Jurnal Masyarakat Informatika *ISSN: 2086-4930*
Vol. 13, No. 1, 2022 *e-ISSN: 2777-0648*

Implementasi Kriptografi dengan Menggunakan Algoritma Arnold's Cat Map dan Henon Map

Candra Irawan[*1)], Eko Hari Rachmawanto[2)]**

[*]Program Studi Sistem Informasi, Universitas Dian Nuswantoro
[**]Program Studi Teknik Informatika, Universitas Dian Nuswantoro
[1)]candra.irawan@dsn.dinus.ac.id, [2)]eko.hari@dsn.dinus.ac.id

Abstrak

Algoritma kriptografi merupakan sebuah seni matematis yang diimplementasikan untuk proses enkripsi dan dekripsi, medkanisme ini mengarah untuk mengenkripsi data asli menggunakan kombinasi berbeda dari kata, angka, atau ekspresi. Keamanan data terenkripsi sepenuhnya bergantung pada dua aspek penting, yaitu : kerahasiaan kunci dan kekuatan algoritma kriptografi. Teori chaos digunakan untuk memanggil bilangan secara acak, sehingga sifat dari gambar seperti redudansi data atau tingkat korelasi tinggi, hubungan antara nilai piksel dan biasanya berukuran besar akan diproses sehingga menghasilkan enkripsi menjadi kecil serta semakin acak bilangan yang dimunculkan semakin baik pula keamanannya. Macam-macam metode pada teori ini antara lain : Henon Map, Logistic Map, Arnold's Cat Map, Duffing Map, Tent Map, Beta Map dan sebagainya. Pada penilitian ini akan menggunakan dua metode yaitu Arnold's Cat Map dan Henon Map untuk proses enkripsi dan dekripsi. Serta untuk menutupi kekurangan Henon Map jika citra awalnya homogen, citra hasil enkripsinya akan sama dengan data awal, maka pada penelitian ini akan di klasifikasikan menjadi citra homogen dan heterogen dengan ekstraksi ciri orde 1 menggunakan standar deviasi dan nilai mean.

Kata kunci : *Arnold's Cat Map, Chaos, Henon Map, Kriptografi*

Abstract

Cryptographic algorithm is a mathematical art that is implemented for encryption and decryption processes, this mechanism leads to encrypting original data using different combinations of words, numbers, or expressions. The security of encrypted data completely depends on two important aspects, namely: the secrecy of the key and the strength of the cryptographic algorithm. Chaos theory is used to call numbers randomly, so that the properties of the image such as data redundancy or a high degree of correlation, the relationship between pixel values and usually large sizes will be processed so that the encryption becomes smaller and the more random the numbers are generated, the better the security. The various methods in this theory include: Henon Map, Logistic Map, Arnold's Cat Map, Duffing Map, Tent Map, Beta Map and so on. In this research, two methods will be used, namely Arnold's Cat Map and Henon Map for the encryption and decryption process. As well as to cover the shortcomings of Henon Map if the initial image is homogeneous, the encrypted image will be the same as the initial data, so in this study it will be classified into homogeneous and heterogeneous images with first-order feature extraction using standard deviation and mean value.

Keywords : *Arnold's Cat Map, Chaos, Henon Map, Cryptography*

1 PENDAHULUAN

Algoritma kriptografi merupakan sebuah seni matematis yang diimplementasikan untuk proses enkripsi dan dekripsi, mekanisme ini mengarah untuk mengenkripsi data asli menggunakan kombinasi berbeda dari kata, angka, atau ekspresi. Keamanan data terenkripsi sepenuhnya bergantung pada dua aspek penting, yaitu : kerahasiaan kunci dan kekuatan algoritma kriptografi [1], maka dari itu diharapkan dari suatu algoritma dan metode yang ada seharusnya semakin rumit proses enkripsinya akan semakin acak hasil enkripsi yang dimunculkan.

Teori chaos digunakan untuk memanggil bilangan secara acak, sehingga sifat dari gambar seperti redudansi data atau tingkat korelasi tinggi, hubungan antara nilai piksel dan biasanya berukuran besar akan diproses sehingga menghasilkan enkripsi menjadi kecil serta semakin acak bilangan yang dimunculkan semakin baik pula keamanannya [2], [3]. Macam-macam metode pada teori ini antara lain : Henon Map, Logistic Map, Arnold's Cat Map, Duffing Map, Tent Map, Beta Map dan sebagainya [4].

Berbagai algoritma enkripsi citra menggunakan chaos telah diusulkan, seperti algoritma Arnold's Cat Map dikombinasikan dengan algoritma Logistic Map 2-D menggunakan citra grayscale dilengkapi dengan proses confussion dan diffusion [3]. Terdapat penelitian lainnya, algoritma Arnold's Cat Map diproses bersama matrik N x N 2-D dan transpose dari matrik tersebut dihitung yang akan menghasilkan periode atau iterasi lebih tinggi daripada algoritma Arnold's Cat Map yang biasanya [5]. Algoritma yang diusulkan selanjutnya yaitu penggunaan algoritma Arnold's Cat Map dilanjutkan prosesnya oleh algoritma Henon Map yang akan memetakan nilai-nilai piksel dengan operasi XOR [6]. Peneliti lain mengimplementasi algortima Henon Map dilanjutkan dengan proses confusion dan diffusion yang dibandingkan dengan algoritma Logistic Map 2-D untuk menguji apakah algoritma Henon Map lebih baik daripada algoritma Logistic Map 2-D [7].

Henon Map mudah diaplikasikan pada data dua dimensi seperti gambar atau citra, karena Henon Map mempunyai persamaan dua dimensi [2]. Namun jika data awalnya bersifat sama atau homogen, maka hasil ciphernya tidak berbeda dan relatif sama dengan data awal [8]. Salah satu metode chaos lainnya yang populer dipakai yaitu Arnold's Cat Map yang dapat mengubah posisi piksel pada citra asli ke beberapa posisi baru yang tampak disusun ulang secara acak [6], dan hasil pengacakan posisi piksel tergantung pada parameter sistem [9], proses dekripsinya sederhana yaitu dengan melakukan pengulangan iterasi atau periode kembali beberapa kali, maka citra asli akan kembali muncul [5]. Namun mempunyai kelemahan dalam penyimpanan kuncinya [10].

Berdasarkan studi literatur yang telah ada sebelumnya, banyak peneliti yang menggunakan lebih dari satu algoritma chaos yang digabungkan atau menambahkannya dengan proses lainnya agar metodenya lebih kompleks sehingga keamanannya lebih baik. Untuk itu penilitian ini akan menggunakan dua metode yaitu Arnold's Cat Map dan Henon Map untuk proses enkripsi dan dekripsi. Serta untuk menutupi kekurangan Henon Map jika citra awalnya homogen, citra hasil enkripsinya akan sama dengan data awal, maka pada penelitian ini akan di klasifikasikan menjadi citra homogen dan heterogen dengan ekstraksi ciri orde 1 menggunakan standar deviasi dan nilai mean. Dan nilai untuk menguji performa kedua algoritma yang akan

dipakai berupa pengukuran nilai differential attack untuk pengukuran error citra yang diuji menggunakan nilai Avalanche Effect (AE), Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), kemudian nilai measurement of encryption quality untuk pengukuran kualitas citra yang diuji dengan nilai Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), serta analisis statistik yang akan mengukur nilai Koefesien Korelasi (Correlation Coefficient).

2 TINJAUAN PUSTAKA

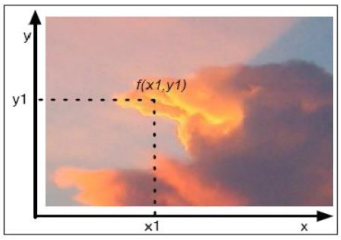
2.1 KRIPTOGRAFI

Kriptografi berasal dari dua kata: cryptos dan graphein. Cryptos berarti rahasia, dan graphein berarti menulis. Karena itu kriptologi berarti penulisan rahasia [11]. Kriptografi merupakan sebuah cara untuk menyampaikan pesan dari pengirim menuju penerima pesan yang seharusnya tanpa diketahui orang lain. Pesan dienkripsi sebelum pengiriman dan penerima melakukan dekripsi agar isi pesan tersebut bisa terbaca (Hadiman, Tjandra and Fadillah, 2020).

Kriptografi mempunyai dua proses, yaitu enkripsi disisi pengirim dan dekripsi disisi penerima [6]. Enkripsi merupakan proses mengubah citra asli (plain image) menjadi citra acak agar citra tersebut tidak bisa terbaca oleh pihak lain selain pengirim dan penerima. Citra acak tersebut dinamakan cipher image. Setelah pesan diterima oleh penerima, cipher image diubah kembali ke citra asli menggunakan kunci agar pesan tersebut dapat terbaca kembali. Proses tersebut dinamakan dekripsi [13].

2.2 CITRA DIGITAL

Representasi visual dari sebuah objek disebut citra. Citra juga bisa diartikan sebagai sebuah fungsi dari 2 objek dimensi f(x,y), dimana fungsi x dan y merupakan koordinat spasial dan f merupakan besaran disetiap pasang kordinat(x,y) yang dinamakan intensitas. Citra digital merupakan representasi data yang memiliki dua koordinat (tata letak) dan informasi intensitas (warna), dan bisa digunakan sebagai sinyal multidimensi [14, p. 1].



Gambar 1 Koordinat Citra Digital

Matriks M x N merupakan dimensi ukuran pada citra digital, dengan M merupakan tingginya atau sebagai baris dan N merupakan lebarnya sebagai kolomnya [2].

2.3 CHAOS

Pembangkit bilangan atau angka acak imajiner yang sulit untuk diprediksi oleh pihak lain atau Cryptographyically Secure Pseudorandom Generator (CSPRNG) biasa dikenal sebagai Chaos. Chaos diperkenalkan oleh Edward Lorentz seorang ahli meteorologi ketika sedang membuat model perkiraan cuaca pada tahun 1960. Model tersebut di iterasi agar menghasilkan perkiraan cuaca di kurun waktu mendatang. Semakin lama waktu perkiraan cuaca yang

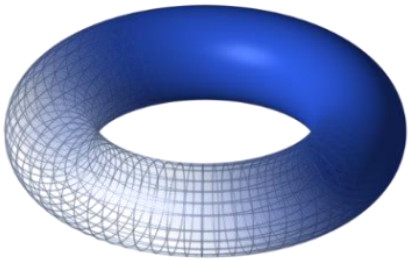
dihitung, semakin panjang iterasi yang harus dilakukan. Dengan mengubah sedikit awal iterasi yang hanya sebesar 0.000127, ia menemukan bahwa perkiraan cuaca yang dihasilkan mengalami divergensi yang besar [2]. Macam-macam metode pada teori ini antara lain : Henon Map, Logistic Map, Arnold's Cat Map, Duffing Map, Tent Map, Beta Map dan lain sebagainya [4].

2.4 HENON MAP

Michel Henon memperkenalkan Henon Map pada tahun 1978 sebagai model yang disederhanakan dari model Lorenz [15]. Henon Map dikenal sebagai sistem dinamis diskrit yang paling umum dipelajari dan digunakan yang memerlukan titik (x0,y0) untuk membuat titik baru yang acak [6]. Henon Map terbagi menjadi dua jenis yakni non kanonik dan kanonik, dimana non kanonik akan menghasilkan nilai acak yang berjarak dan dapat berulang secara berkala, sedangkan kanonik akan menghasilkan nilai acak yang tidak dapat berulang hampir mendekati tak hingga [2].

2.5 ARNOLD'S CAT MAP

Di tahun 1960-an Vladimir Igorevich Arnold seorang ahli matematika Rusia, mendeskripsikan sebuah Continuous Automorphisim of the Torus (CAT) dan menerapkannya ke gambar kucing [5].



Gambar 2 Skema Continuous Automorphisim of the Torus (CAT)

Transformasi citra untuk dapat terenkripsi dengan cara mengacak urutan piksel pada cirtra, lalu untuk mengembalikan ke citra asli cukup dilakukan pengulangan iterasi kembali beberapa kali, maka citra asli muncul kembali [5]. Jumlah dari iterasi dikenal sebagai periode Arnold, banyaknya iterasi tergantung pada ukuran gambar, untuk gambar dengan ukuran berbeda maka periode Arnold juga akan berbeda [16]. Dalam algoritma ini koordinat piksel dalam dimensi N x N dikalikan dengan matriks 2 x 2 khusus untuk mendapatkan koordinat X dan Y yang baru. Properti pembeda dari perkalian adalah perhitungan bidang tertutup, yang disediakan oleh operasi modulo N [17].

2.6 AVALANCHE EFFECT (AE)

Perubahan dalam satu bit dari plaintext atau satu bit kunci harus menghasilkan perubahan dalam banyak bit teks kata sandi disebut sebagai Avalanche Effect (AE). Kuncinya akan menghasilkan perubahan pada banyak bit dalam ciphertext. Nilai ideal untuk AE dikategorikan baik jika perubahan dalam bit bernilai sebesar 45%-60% (50% adalah hasil yang sangat baik). Ini karena perubahan ini berarti membuat perbedaan yang cukup sulit bagi cryptanalyst untuk melakukan serangan [18]. Nilai AE diformulasikan dengan rumus [18]:

$$\text{AE} = \frac{\sum bit\_berubah}{\sum bit\_total}\ x\ 100\% \quad (1)$$

2.7 UNIFIED AVERAGE CHANGING INTENSITY (UACI)

UACI merupakan tolok ukur standar rata-rata perbedaan intensitas diantara dua citra yang terenkripsi [2]. Menurut [19] nilai ideal untuk UACI masing-masing bernilai antara 33,25% dan 33,48%, dan perhitungannya bisa dilakukan dengan rumus [20] :

$$\text{UACI} = \frac{1}{W\ x\ H}\sum_{i,j}\frac{|\ C1(i,j)-C2(i,j)|}{255}\ x\ 100\% \quad (2)$$

di mana :
W = lebar citra
H = panjang citra
C1(i,j) = citra hasil1 (cipher-image1)
C2(i,j) = citra hasil2 (cipher-image2)

2.8 NUMBER OF PIXELS CHANGE RATE (NPCR)

Selain UACI, perhitungan yang paling umum digunakan untuk mengukur sensitivitas sistem kriptografi terhadap modifikasi kecil pada gambar biasa yaitu NPCR. NPCR menghitung perbandingan pada masing-masing piksel diantara dua citra yang terenkripsi dari citra asli yang sesuai jika terdapat perubahan pada kunci sebesar 1 bit [2]. Menurut [19] nilai ideal untuk NPCR lebih besar dari 99.6%, dan perhitungannya bisa dilakukan dengan rumus [20] :

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W\ x\ H}\ x\ 100\% \quad (3)$$

$$\text{D(i,j)} = \begin{cases} 0, C1(i,j) \neq C2(i,j) \\ 1, C1(i,j) = C2(i,j) \end{cases} \quad (4)$$

di mana :
W = lebar citra
H = panjang citra
D(i,j) = nilai dari kedua citra yang dibandingkan (0 atau 1)
C1(i,j) = citra hasil1 (cipher-image1)
C2(i,j) = citra hasil2 (cipher-image2)

2.9 MEAN SQUARE ERROR (MSE)

MSE merupakan salah satu kriteria yang menggunakan nilai-nilai random untuk menghitung estimasi dengan cara membandingkan perbedaan nilai piksel-piksel citra asli dengan citra yang terenkripsi pada letak piksel yang sama. Satuan nilai yang digunakan oleh MSE yaitu deciBell (dB). Nilai MSE harus lebih kecil dari PSNR, dan rumus untuk menghitung MSE sebagai berikut [2] :

$$\text{MSE} = \sum_{m=1}^{M}\sum_{n=1}^{N}[\ P(m,n) - P'(m,n)]^2 \quad (5)$$

dimana :
P(m,n) = citra asli berdimensi M x N

P'(m,n) = citra enkripsi

2.10 PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR diperoleh dari besar maupun kecil nilai MSE yang diperoleh dari suatu citra, semakin kecil nilai MSE maka semakin kecil nilai PSNRnya, begitu pula sebaliknya semakin besar nilai MSE maka semakin besar nilai PSNRnya dan semakin baik hasil yang diperoleh citra enkripsinya. Sama seperti MSE, satuan dari nilai PSNR yaitu deciBell (dB). Nilai PSNR yang terbaik yang diperoleh untuk kualitas citra enkripsi kurang dari 10 dB. Untuk menghitung PSNR, bisa melalui rumus dibawah ini [2] :

$$\text{PSNR} = 20 \text{ x } \log_{10} \left(\frac{255}{\sqrt{MSE}}\right) \quad (6)$$

2.11 KOEFISIEN CORELASI (CORRELATION COEFFISIENT)

Merupakan sebuah pengukuran statistik untuk menghitung seberapa kuat derajat korelasi diantara dua variabel yang terdiri dari citra asli dan citra terenkripsi agar bisa diketahui besarnya perbedaan dari masing-masing piksel dari dua variabel yang berdekatan [2]. Besarnya nilai koefisien korelasi untuk citra asli lebih mendekati 1, sedangkan untuk citra terenkripsi lebih mendekati 0 [21]. Koefesien korelasi diformulasikan dengan menggunakan rumus [21] :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (7)$$

3 METODE PENELITIAN

Penelitian ini bertujuan untuk mengetahui kinerja algoritma Arnold's Cat Map dan Henon Map pada citra yang berjenis homogen dan heterogen. Pada penelitian ini menggunakan 4 metode, yang pertama algoritma Arnold's Cat Map, kedua Henon Map, ketiga Arnold's Cat Map-Henon Map dan yang keempat Henon Map-Arnold's Cat Map. Sebagai perbandingan kinerja algoritma untuk mencari yang terbaik dari metode-metode tersebut, maka diukur dengan parameter uji berupa Avalanche Effect (AE), Unified Average Changing Intensity (UACI), Number of pixels Change Rate (NPCR), Mean Square Error (MSE), dan Peak Signal to Noise Ratio (PSNR) yang akan diimplementasikan menggunakan aplikasi Matlab R2019b.

3.1 TEKNIK PENGUMPULAN DATA

Data yang digunakan dalam penelitian ini merupakan data citra digital yang diambil dari direktori aplikasi Matlab R2019b dengan format BMP, TIFF, dan PNG saja, dengan citra yang berjenis homogen dan heterogen.

3.2 TEKNIK ANALISIS DATA

Teknik analisis data yang akan digunakan pada penelitian ini antara lain adalah citra uji yang akan digunakan adalah citra yang heterogen dan homogen berdimensi 201x201 piksel. Citra yang tidak sesuai dimensinya akan diresize sesuai dengan ukuran.

3.3 METODE YANG DIUSULKAN

Metode yang diusulkan dalam penelitian ini adalah metode Arnold's Cat Map dan Henon Map. Dalam penelitian ini dibagi menjadi 4 proses, yaitu metode Arnold's Cat Map digabungkan dengan Henon Map, lalu kebalikan dari proses pertama metode Henon Map digabungkan dengan Arnold's Cat Map, yang ketiga menggunakan metode Arnold's Cat Map saja, dan yang terakhir menggunakan metode Henon Map saja. Selanjutnya, masing-masing dari 4 proses tersebut di dalamnya ada 2 proses lagi yaitu proses enkripsi dan dekripsi yang merupakan unsur dalam kriptografi.

3.3.1 ARNOLD'S CAT MAP

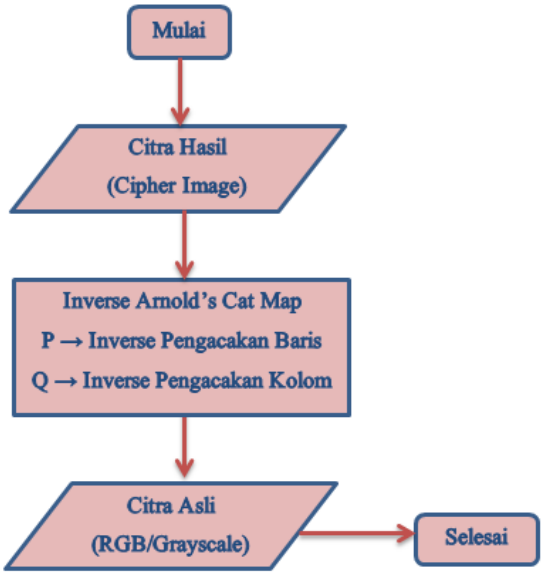
Pertama memilih citra yang akan di enkripsi pada menu yang telah disediakan yang di dalamnya sudah ada beberapa citra dengan format TIF, PNG, dan JPEG dan sudah diurutkan sesuai abjad, citra-citra tersebut ada yang grayscale dan ada juga yang RGB. Kemudian di lanjutkan dengan langkah berikut ini :

1. Pilih citra pada menu.
2. Dapatkan dimensi citra, jika dimensi citra M x N belum berbentuk persegi atau kotak (M=N), maka ubah ukurannya (resize) menjadi kotak.
3. Posisi piksel citra yang baru (sudah diresize) akan diacak oleh oleh algoritma Arnold's Cat Map dengan parameter P dan Q pada Arnold's Cat Map bernilai P = 3 dan Q = 1.
4. Citra terenkripsi (Cipher Image) sementara tersimpan.
5. Mencetak citra asli dan citra yang sudah terenkripsi.

Gambar 3 Diagram Alir Proses Enkripsi Arnold's Cat Map

Berikut proses dekripsi Arnold's Cat Map:

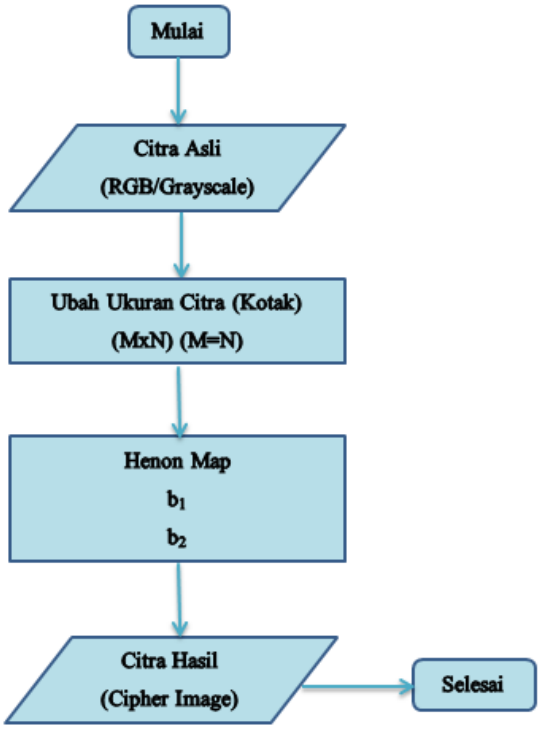
1. Citra enkripsi (Cipher Image) diambil sebagai input untuk Inverse Arnold's Cat Map. Dengan nilai parameter sama P = 3 dan Q = 1.
2. Setelah proses tersebut citra asli (plain image) akan dihasilkan kembali



Gambar 4 Diagram Alir Proses Dekripsi Cat Map

3.3.2 HENON MAP

Pertama memilih citra yang akan di enkripsi pada menu yang telah disediakan yang di dalamnya sudah ada beberapa citra dengan format TIF, PNG, dan JPEG dan sudah diurutkan sesuai abjad, citra-citra tersebut ada yang grayscale dan ada juga yang RGB. Kemudian di lanjutkan dengan langkah berikut ini :



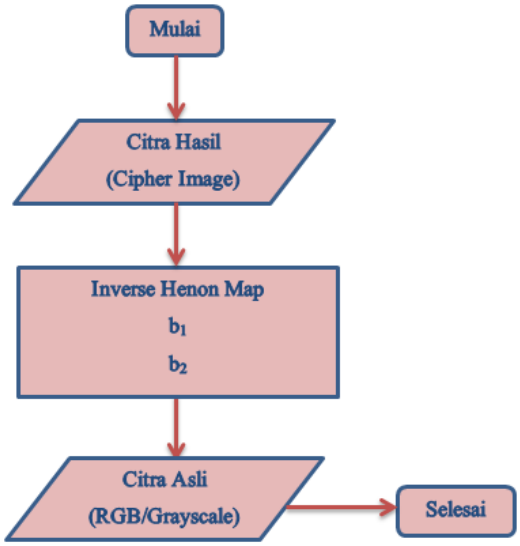
Gambar 5 Diagram Alir Proses Enkripsi Henon Map

1. Dapatkan dimensi citra, jika dimensi citra M x N belum berbentuk persegi atau kotak (M=N), maka ubah ukurannya (resize) menjadi kotak.
2. Posisi piksel citra yang baru (sudah diresize) akan diacak oleh oleh algoritma persaamaan Henon Map dengan memasukkan nilai b_1 dan b_2, nilai standar parameter pada Henon Map adalah b1 = 1.4 dan b2 = 0.3.
3. Citra terenkripsi (cipher image) sementara tersimpan.
4. Mencetak citra asli dan citra yang sudah terenkripsi.

Berikut proses dekripsi Henon Map:

1. Citra enkripsi (Cipher Image) diambil sebagai input Inverse Henon Map. Dengan nilai parameter sama b1 = 1.4 dan b2 = 0.3.
2. Setelah menjalani proses tersebut citra asli (plain image) akan dihasilkan kembali.

ISSN: 2086-4930
e-ISSN: 2777-0648



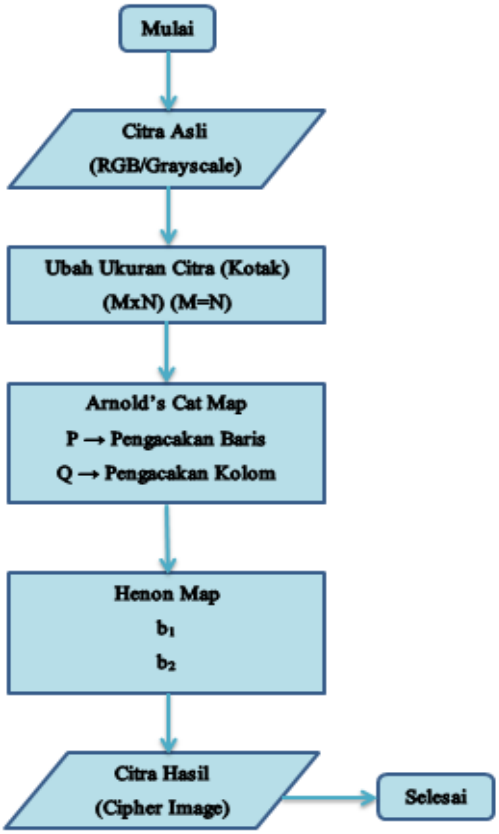
Gambar 6 Diagram Alir Proses Dekripsi Henon Map

3.3.3 ARNOLD'S CAT MAP DAN HENON MAP

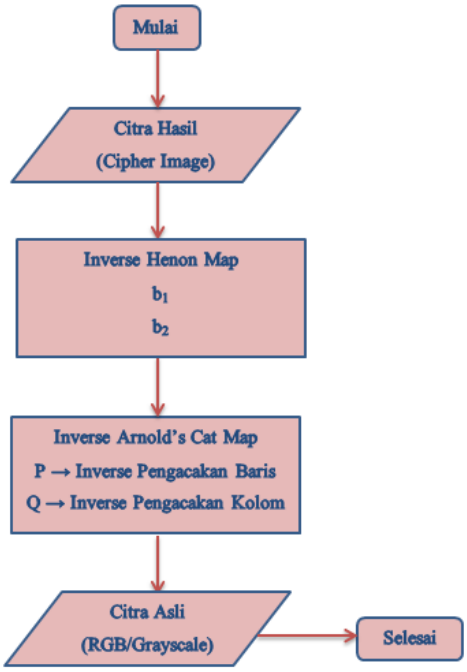
Pertama memilih citra yang akan di enkripsi pada menu yang telah disediakan yang di dalamnya sudah ada beberapa citra dengan format TIF, PNG, dan JPEG dan sudah diurutkan sesuai abjad, citra-citra tersebut ada yang grayscale dan ada juga yang RGB. Kemudian di lanjutkan dengan langkah berikut ini :

1. Pilih citra pada menu
2. Dapatkan dimensi citra, jika dimensi citra M x N belum berbentuk persegi atau kotak (M=N), maka ubah ukurannya (resize) menjadi kotak.
3. Posisi piksel citra yang baru (sudah diresize) akan diacak oleh oleh algoritma Arnold's Cat Map dengan parameter P dan Q pada Arnold's Cat Map bernilai P = 3 dan Q = 1.
4. Output dari Arnold's Cat Map diambil sebagai input untuk Henon Map yang selanjutnya mengacak gambar kembali menggunakan persaamaan Henon Map dengan memasukkan nilai b_1 dan b_2, nilai standar parameter pada Henon Map adalah $b_1 = 1.4$ dan $b_2 = 0.3$.
5. Citra terenkripsi (cipher image) sementara tersimpan.
6. Mencetak citra asli dan citra yang sudah terenkripsi.

ISSN: 2086-4930
e-ISSN: 2777-0648



Gambar 7 Diagram Alir Proses Enkripsi Arnold's Cat Map dan Henon Map



Gambar 8 Diagram Alir Proses Dekripsi Arnold's Cat Map dan Henon Map

Berikut proses dekripsi Arnold's Cat Map dan Henon Map:

1. Citra enkripsi (cipher image) diambil sebagai input Inverse Henon Map. Dengan nilai parameter sama $b_1 = 1.4$ dan $b_2 = 0.3$.

2. Citra hasil dari Inverse Henon Map diambil sebagai input untuk Inverse Arnold's Cat Map. Dengan nilai parameter sama P = 3 dan Q = 1.
3. Setelah menjalani kedua metode tersebut citra asli (plain image) akan dihasilkan kembali.

3.3.4 HENON MAP DAN ARNOLD'S CAT MAP

Pertama memilih citra yang akan di enkripsi pada menu yang telah disediakan yang di dalamnya sudah ada beberapa citra dengan format TIF, PNG, dan JPEG dan sudah diurutkan sesuai abjad, citra-citra tersebut ada yang grayscale dan ada juga yang RGB. Kemudian di lanjutkan dengan langkah berikut ini :

1. Pilih citra pada menu
2. Dapatkan dimensi citra, jika dimensi citra M x N belum berbentuk persegi atau kotak (M=N), maka ubah ukurannya (resize) menjadi kotak.
3. Posisi piksel citra yang baru (sudah diresize) akan diacak oleh oleh algoritma persaamaan Henon Map dengan memasukkan nilai b_1 dan b_2, nilai standar parameter pada Henon Map adalah b1 = 1.4 dan b2 = 0.3.
4. Output dari Henon Map diambil sebagai input untuk Arnold's Cat Map yang selanjutnya mengacak gambar kembali menggunakan persaamaan Arnold's Cat Map dengan parameter P dan Q pada Arnold's Cat Map bernilai P = 3 dan Q = 1.
5. Citra terenkripsi (cipher image) sementara tersimpan.
6. Mencetak citra asli dan citra yang sudah terenkripsi.

Gambar 9 Diagram Alir Proses Enkripsi Henon Map dan Arnold's Cat Map

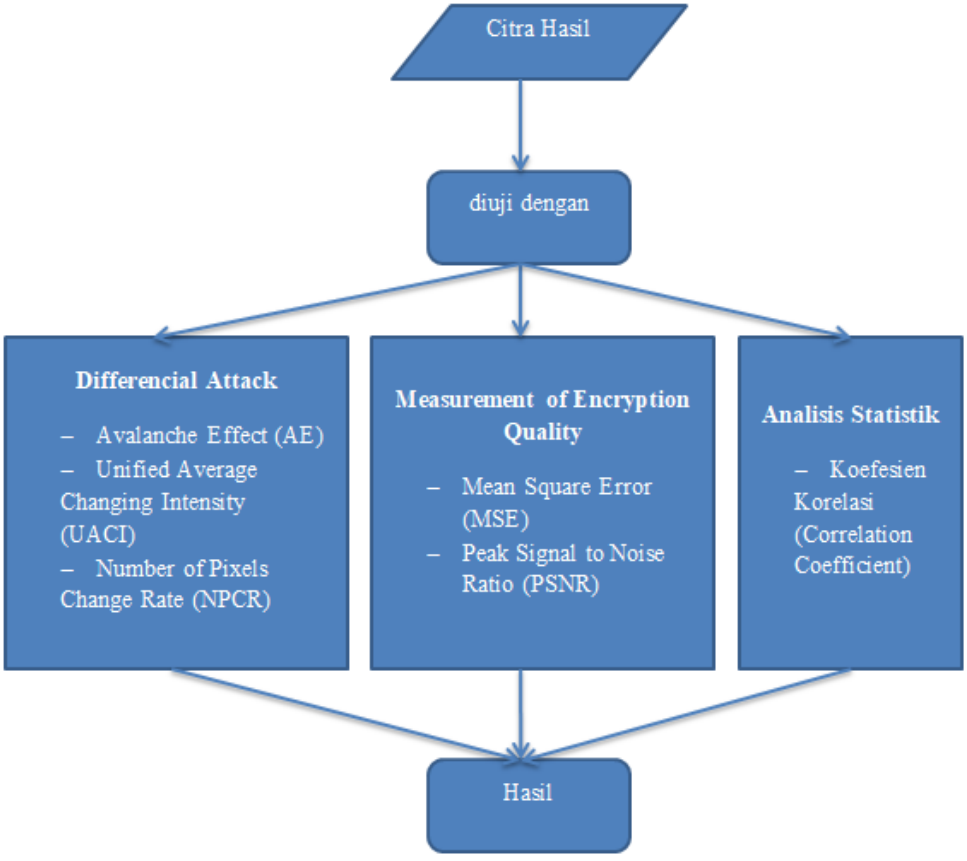
Berikut proses dekripsi Henon Map dan Arnold's Cat Map:

1. Citra enkripsi (cipher image) diambil sebagai input Inverse Arnold's Cat Map. Dengan nilai parameter sama P = 3 dan Q = 1.
2. Citra hasil dari Inverse Henon Map diambil sebagai input untuk Inverse Henon Map. Dengan nilai parameter sama b_1 = 1.4 dan b_2 = 0.3.

ISSN: 2086-4930
e-ISSN: 2777-0648

3. Setelah menjalani kedua metode tersebut citra asli (plain image) akan dihasilkan kembali.

Gambar 10 Diagram Alir Proses Dekripsi Henon Map dan Arnold's Cat Map



Gambar 11 Diagram Alir Proses Pengujian Citra

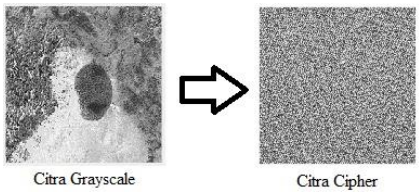
3.4 CARA PENGUJIAN METODE

Pengujian metode dilakukan dengan menggunakan beberapa parameter uji yang biasa digunakan dalam pengujian metode dalam teknik kriptografi yaitu pengukuran nilai differential attack untuk pengukuran error citra yang diuji menggunakan nilai Avalanche Effect (AE), Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), kemudian nilai measurement of encryption quality untuk pengukuran kualitas citra yang diuji dengan nilai Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) , serta analisis statistik yang akan mengukur nilai Koefesien Korelasi (Correlation Coefficient).

4 HASIL DAN PEMBAHASAN

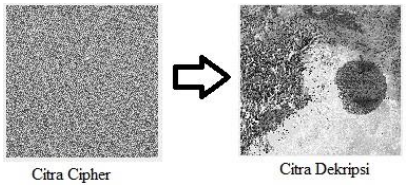
4.1 HASIL ALGORITMA ARNOLD'S CAT MAP

Pada langkah ini menjelaskan proses enkripsi dan dekripsi dari algoritma Arnold Cat Map. Citra di enkripsi menggunakan algoritma Arnold Cat Map yang menghasilkan citra cipher. Berikut hasil enkripsi dari algoritma Arnold's Cat Map.



Gambar 12 Hasil Enkripsi Arnold Cat Map

Pada Gambar 4.1 ditunjukan citra grayscale yang telah di enkripsi menggunakan algoritma Arnold Cat Map. Dekripsi menggunakan citra cipher untuk mengembalikan citra menjadi grayscale input. Proses dekripsi dilakukan dengan mengembalikan nilai pixel ke posisi semula.

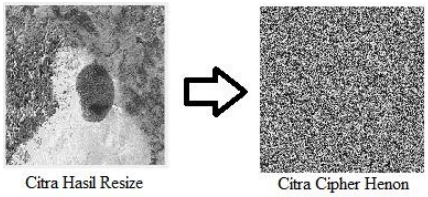


Gambar 13 Hasil Dekripsi

Pada gambar 4.2 ditunjukan citra cipher dan citra dekripsi setelah melalui proses dekripsi. Citra hasil dekripsi merupakan citra grayscale yang posisi pixelnya dikembalikan seperti semula.

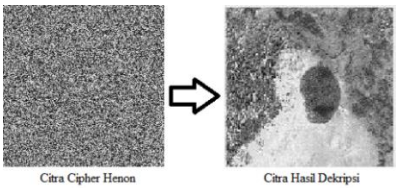
4.2 HASIL ALGORITMA HENON MAP

Pada langkah ini menjelaskan proses enkripsi dan dekripsi dari Henon Map. Citra di enkripsi menggunakan algoritma Henon Map yang menghasilkan citra cipher.



Gambar 14 Hasil Enkripsi Henon Map

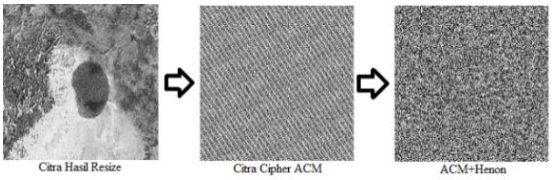
Dekripsi menggunakan citra cipher untuk mengembalikan citra menjadi grayscale input. Proses dekripsi dilakukan dengan mengembalikan nilai pixel ke posisi semula.



Gambar 15 Hasil Dekripsi Henon Map

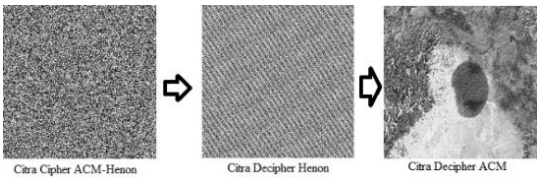
4.3 HASIL ALGORITMA ARNOLD'S CAT MAP DAN HENON MAP

Pada langkah ini menjelaskan proses enkripsi dan dekripsi dari Arnold Cat Map dengan kombinasi Henon Map. Citra di enkripsi menggunakan algoritma Arnold Cat Map kemudian di enkripsi lagi menggunakan Henon Map yang menghasilkan citra cipher.



Gambar 16 Hasil Enkripsi ACM - Henon Map

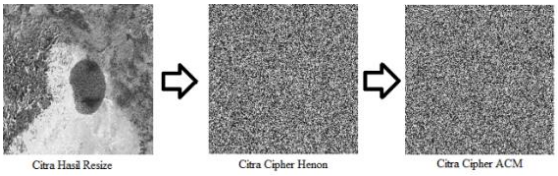
Dekripsi menggunakan citra cipher hasil enkripsi algoritma ACM-Henon untuk mengembalikan citra menjadi grayscale input. Proses dekripsi dilakukan dengan mengembalikan nilai pixel ke posisi semula. Dekripsi dimulai dengan mendekripsi citra cipher menggunakan algoritma Henon Map kemudian dilanjutkan dengan Arnold Cat Map.



Gambar 17 Citra Dekripsi ACM-Henon Map

4.4 HASIL ALGORITMA HENON MAP DAN ARNOLD'S CAT MAP

Pada langkah ini menjelaskan proses enkripsi dan dekripsi dari Henon Map dan kombinasi Arnold Cat Map. Citra di enkripsi menggunakan algoritma Henon Map yang menghasilkan citra cipher kemudian dilanjutkan enkripsi menggunakan Arnold Cat Map.



Gambar 18 Citra Enkripsi Henon-ACM

Dekripsi menggunakan citra cipher hasil enkripsi algoritma Henon-ACM untuk mengembalikan citra menjadi grayscale input. Proses dekripsi dilakukan dengan mengembalikan nilai pixel ke posisi semula. Dekripsi dimulai dengan mendekripsi citra cipher menggunakan algoritma Arnold Cat Map kemudian dilanjutkan dengan Henon Map.

Gambar 19 Citra Dekripsi Henon ACM

4.5 HASIL PENGUJIAN DAN EVALUASI CORRELATION COEFFICIENT

Pengujian koefisien korelasi dilakukan dengan mengambil piksel-piksel citra yang berdekatan secara berpasangan. Distribusi korelasi dari piksel-piksel yang berdekatan pada citra asli dan citra cipher masing-masing diuji pada posisi piksel secara horisontal, vertikal dan diagonal. Hasil pengujian correlation coefficient citra dapat dilihat pada tabel 4.1

Tabel 1 Perbandingan Hasil

Algoritma	Diagonal	Vertical	Horizontal	Rata-rata
Original	0.83744	0.89868	0.89431	0.87681
ACM	0.41255	0.69972	0.49969	0.53732
Henon Map	-0.00126	-0.0022	0.00338	-0.00004
ACM+Henon Map	0.00087	-0.0058	0.00060	-0.00147
Henon+ACM	0.00179	0.00152	0.00012	0.00114

4.6 HASIL PENGUJIAN DAN EVALUASI DIFFERENTIAL ATTACK

Differential attack didasarkan pada pengukuran error citra yang diuji. Terdapat tiga jenis parameter pada differential attack pada penelitian ini yaitu Mean Absolute Error (MAE), Number of Pixels Change Rate (NPCR) dan Unified Average Changing Intensity (UACI).

Tabel 2 Perbandingan Differential Attack

Algoritma	NPCR	UACI	MAE
ACM	0.75213	0.17103	43.61257
Henon Map	0.99624	0.35672	90.96282
ACM+Henon	0.99624	0.35672	90.96282
Henon+ACM	0.99622	0.35658	90.92709

4.7 HASIL PENGUJIAN DAN EVALUASI MEASUREMENT OF ENCRIPTION QUALITY

Kriteria penilaian pengukuran kualitas enkripsi didasarkan pada pengukuran kualitas citra yang diuji. Hasil pengujian Encryption Qualiti menggunakan PSNR ditunjukan pada tabel 4.3

Tabel 3 Rata-Rata Nilai PSNR

ACM	Henon Map	ACM + Henon Map	Henon Map + ACM
13.2660	7.6360	7.6452	7.6400

5 KESIMPULAN

Berdasarkan hasil penelitian tentang implementasi Kriptografi Citra Menggunakan Algoritma Arnold's Cat Map Dan Henon Map didapatkan hasil penelitian yaitu enkripsi Arnold Cat Map memiliki nilai korelasi yang tinggi sehingga dibandingkan dengan algoritma lain memiliki tingkat reduksi citra yang rendah. Sedangkan pengujian Henon Map, ACM+Henon Map, Henon Map + ACM memiliki nilai korelasi yang mendekati 0 yang artinya algoritma yang diusulkan tersebut berhasil mereduksi citra yang berdekatan. Differential Attach yang terdiri dari NPCR, UACI dan MAE algoritma enkripsi ACM memiliki nilai yang lebih kecil dibanding dengan Henon Map, ACM-Henon dan Henon ACM, hal tersebut menunjukan algoritma enkripsi ACM masih mendekati citra asli sedangkan citra cipher algoritma Henon Map, ACM-Henon dan Henon ACM semakin berbeda dengan citra asli. Citra cipher ACM memiliki nilai PSNR lebih rendah dibanding citra cipher Henon Map, ACM-Henon dan Henon ACM. Hal tersebut menunjukan citra cipher ACM lebih lemah terhadap serangan dibanding citra cipher Henon Map, ACM-Henon dan Henon ACM.

DAFTAR PUSTAKA

[1] A. Syahputra, I. Algoritma, and F. Untuk, "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video," vol. 10, pp. 70–77, 2021.

[2] R. B. Fernandez *et al.*, "PENGGUNAAN METODE HENON MAP DAN CHAOS LOGISTIC MAP (CLM) DALAM ENKRIPSI CITRA DIGITAL 24-BIT," vol. 5, no. 1, pp. 52–70, 2017.

[3] R. Sujarani and D. Manivannan, "Available Online through Research Article," *Ijrap.Net*, vol. 4, no. 1, pp. 4060–4066, 2016.

[4] P. S. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 3, pp. 1289–1308, 2020, doi: 10.1007/s12652-019-01385-0.

[5] D. Elmaci and N. Bas Catak, "An Efficient Image Encryption Algorithm for the Period of Arnold ' s CAT Map," vol. 2, no. 2, 2018.

[6] P. Sankhe, S. Pimple, S. Singh, A. Lahane, S. V. Sem, and C. Engg, "An Image Cryptography using Henon Map and Arnold Cat Map .," pp. 1900–1904, 2018.

[7] A. Afifi, "A Chaotic Confusion-Diffusion Image Encryption Based on Henon Map," *Int. J. Netw. Secur. Its Appl.*, vol. 11, no. 4, pp. 19–30, 2019, doi: 10.5121/ijnsa.2019.11402.

[8] T. Anna, M. A. I. Pakereng, and Y. R. Beeh, "Implementasi Algoritma Chaos-Based Feedback Stream Cipher pada Enkripsi-Dekripsi Data Citra Digital," *J. Inform.*, vol. 5, no. 2, pp. 151–169, 2009.

[9] R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, "Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map," *Proc. 2018 Int. Conf. Curr. Trends Towar. Converging Technol. ICCTCT 2018*, pp. 1–5, 2018, doi: 10.1109/ICCTCT.2018.8551137.

[10] A. Susanto, "Penerapan Teori Chaos di dalam Kriptografi," 2008.
[11] M. W. Habiby and D. Lestari, "Cryptography System for Information Security Using Chaos Arnold ' s Cat Map Function," pp. 61–66, 2017.
[12] W. J. Hadiman, J. Tjandra, and I. Fadillah, "W.J Hadiman 1 , J Tjandra 1 , I Fadillah 1 1," pp. 1–6, 2020.
[13] Suhardi, "APLIKASI KRIPTOGRAFI DATA SEDERHANA DENGAN METODE EXLUSIVE-OR (XOR)," vol. 03, pp. 23–31, 2016.
[14] C. Solomon and T. Breckon, *Fundamentals of Digital Image Processing*. 2011.
[15] A. S. Bader, S. Hameed, and M. A. A. K., "Key Generation based on Henon map and Lorenz system," *Al-Mustansiriyah J. Sci.*, vol. 31, no. 1, p. 41, 2020, doi: 10.23851/mjs.v31i1.734.
[16] N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egypt. Informatics J.*, vol. 17, no. 1, pp. 139–146, 2016, doi: 10.1016/j.eij.2015.10.001.
[17] A. Bostan, M. Karakaya, and G. Şengül, "CHAOS- BASED DATA ENCRYPTION USING ARNOLD ' S CAT MAP," vol. 4, no. 1, pp. 25–30, 2018.
[18] N. R. D. P. Astuti, I. Arfiani, and E. Aribowo, "Analysis of the security level of modified CBC algorithm cryptography using avalanche effect Analysis of the security level of modified CBC algorithm cryptography using avalanche effect," pp. 2–10, 2019, doi: 10.1088/1757-899X/674/1/012056.
[19] S. A. Mehdi and Z. L. Ali, "Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper- Chaotic System," *Al-Mustansiriyah J. Sci.*, vol. 31, no. 1, p. 54, 2020, doi: 10.23851/mjs.v31i1.739.
[20] S. Muhajer, A. Monem, and S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," *J. Inf. Secur. Appl.*, vol. 50, p. 102410, 2020, doi: 10.1016/j.jisa.2019.102410.
[21] R. Munir, "Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map," vol. 1, pp. 166–181, 2012.