PENGEMBANGAN ALGORITMA KRIPTOGRAFI PADA CITRA DIGITAL UNTUK KEAMANAN DATA

SEMINAR BIDANG KAJIAN

Rama Dian Syah

99219031

PROGRAM DOKTOR TEKNOLOGI INFORMASI

UNIVERSITAS GUNADARMA

2021

Daftar Isi

Bab 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan komunikasi menyebabkan digitalisasi pada media seperti text, gambar, suara, dan video. Digitalisasi media dapat memudahkan akses dan modifikasi terhadap konten pada data yang ditransmisikan. Kemudahan yang pada digitalisasi media menyebabkan peluang terhadap kejahatan yang mungkin terjadi seperti akses tidak sah, modifikasi konten, pelanggaran hak cipta, dan lain-lain [1]. Keamanan data menjadi sangat penting pada media digital untuk menghindari kejahatan yang mengancam data yang bersifat rahasia dan privasi.

Berbagai teknologi dan komunikasi menggunakan media gambar atau citra di semua aspek untuk memudahkan pengguna. Citra dapat mengandung berbagai arti dan makna dalam menggambarkan suatu objek data atau informasi. Citra yang ditransmisikan melalui media sosial dari pihak penerima ke pengirim mungkin diakses oleh pihak yang tidak berwenang. Keamanan citra diperlukan untuk komunikasi yang aman.

Kriptografi merupakan ilmu yang berhubungan dengan transformasi data untuk membuat artinya tidak dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Kriptografi menggunakan berbagai macam teknik matematika untuk menjaga konten pada pesan terenkripsi [2].

Metode *Chaos* merupakan teknik enkripsi yang menjelaskan gerakan dinamika yang kompleks dan tidak terduga dari sebuah sistem yang tergantung dari kondisi awal. Terdapat beberapa algoritma kriptografi yang berbasis metode *chaos*. Penelitian sebelumnya yang telah meneliti kriptografi citra digital berbasis metode *chaos* yaitu menggunakan algoritma *Arnold's Cat Map (ACM)* [3], *Algoritma Bernoulli Map* [4].

Konsep dari algoritma *Arnold's Cat Map* adalah memutar pixel citra secara terus menerus sehingga bentuk menjadi bentuk yang tidak beraturan. Hasil yang di hasilkan tentu berbeda untuk tiap kunci yang ditentukan sedangkan algoritma *Bernoulli Map* merupakan fungsi chaos untuk membangkitkan bilangan acak yang akan digunakan sebagai *keystream* (dengan operasi XOR sederhana) atau untuk mengacak susunan pixel di dalam citra.

Dengan perbedaan dari karakter dari kedua algoritma tersebut dapat meningkatkan keamanan teknik kriptografi. Suatu citra asli akan diacak susunan pixelnya oleh algoritma

Arnold's Cat Map, kemudian algoritma Bernoulli Map akan membangkitkan *keystream* dengan operasi XOR yang akan menghasilkan citra enkripsi. Hasil dari proses tersebut akan dianalisis dengan beberapa metode analisa.

1.2 Identifikasi Masalah

Penerapan teknik enkripsi pada citra digital pada umumnya akan mebutuhkan waktu yang lama. Hal ini dikarenakan sebuah citra bervolume relatif sangat besar dibanding data tekstual. Selain itu, citra terdapat *pixel-pixel* di dalamnya yang seharusnya *pixel* tersebut teracak dengan baik pada saat proses enkripsi. Karena hal tersebut, maka teori *chaos* sangan cocok untuk teknik enkripsi citra. Teori *chaos* memiliki karakter yaitu sensitivitas terhadap kondisi awal, berkelakuan acak, dan tidak memiliki periode berulang [5].

Penelitian mengenai teknik enkripsi citra digital menggunakan teori *chaos* sedang banyak dilakukan dan diterapkan ke beberapa algoritma. *Arnold's Cat Map* dan *Bernoulli Map* merupakan algoritma yang menggunakan teori *chaos*. Perbedaan karakter algoritma dapat dikombinasikan sehingga meningkatkan keamanan pada teknik enkripsi.

1.3 Batasan Penelitian

1. Implementasi algoritma kriptografi pada citra digital.
2. Pengujian hasil uji enkripsi dan dekripsi yang dilakukan.

1.4 Perumusan Masalah Penelitian

1. Bagaimana membangun algoritma kriptografi yang digunakan untuk proses enkripsi dan dekripsi citra digital?
2. Bagaimana pengujian dari hasil proses enkripsi dan dekripsi?
3. Bagaimana kesimpulan dari pengujian yang sudah dilakukan?

1.5 Tujuan Penelitian

1. Mengembangkan algoritma kriptografi.
2. Menganalisis algoritma yang digunakan untuk mengetahui kemampuan algoritma
3. Membuat aplikatif dalam menerapkan algoritma pada citra digital untuk keamanan transmisi data

1.6 Manfaat Penelitian

Hasil dari penelitian ini memberi manfaat dan kontribusi pengembangan teknologi perangkat lunak yang dapat memberi keamanan pada citra digital pada saat pendistribusian citra digital pada media teknologi komunikasi. Selain itu penelitian ini memberikan kontribusi keilmuan berupa pengembangan algoritma kriptografi.

Bab 2

TINJAUAN PUSTAKA

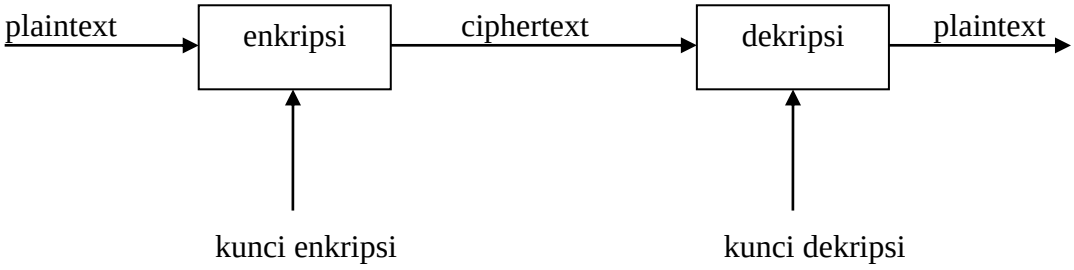
2.1 Kriptografi

Kriptografi adalah suatu teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi keaslian data [5]. Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

- *Plaintext* (M) adalah pesan yang hendak dikirim (berisi data asli).
- *Ciphertext* (C) adalah pesan terenkripsi yang merupakan hasil enkripsi
- Enkripsi adalah proses pengubahan *plaintext* menjadi *chipertext*.
- Dekripsi adalah kebalikan dari enkripsi yaitu mengubah *ciphertext* menjadi *plaintext* (data awal)
- Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi.

2.2 Proses Enkripsi dan Dekripsi

Kriptografi terdiri dari dua proses utama yaitu proses enkripsi dan dekripsi. Proses enkripsi mengubah *plaintext* menjadi *ciphertext* dengan menggunakan kunci tertentu sehingga informasi pada pesan tersebut sukar dimengerti.



Gambar 2.1 Diagram Proses Enkripsi dan Dekripsi

Pada Gambar 2.1 terdapat *plaintext* yang merupakan masukan pada proses enkripsi dengan kunci enkripsi yang sudah ditentukan. Hasil dari proses enkripsi adalah *ciphertext*, kemudian *ciphertext* digunakan untuk masukan pada proses dekripsi dengan kunci dekripsi yang sudah ditentukan. Hasil dari proses dekripsi adalah *plaintext*. Pesan yang digunakan untuk proses enkripsi dan pesan yang dihasilkan dari proses dekripsi merupakan pesan yang sama yaitu *plaintext*.

2.3 Tujuan Kriptografi

Terdapat beberapa tujuan dalam kriptografi [6]:

1. Kerahasiaan

   Menjaga isi informasi dari semua pihak kecuali yang memiliki otoritas terhadap informasi.

2. Integritas data

   Menjaga pesan dari pengubahan atau manipulasi data dari pihak yang tidak berwenang

3. Autentikasi

   Berhubungan dengan identifikasi atau pengenalan. Dua belah pihak harus saling memperkenalkan diri.

4. Non-repudiasi

   Mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirim/membuat.

2.4 Arnold's Cat Map

Algoritma *Arnold's Cat Map* (ACM) diperkenalkan pertama kali oleh seorang ahli matematik Rusia yang bernama Vladimir Arnold. Konsep kritptografi dari *Arnold's Cat Map* yaitu mengacak posisi atau susunan *pixel* di dalam citra tetapi tidak mengubah nilai pixel di dalam citra [6]. Algoritma Arnold's Cat Map untuk proses enkripsi didefinisikan sesuai persamaan 2.1 dan proses dekripsi didefiniskan pada persamaan 2.2

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \tag{2.1}$$

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N) \tag{2.2}$$

Keterangan:

x_{i+1} dan y_{i+1} : posisi pixel baru (Citra Enkripsi)

p dan q : kunci rahasia

x_i dan y_i : posisi pixel semula (citra asli)

N : ukuran citra

2.5 Bernoulli Map

Algoritma *Bernoulli Map* yang dilakukan oleh Hossam dan Ayman merupakan fungsi *chaos* yang digunakan pada kriptografi [4]. Perilaku acak yang dapat ditimbulkan dari algoritma ini dapat memberikan kombinasi yang baik dari kecepatan, keamanan yang tinggi dan kerumitan. Algoritma *Bernoulli Map* dapat didefinisikan pada persamaan 2.3 [4].

$$X_{n+1} = r \times X_n \ mod \ 1 \tag{2.3}$$

Persamaan 2.3 digunakan untuk proses enkripsi dan dekripsi pada algoritma *Bernoulli Map*, nilai X_n dan r merupakan kunci rahasia. Untuk nilai X_n mengambil nilai rentang $X_n \in [0, 1]$ dengan nilai awal X_n yaitu 0,1 sedangkan untuk nilai r mengambil nilai rentang $r \in [0, \infty]$ dan r merupakan bilangan desimal.

2.6 Pengembangan Algoritma

Algoritma yang akan diusulkan yaitu algoritma ACM dan Bernoulli Map. Algortima ACM yaitu algoritma memiliki konsep mengacak susunan pixel dalam citra tetapi tidak mengubah nilai piksel di dalam citra tetapi tidak mengubah nilai piksel di dalam citra. Sedangkan Algoritma Bernoulli Map yang memiliki konsep mengubah nilai piksel dalam citra [4]. Kedua algoritma dikombinasikan karena memiliki karakter yang berbeda sehingga dapat menghasilkan algoritma yang lebih kuat.

2.7 Kajian Penelitian

Terdapat beberapa penelitian sebelumnya yang menjadi referensi penulis dalam melakukan penelitian ini, terutama penelitian tentang algoritma berbasis Chaos.

Tabel 2.1. Penelitian Sebelumnya

Peneliti	Metode	Hasil	Kelebihan	Kekurangan
Hamza, Y. A (2019)	Algoritma Arnold's Cat Map	Algoritma Arnold's Cat mampu diterapkan untuk kriptografi dan steganografi	Algoritma yang diusulkan menghasilkan nilai PSNR yang tinggi	Algoritma yang diusulkan hanya diimplementasikan pada citra *greyscale*

Manocher C., Bobby D., dan Ruji P. (2019)	Algoritma Chaotic Logistic Map dan Pseudo-Random Generator	Algoritma yang diusulkan dapat menghasilkan citra terenkripsi yang aman untuk ditransmisikan secara online	Kombinasi Pseudo-Random Generator dan Logistic Map dapat meningkatkan keamanan	Tidak ada Analisa kualitas citra seperti PSNR dan MSE
Manzar Ali Khan (2019)	Algoritma GingerBreadman Map	Perbandingan beberapa algoritma kriptografi	Algoritma yang diusulkan tahan dan aman tarhadap serangan kriptografi berdasarkan perbandingan algoritma	Algoritma yang digunakan untuk perbandingan tidak terlalu dijelaskan
Anak Agung Putri Ratna (2021)	Arnold's Cat Map dan Henon Map	Analisis Korelasi dari algoritma yang diusulkan	Algoritma yang disulkan memiliki nilai korelasi yang mendekati 0 membuktikan tingkat keamanan yang baik	Iterasi berpengaruh terhadap waktu proses enkripsi

Penelitian yang dilakukan oleh Hamza [1], algoritma yang diusulkan menggunakan algoritma Arnold's Cat Map dan LSB. Algoritma ini diimplementasikan untuk kriptografi dan steganografi. Penelitian tersebut diimplementasikan pada citra *grayscale* dan menghasilkan nilai PSNR yang tinggi terhadap hasil proses algoritma.

Penelitian yang dilakukan oleh Manocher [7], algoritma yang diusulkan menggunakan algoritma *Logistic Map* yang dikombinasikan dengan Pseudo-Random Generator. Algoritma yang diusulan tersebut dapat meningkatkan keamanan berdasarkan pengujian sensitivitas kunci dan koefisian korelasi.

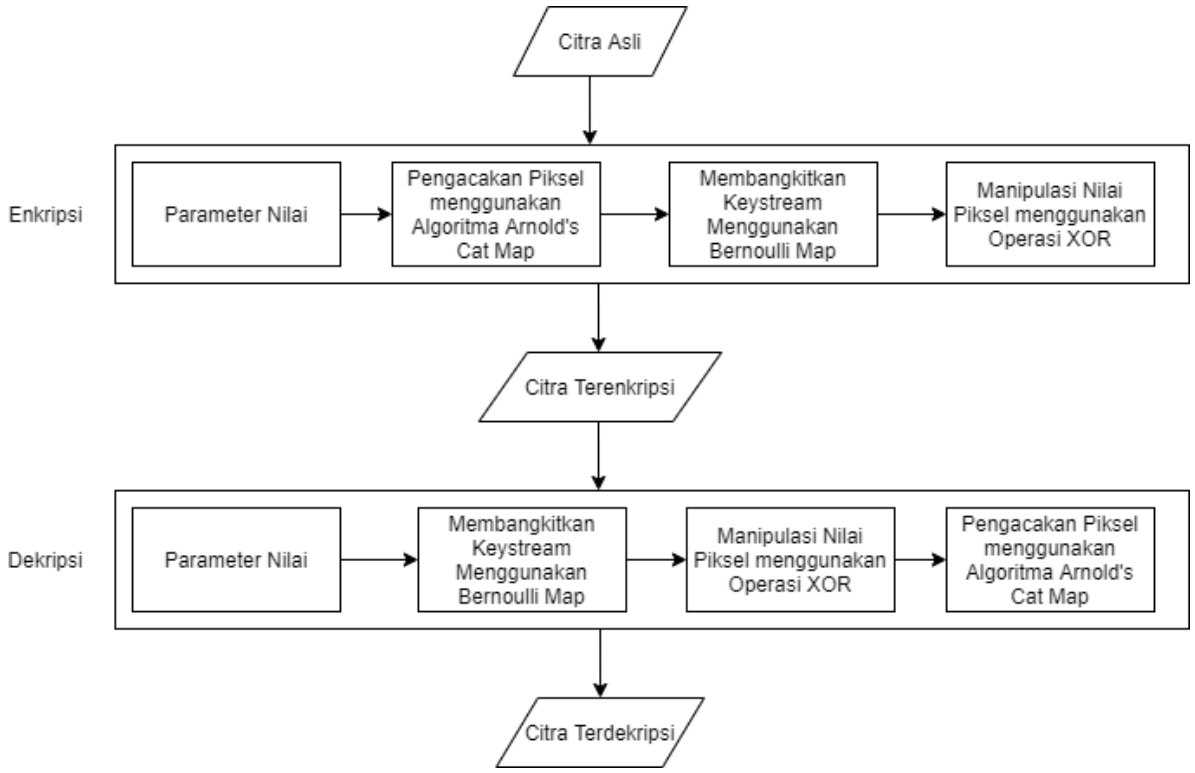
Penelitian yang dilakukan oleh Manzar [8], algoritma yang diusulkan menggunakan algoritma Gingerbreadman Map. Hasil dari algoritma yang diusulkan melalui beberapa pengujian yaitu entropi, korelasi, dan sensitivitas kunci. Pengujian yang dilakukan terhadap algoritma yang diusulkan membuktikan bahwa algoritma tahan dan aman dari serangan kriptografi.

Penelitian yang dilakukan oleh Agung [9], algoritma yang diusulkan menggunakan algoritma Arnold's Cat Map dan Henon Map. Algoritma yang diusulkan melakukan pengujian korelasi menghasilkan nilai korelasi yang mendekati 0 dan membuktikan tingkat kemananan yang baik.

Bab 3

METODOLOGI PENELITIAN

Tahapan penelitian terbagi menjadi beberapa tahapan ditunjukkan pada Gambar 3.1



Gambar 3.1 Metodologi Penelitian

3.1 Enkripsi

Tahap enkripsi merupakan dimana citra asli diubah menjadi citra terenkripsi. Enkripsi dilakukan pada beberapa algoritma yaitu:

1. **Arnold's Cat Map**

   Tahap enkripsi dilakukan dengan menggunakan proses persamaan Arnold's Cat Map dimana citra asli yang berbentuk matriks dikalikan dengan nilai parameter. Kemudian hasil dari perkalian dimodkan dengan ukuran citra semula, sehingga menghasilkan koordinat piksel yang baru.

2. **Bernoulli Map**

   Hasil dari proses Arnold's Cat Map dilakukan proses enkripsi dengan membangkitkan keystream menggunakan persamaan Bernoulli Map dengan nilai parameter.

Keystream akan di-XOR dengan piksel citra sehingga akan menghasilkan piksel citra terenkripsi.

3.2 Dekripsi

Tahap dekripsi dilakukan dengan citra terenkripsi sebagai input. Proses dekripsi dimulai dengan nilai parameter diproses menggunakan Algoritma Bernoulli Map, kemudian masuk ke Algoritma Arnold's Cat Map sehingga mengembalikan piksel dengan nilai dan koordinat semula pada citra terdekripsi atau citra asli.

3.3 Pengujian

Tahapan pengujian dilakukan untuk mengetahui hasil dari citra yang diproses menggunakan algoritma yang diusulkan. Berikut beberapa pengujianyang dilakukan yaitu:

1. Pengujian Waktu Enkripsi dan Dekripsi

   Pengujian bertujuan untuk mendapatkan waktu proses enkripsi dan dekripsi pada algoritma dan disajikan dalam bentuk tabel dan grafik.
2. Pengujian Histogram

   Pengujian dilakukan untuk mendapatkan histogram yang akan menjelaskan penyebaran intesitas *pixel* pada citra asli, citra terenkripsi dan citra terdekripsi.
3. Pengujian PSNR (*Peak Signal Noise to Ratio*)

   Pengujian dilakukan untuk mendapatkan nilai pnsr dalam satuan decibel (dB). Nilai psnr akan menjelaskan kualitas dua buah citra yaitu citra asli dan citra terdekripsi.
4. Pengujian Korelasi

   Pengujian dilakukan untuk mendapatkan nilai koefisien korelasi horizontal, vertikal, dan diagonal dari citra hasil enkripsi dan dekripsi.
5. Pengujian Integritas

   Pengujian dilakukan untuk mengetahui kualitas citra terenkripsi sebelum dan sesudah perubahan nilai piksel pada citra terenkripsi.
6. Pengujian Sensitivitas

   Pengujian dilakukan untuk menguji ketahanan kunci pada algoritma

Daftar Pustaka

[1] Y. A. Hamza, "Highly Secure Image Steganography Approach Using Arnold's Cat Map and Maximum Image Entropy," *Proc. Int. Conf. Inf. Commun. Technol.*, pp. 134–138, 2019, doi: 10.1145/3321289.3321323.

[2] M. R. Joshi and R. A. Karkade, "Network Security with Cryptography," *Int. J. Comput. Sci. Mob. Comput.*, 2015.

[3] M. Brindha, "Periodicity Analysis of Arnold Cat Map and Its Application to Image Encryption," *2017 Int. Conf. Inven. Comput. Informatics*, pp. 495–498, 2017, doi: 10.1109/ICICI.2017.8365401.

[4] H. E. H. Ahmed and A. H. A. El-aziem, "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher," *Recent Adv. Telecomunication, Informatics Educ. Technol.*, pp. 274–283, 2014.

[5] R. Munir, "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif," *JUTI J. Ilm. Teknol. Inf.*, vol. 10, no. 2, pp. 89–95, 2012, doi: 10.12962/j24068535.v10i2.a310.

[6] B. A. Wijakosno, "Steganografi Pada Citra Digial Dengan Metode Catmap dan Outguess," *J. String*, vol. 1, no. 3, pp. 317–324, 2017, doi: 10.30998/string.v1i3.1561.

[7] M. C. Alipour, B. D. Gerardo, and R. P. Medina, "A Secure Image Encryption Architecture Based on Pseudorandom Number Generator and Chaotic Logistic map," *Proc. 2019 2nd Int. Conf. Data Sci. Inf. Technol.*, pp. 154–159, 2019, doi: 10.1145/3352411.3352436.

[8] M. A. Khan, "New Image Encryption Scheme Using Chaotic Maps," *Proc. 3rd Int. Conf. Vision, Image Signal Process.*, pp. 1–6, 2019, doi: 10.1145/3387168.3389111.

[9] A. A. P. Ratna *et al.*, "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion," *Adv. Sci. Technol. Eng. Syst.*, vol. 6, no. 1, pp. 316–326, 2021, doi: 10.25046/aj060136.