{pq+1-pq} \\ \frac{-q}{pq+1-pq} & \frac{1}{pq+1-pq} \end{bmatrix} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(N \qquad (5)$$

Persamaan dekripsi Arnold's Cat Map meru-

pakan invers dari persamaan enkripsi Arnold's Cat Map. Diagram alur dekripsi menggunakan gabungan Arnold's Cat Map dan Bernoulli Map terdapat pada Gambar 3.



Gambar 3: Diagram Alur Dekripsi

Hasil dan Pembahasan

Data uji coba yang digunakan merupakan citra digital dengan tipe warna Grayscale dan RGB dengan ukuran 300 × 300. Berikut citra uji coba terdapat pada Tabel 1.

Tabel 1: Citra Asli

Citra *Grayscale*	Citra RGB
	
(a).png	(b).png

Sumber: https://homepages.cae.wisc.edu

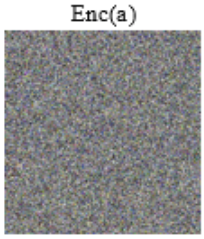
Citra asli (a) dan (b) dilakukan proses enkripsi dan dekripsi dengan parameter p = 30, q = 90, iterasi m = 5, Xn = 0.1 dan r = 1.5. Hasil dari proses enkripsi dan dekripsi terdapat pada Tabel 2.

Citra pada Tabel 2, enc(a) merupakan citra hasil enkripsi citra (a). Hasil enkripsi terlihat sangat baik karena sudah tidak terlihat lagi citra aslinya. Citra dec(a) merupakan citra hasil dekripsi citra enc(a). Pada citra (a), enc(a), dan dec(b) dilakukan proses yang sama.

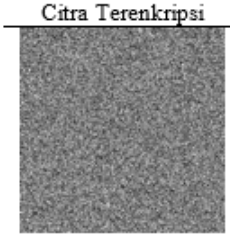
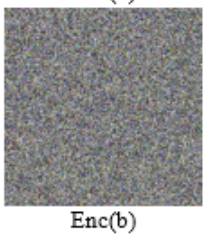
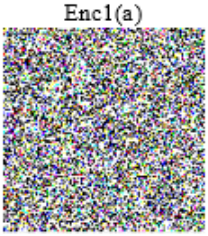
Analisis Perbedaan Data

Analisis dilakukan dengan mengubah nilai piksel pada citra terenkripsi. Nilai piksel yang dirubah adalah piksel dengan nilai 100 menjadi piksel dengan nilai 0. Kemudia citra yang sudah mengalami perubahan akan didekripsi dengan kunci rahasia yang sama pada saat proses enkripsi. Hasil dari proses perbedaan data terdapat pada Tabel 3.

Tabel 2: Hasil Proses Enkripsi dan Dekripsi Citra

Citra Asli	Citra Terenkripsi	Citra Terdekripsi
		
(a)	Enc(a)	Dec(a)
		
(b)	Enc(b)	Dec(b)

Tabel 3: Hasil Modifikasi Piksel Citra

Citra Sebelum Modifikasi Piksel		Citra Sesudah Modifikasi Piksel	
Citra Terenkripsi	Citra Terdekripsi	Citra Terenkripsi	Citra Terdekripsi
			
Enc(a)	Dec(a)	Enc1(a)	Dec1(a)
			
Enc(b)	Dec(b)	Enc1(b)	Dec1(b)

Pada citra enc1(a) dan enc1(b) terdapat noise. Hasil citra dec(a) dan dec (b) hampir sama dengan citra dec1(a) dan dec 1(b). Hal ini membuktikan bahwa metode algoritma tidak menjamin integritas data karena seharusnya apabila terjadi perubahan pada citra terenkripsi maka proses dekripsi akan gagal.

Analisis Kualitas Citra

Analisis kualitas citra dilakukan dengan cara melihat nilai PSNR (Peak Signal Noise to Ratio) antara citra terdekripsi sebelum modifikasi piksel dan citra terdekripsi sesudah modifikasi piksel. Persamaan PSNR terdapat pada persamaan 6 [7].

$$\text{PSNR} = 10\,\text{Log}_{10}\left(\frac{a^2 \text{max}}{\text{MSE}}\right) \qquad (6)$$

Untuk menemukan nilai PSNR, harus menentukan nilai MSE (Mean Square Error) terlebih dahulu. Persamaan MSE terdapat pada persamaan berikut 7.

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{X=1}^{M} \sum_{y=1}^{N} (a_{xy} - b_{xy})^2 \qquad (7)$$

Nilai x dan y merupakan koordinat piksel, m dan n merupakan dimensi citra. Nilai a dan b adalah nilai piksel pada citra. Berikut hasil dari analisis kualitas citra terdapat pada Tabel 4.

Tabel 4: Hasil Analisis Kualitas Citra

Citra Asli	Citra Terenkripsi Setelah Modifikasi Piksel	PSNR (dB)
 (a)	 Dec1(a)	19.29 dB
 (b)	 Dec1(b)	18.96 dB

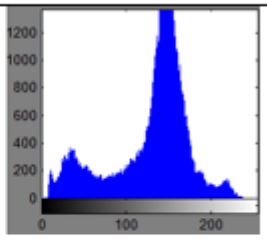
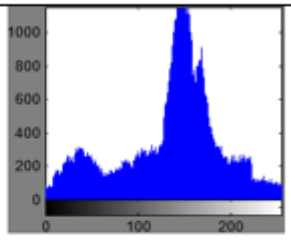
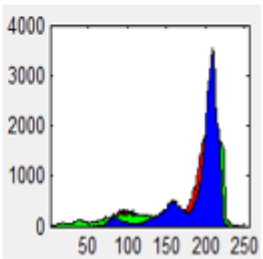
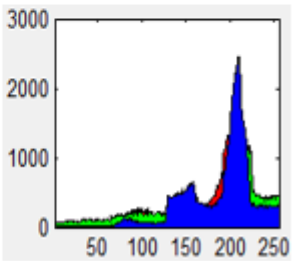
Apabila nilai PSNR menunjukkan inf maka citra identik. Pada tabel 4 nilai PSNR terdapat angka karena citra setelah modifikasi piksel terdapat noise, tetapi kemiripan citra sangat tinggi apabila dilihat secara kasat mata.

Analisis Histogram

Histogram pada citra merupakan nilai intensitas piksel pada suatu citra [8]. Analisis histogram dilakukan dengan membandingkan histogram antara citra asli dan citra terdekripsi setelah modifikasi piksel. Berikut hasil dari proses analisis histogram terdapat pada Tabel 5.

Histogram yang dihasilkan citra pada Tabel 5 terlihat ada perbedaan nilai frekuensi histogram. Nilai frekuensi histogram pada citra asli lebih tinggi dari pada citra dekripsi setelah modifikasi piksel sehingga citra tidak identik.

Tabel 5: Analisis Histogram

Citra Asli	Histogram Citra Asli	Citra Terdekripsi Setelah Modifikasi Piksel	Histogram Citra Terdekripsi Setelah Modifikasi Piksel
 (a)		 Dec1(a)	
 (b)		 Dec1(b).png	

Penutup

Berdasarkan hasil penelitian analisis integritas pada kriptografi citra digital menggunakan Penggabungan Algoritma Arnold's Cat Map dan Bernoulli Map dapat disimpulkan bahwa :

1. Terdapat kemiripan antara citra terdekripsi sebelum modifikasi piksel dan setelah modifikasi piksel sehingga algoritma kriptografi tidak menjamin integritas data. Pada citra terdekripsi setelah modifikasi piksel terdapat

noise.

2. Kualitas citra pada citra terdekripsi sebelum dan sesudah modifikasi piksel tidak memiliki kemiripan yang identik. Hal ini dibuktikan pada nilai PSNR yang tidak bernilai inf.
3. Nilai frekuensi pada hisogram terdapat perbedaan antara citra terdekripsi sebelum dan sesudah modifikasi piksel. Nilai pada citra terdekripsi setelah modifikasi piksel lebih rendah karena terdapat noise.

Daftar Pustaka

[1] M.R. Joshi and R.A. Karkade, "Network Security with Cryptography", International Journal of Computer Science and Mobile Computing, Volume 4, Pages 201-204, Januari 2015.

[2] V. Poornachander, "Security Issues on Cryptography and Network Security", International Journal of Computer Science and Information Technologies, Volume 7, Pages 1648-1654, 2016.

[3] M.T Suryadi, E. Nurpeti and D. Widya, "Performance of Chaos-Based Encryption Algorithm for Digital Image", Telecommunication Computing Electronics and Control, Volume 12, Pages 675-682, September 2014.

[4] R. Munir, "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif", Jurnal Ilmiah Teknologi Informasi, Volume 10, Pages 89-95, Juli 2012.

[5] H.E.H. Ahmed and A.H.A El-aziem, "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher", Recent Advances In Telecommunication, Informatics and Education Technologies, Pages 274-283, Desember 2014.

[6] K. Gupta and S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, Volume 2, Pages 139-150, Oktober 2011.

[7] D.M Setiadi, E.H Rachmawanto and C.A. Sari, "Implementasi One Time Pad Kriptografi pada Gambar Grayscale dan Gambar Berwarna," in Proc. Nasional Multi Disiplin Ilmu, pp. 50-56, 2017.

[8] H. Kaur and N. Sohi, "A Study for Application of Histogram in Image Enhancement", The International Journal of Engineering and Science, Volume 6, Pages 59-63, Juni 2017.