Aplikasi Algoritma Arnold Cat Map dalam Enkripsi Gambar Digital

Rika Dewi, 13517147
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517147@std.stei.itb.ac.id

***Abstrak*—Teknologi mempermudah proses pertukaran informasi termasuk gambar digital. Isu keamanan pun muncul sebagai konsekuensi atas hal ini. Oleh karena itu berkembang cara untuk mengenkripsi data berupa gambar digital, salah satunya dengan menggunakan algoritma Arnold Cat Map. Proses enkripsi ini mengacak susunan tiap *pixel* pada gambar digital tanpa mengubah atau menghilangkan nilai dari *pixel* tersebut.**

***Kata Kunci*—Arnold Cat Map, enkripsi, dekripsi, *pixel*.**

I. PENDAHULUAN

Peradaban manusia kini telah memasuki era globalisasi. Pertukaran informasi terjadi sangat cepat dan tidak terbatas oleh jarak. Teknologi yang mendukung hal ini adalah internet. Hampir semua orang memiliki akses terhadap setiap informasi melalui internet.

Data menjadi sesuatu yang tidak bisa dibendung lagi. Akses terhadap tulisan, gambar, atau media lainnya menjadi susah untuk dikontrol. Hal ini menyebabkan muncul isu tentang kerahasiaan dan privasi dari data itu sendiri, tidak terkecuali pada gambar digital.

Kriptografi adalah salah satu bidang yang bergerak untuk menyelesaikan isu ini. Kriptografi sendiri memiliki dua proses utama yaitu enkripsi dan dekripsi. Enkripsi yaitu proses mengubah data menjadi tidak dikenali oleh orang lain yang tidak terotorisasi. Dekripsi yaitu proses untuk mengembalikan data ke keadaan sebelum dienkripsi.

Berbagai teknik kriptografi kini semakin berkembang, terutama untuk mengenkripsi data berupa tulisan. Sedangkan untuk gambar digital, tidak banyak teknik kriptografi yang dapat mengenkripsinya secara efisien. Beberapa algoritma untuk mengenkripsi data tulisan tidak bisa digunakan begitu saja untuk mengenkripsi gambar digital.

Salah satu metode yang diperkenalkan dalam kriptografi adalah teknik *chaos*. Banyak orang mendefinisikan *chaos* sebagai sekedar acak-acakan belaka. Namun teori *chaos* mendefinisikan *chaos* sebagai sebuah keacakan yang sebenarnya dapat diprediksi. Sebuah algoritma yang mengadopsi teknik *chaos* ini yaitu Arnold Cat Map.

Arnold Cat Map adalah sebuah algoritma yang diciptakan sebagai metode untuk mengacak susunan *pixel* pada sebuah gambar. Namanya didapatkan dari penggunaan gambar kucing pada saat teknik ini dipublikasi pertama kali oleh penemunya. Keunggulan dari algoritma Arnold Cat Map adalah setiap *pixel* yang dihasilkan dari algoritma ini nilainya tidak berubah, sehingga tidak jarang orang menggunakan teknik ini untuk mengenkripsi sebuah gambar.

II. TEORI DASAR

A. Bilangan bulat

Bilangan bulat adalah himpunan bilangan yang dituliskan tanpa komponen desimal atau pecahannya. Bilangan bulat terdiri dari bilangan positif, negatif, dan nol. Dalam matematika, bilangan bulat seringkali dilambangkan dalam huruf **Z**.

Himpunan bilangan bulat ini tertutup pada operasi penjumlahan dan perkalian. Hal ini berarti jika dua buah bilangan bulat dijumlahkan akan menghasilkan bilangan bulat. Begitu pula kedua bilangan bulat yang dikalikan akan menghasilkan bilangan bulat sebagai hasilnya juga. Sedangkan untuk pembagian, kedua bilangan bulat yang dibagi belum tentu memunculkan bilangan bulat sebagai hasilnya.

Misalkan a dan b adalah bilangan bulat dengan $a \neq 0$. Sifat pembagian bilangan bulat yaitu menghasilkan bilangan bulat jika a habis membagi b, dan tidak menghasilkan bilangan bulat jika a tidak habis membagi b. a dikatakan habis membagi b, jika terdapat bilangan bulat c sehingga b = ac. Habis membagi dinotasi sebagai berikut

$$a \mid b, \qquad b = ac, c \in \boldsymbol{Z}, a \neq 0 \tag{1}$$

B. Algoritma Eucledian

Algoritma Eucledian adalah algoritma untuk mencari *Greatest Common Divisor* (GCD) atau Faktor Persekutuan Terbesar (FPB) dari dua buah bilangan bulat. Misal a dan b bilangan bulat. FPB dari a dan b adalah bilangan bulat terbesar d sehingga d | a dan d | b.

Teorema Eucledian menyatakan bahwa jika ada bilangan bulat m dan n, dengan n > 0, maka terdapat bilangan bulat unik q (*quotient*) dan r (*remainder*) yang dapat dituliskan sebagai

$$m = nq + r, \qquad 0 \leq r < n \tag{2}$$

Menurut Teorema Eucledian, PBB(m,n) = PBB(n,r) dan PBB(r,0) = r. Dengan sifat tersebut, penerapan algoritma Eucledian berulang dapat menghasilkan PBB dari dua bilangan.

Misalkan akan dicari PBB dari 36 dan 28 dengan menggunakan algoritma Eucledian. Langkah-langkah untuk mendapatkan PBB dari 36 dan 28 adalah sebagai berikut

$$36 = 28\,(1) + 8$$
$$28 = 8\,(3) + 4$$
$$8 = 4\,(2) + 0$$

Dengan memanfaatkan Teorema Eucledian didapatkan bahwa PBB(36,28) = PBB (4,0) = 4.

C. Aritmatika Modulo

Aritmatika modulo adalah operasi bilangan yang menghasilkan sisa hasil bagi dua buah bilangan. Misalkan a dan m adalah bilangan bulat, maka operasi modulo dapat dinotasikan sebagai a mod m = r, sedemikian sehingga

$$a = km + r, \qquad 0 \le r < m, k \in \boldsymbol{Z} \tag{3}$$

m disebut sebagai modulo atau modulus dengan hasil dari operasi modulo ini terletak di antara himpunan {0,1,2, … , m-1}.

Dua buah bilangan bulat positif a dan b merupakan kongruen modulo dari bilangan bulat positif m, jika m | (a-b). Kekongruenan ini dinotasikan sebagai berikut

$$a \equiv b\ (mod\ m)$$

Inverse modulo atau balikan modulo adalah bilangan bulat x yang memenuhi persamaan

$$xa \equiv 1\ (mod\ m)$$

Inverse modulo dinotasikan sebagai

$$a^{-1}(mod\ m) = x$$

Jika a dan m relatif prima dan m > 1, maka balikan (*inverse*) dari a (mod m) dipastikan ada.

D. Transformasi Matriks Dua Dimensi

Transformasi digunakan untuk memindahkan titik pada suatu bidang. Transformasi geometri adalah proses yang membahas tentang perubahan secara geometri, baik perubahan letak, bentuk, dan penyajiannya berdasarkan gambar dan matriks. Misalkan sebuah titik (x,y) ditransformasi T menjadi (x', y'). Matriks yang bersesuian dengan transformasi T adalah matriks yang memenuhi persamaan berikut

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Transformasi pada bidang dapat dibagi menjadi beberapa jenis yaitu translasi, refleksi, rotasi, dilatasi, peregangan, dan gusuran (*shear*). Translasi (pergeseran) merupakan perubahan objek dengan cara menggeser dari satu posisi ke posisi lainnya pada jarak tertentu. Matriks transformasi dari pergeseran sumbu x sejauh a dan pergesaran sumbu y sejauh b yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix}$$

Refleksi (pencerminan) merupakan hasil bayangan benda yang terbentuk dari sebuah cermin tertentu. Matriks transformasi untuk refleksi ini bervariasi tergantung dari titik acuan pencerminan yang digunakan. Salah satu contohnya yaitu matriks transformasi untuk pencerminan terhadap titik pusat O yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Rotasi (perputaran) merupakan perubahan kedudukan objek dengan cara diputar melalui pusat dan sudut tertentu. Besarnya sudut rotasi disepakati bernilai positif untuk arah berlawanan jarum jam. Matriks transformasi dengan titik pusat O sejauh θ yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Dilatasi adalah pembesaran atau pengecilan suatu objek. Matriks transformasi dengan titik pusat O dan faktor skala k yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Regangan (*stretch*) adalah pembesaran atau pengecilan pada salah satu absis atau ordinat saja. Matriks transformasi peregangan pada arah sumbu x (kiri) dan arah sumbu y (kanan) dengan titik pusat O dan faktor skala k yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \qquad \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & k \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

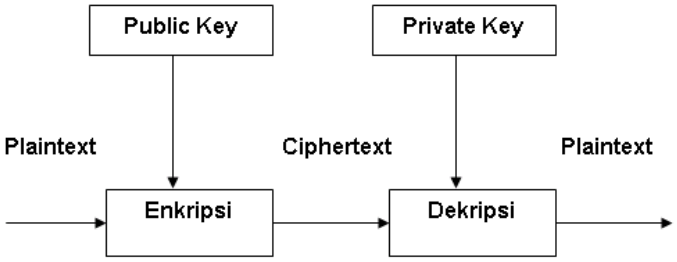
Gusuran (*shear*) adalah pergeseran terhadap dua arah saling berlawanan yang bergantung pada salah satu sumbu saja. Matriks transformasi *shear* pada arah sumbu x (kiri) dan arah sumbu y (kanan) dengan titik pusat O dan faktor skala k yaitu

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \qquad \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

E. Kriptografi

Kata kriptografi berasal dari Bahasa Yunani yaitu *crypto* dan *graphia*. Crypto berarti rahasia (*secret*) dan graphia berarti tulisan (*writing*). Jadi kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain. Menurut Bruce Schneier, kriptografi dapat diartikan pula sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data. Orang yang melakukan enkripsi terhadap suatu pesan atau praktisi kriptografi disebut *cryptographer*.

Sebuah pesan yang tidak disandikan atau dienkripsi disebut sebagai *plaintext* atau *cleartext*. Sedangkan pesan yang telah disandikan dengan algoritma kriptografi disebut *chipertext*. Proses mengubah *plaintext* ke *chipertext* disebut *encryption* atau enkripsi. Sedangkan proses mengubah *chipertext* ke *plaintext* disebut *decryption* atau dekripsi. Proses enkripsi dan dekripsi dapat dilihat pada Gambar 1.



Gambar 1. Terminologi Enkripsi dan Dekripsi
Sumber:
http://meditaruk.blogspot.com/2015/01/kriptografi.html

III. PEMBAHASAN ARNOLD CAT MAP

A. Teori Chaos

Teori *chaos* adalah cabang matematika yang mendeskripsikan perilaku dari suatu fenomena yang terlihat acak dan tidak terprediksi. Teori *chaos* sering kali digunakan untuk memprediksi perilaku dari sebuah sistem dinamis berdasarkan kondisi awalnya. Kondisi awal adalah faktor yang penting dalam teori *chaos*.

Sistem dinamis adalah sistem yang terdiri atas konfigurasi titik-titik yang berubah tiap waktunya. Sebuah sistem dinamis dikatakan berada dalam kondisi *chaos* jika memenuhi karakteristik berikut:

1. bergantung pada kondisi awal,
2. bersifat acak secara topologi, dan
3. memiliki pola periodik.

Sifat pertama yaitu bergantung pada kondisi awal berarti setiap titik pada sistem saling bergantung satu sama lain dalam menentukan perilakunya. Oleh karena itu perubahan kecil terhadap kondisi awal dapat menghasilkan perilaku yang berbeda.

Sifat kedua yaitu acak secara topologi berarti sistem selalu berubah setiap waktu sehingga akan terdapat saat di mana daerah-daerah dalam sistem saling tumpang tindih satu sama lain.

Sifat ketiga yaitu memiliki pola periodik merupakan sifat yang membuat suatu sistem dinamis yang terlihat acak dapat diprediksi. Setiap titik pada sistem akan bergerak secara acak namun mengerucut pada sebuah pola yang perodik.

B. Algoritma Arnold Cat Map

Arnold Cat Map adalah sebuah algoritma pemetaan sekumpulan titik dengan menerapkan prinsip dari teori *chaos*. Algoritma Arnold Cat Map merupakan transformasi dari R^2 ke R^2. Misalkan setiap titik (x,y) ∈ R^2 berada pada ruang S.

$$T: (x, y) \rightarrow (x + y, x + 2y) \; mod \; 1$$

atau dalam notasi matriks,

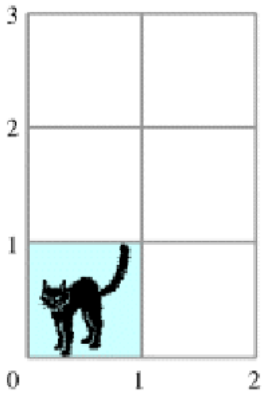
$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \; mod \; 1 \tag{4}$$

Persamaan (4) dapat dituliskan sebagai berikut agar lebih mudah dipahami secara geometri

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \; mod \; 1 \tag{5}$$

Persamaan (5) memperlihatkan bahwa algoritma Arnold Cat Map merupakan komposisi dari transformasi *shear* arah x dengan faktor 1 kemudian dilanjutkan dengan transformasi *shear* arah y dengan faktor 1. Hasil dari transformasi ini kemudian dioperasikan dengan mod 1, sehingga setiap titik (x,y) akan terpetakan kembali pada ruang S.

Algoritma ini akan diilustrasikan dengan menggunakan gambar digital yang dapat dilihat pada Gambar 2. Secara garis besar, algoritma Arnold Cat Map ini dapat dijabarkan menjadi tiga langkah.

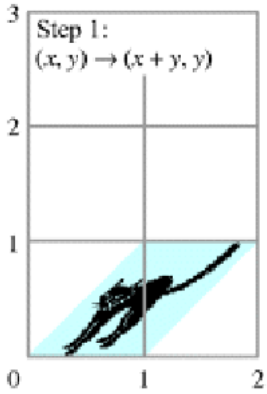


Gambar 2. Ilustrasi Kucing sebelum Ditransformasi [2]

Langkah pertama yaitu transformasi *shear* arah x dengan faktor 1. Matriks transformasinya dapat didefinisikan sebagai berikut

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Pasangan (x,y) merupakan setiap titik pada gambar digital di Gambar 2., sedangkan (x',y') merupakan setiap titik hasil transformasi *shear* dengan arah sumbu x yang terlihat pada Gambar 3.

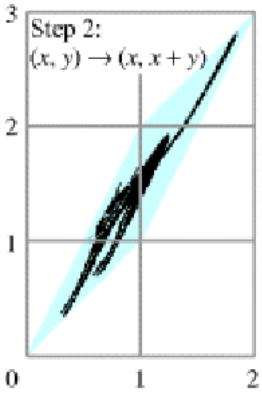


Gambar 3. Ilustrasi Kucing setelah Ditransformasi *Shear* Arah x [2]

Langkah kedua yaitu transformasi *shear* arah y dengan faktor 1. Matriks transformasinya dapat didefinisikan sebagai berikut

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Pasangan (x,y) merupakan setiap titik pada gambar digital di Gambar 3., sedangkan (x',y') merupakan setiap titik hasil transformasi *shear* dengan arah sumbu y yang terlihat pada Gambar 4.

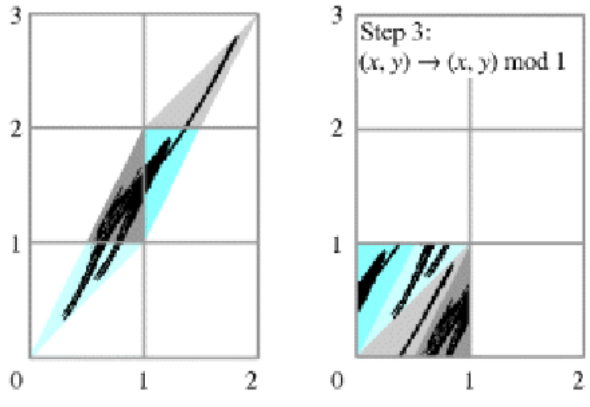


Gambar 4. Ilustrasi Kucing setelah Ditransformasi *Shear* Arah y [2]

Langkah terakhir yaitu menerapkan operasi modulo terhadap setiap titik. Dengan rumus sebagai berikut

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ 1$$

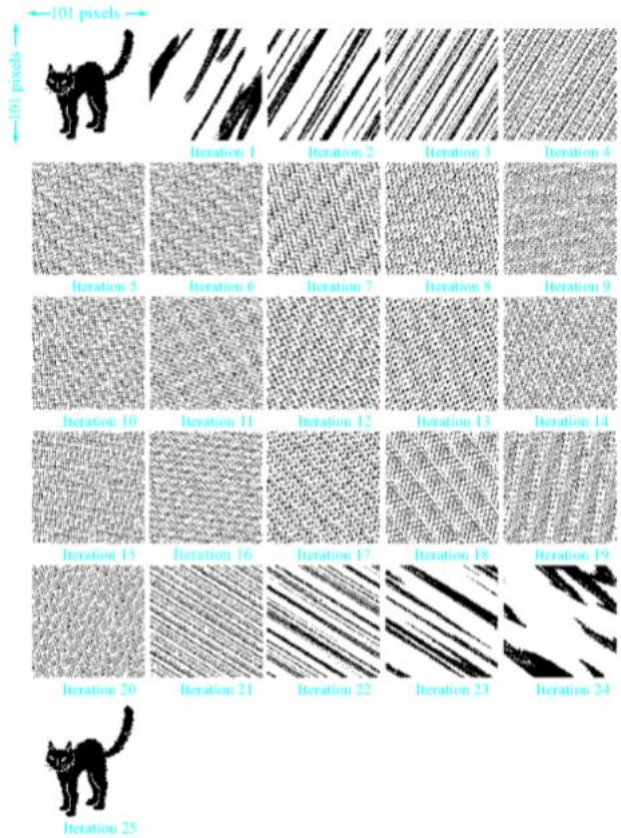
Pasangan (x,y) merupakan setiap titik pada gambar digital di Gambar 5(a)., sedangkan (x',y') merupakan setiap titik hasil pengaplikasian operasi modulo yang terlihat pada Gambar 5(b). Perhatikan bahwa pada Gambar 5(a). sengaja digunakan perbedaan warna pada setiap bidang. Hal ini bermaksud untuk menonjolkan proses penyusunan setiap titik pada gambar digital akibat pengaplikasian opeasi modulo yang tidak mengubah atau menghapus tiap titik pada gambar digital. Data yang terdapat pada Gambar 2. masih sama dengan data pada Gambar 5(b) yang telah dienkripsi menggunakan algoritma Arnold Cat Map. Yang berbeda hanyalah posisi penyusunan tiap titik pada gambar digital.



Gambar 5(a). Ilustrasi Kucing sebelum Diaplikasikan Operasi Modulo (kiri) dan Gambar 5(b). Ilustrasi Kucing sebelum Diaplikasikan Operasi Modulo (kanan) [2]

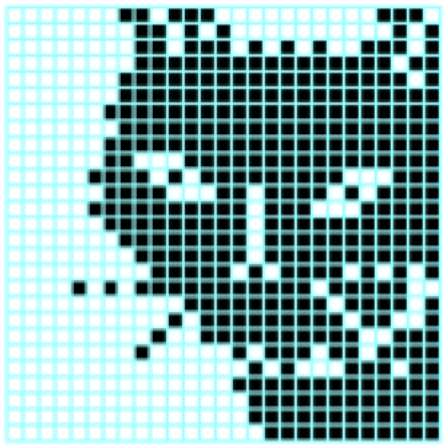
C. Periode

Gambar 5(b) adalah hasil dari sebuah ilustrasi setelah diaplikasikan algoritma Arnold Cat Map sebanyak satu kali. Apabila diperhatikan secara saksama, gambar yang dihasilkan masih dapat dikenali sehingga satu kali pengaplikasian algoritma Arnold Cat Map tidaklah cukup untuk menjamin keamanan dari data kita. Oleh karena itu penerapan dari algoritma Arnold Cat Map ini biasanya dilakukan dalam sejumlah iterasi tertentu.



Gambar 6. Iterasi Pengaplikasian Algorima Arnold Cat Map [2]

Dari Gambar 6. terlihat hal menarik yang terjadi setelah beberapa kali diaplikasikan algoritma Arnold Cat Map. Perhatian bahwa pada iterasi ke-25, gambar yang dihasilkan dari proses enkripsi kembali ke gambar semula. Kejadian ini dapat dijelaskan dengan memandang gambar digital sebagai kumpulan titik-titik diskrit yang disebut sebagai *pixel*. Ilustrasi yang digunakan pada Gambar 6. terdiri atas 101x101 *pixel*. Contoh penggambaran gambar digital sebagai *pixel* dapat dilihat pada Gambar 7.



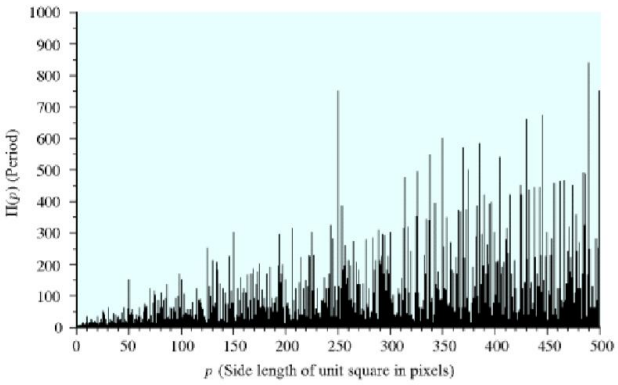
Gambar 7. *Pixel* pada Gambar Digital [2]

Setiap pixel pada gambar digital akan memiliki koordinat posisi tersendiri yang unik dan berbeda satu sama lain. Misalkan sebuah gambar digital memiliki ukuran p x p *pixel* dan terletak

pada daerah S. Setiap *pixel* akan memiliki koordinat (m / p, n / p) dengan m dan n terletak di antara himpunan bilangan bulat {0, 1, 2, … , p - 1}.

Dengan menggunakan matriks transformasi (5), pasangan koordinat (m / p, n / p) akan menghasilkan koordinat (m' / p, n' / p) dengan m' dan n' tetap berada di antara himpunan bilangan bulat {0, 1, 2, … , p - 1}. Hal ini karena algoritma Arnold Cat Map akan mentransformasikan setiap *pixel* pada daerah S ke dalam daerah S pula. Dan karena hanya terdapat p^2 pixel pada daerah S, maka setiap pixel akan kembali ke titik semula setelah maksimum p^2 iterasi dilakukan. Jumlah iterasi yang dibutuhkan untuk sebuah *pixel* kembali ke titiknya yang semula didefinisikan sebagai periode.

Setiap *pixel* pada gambar digital akan memiliki periodenya masing-masing yang unik bergantung pada koordinat awal *pixel* dan ukuran dari gambar digital. Kelipatan Persekutuan Terkecil (KPK) atau *Least Common Multiple* (LCM) dari periode setiap *pixel* pada sebuah gambar digital akan menghasilkan periode dari gambar digital tersebut secara keseluruhan. KPK dari bilangan bulat a dan b dapat dihitung dengan mengkalikan a dan b kemudian membagi hasilnya dengan FPB (a,b). Perhitungan nilai FBP sendiri dapat menggunakan algoritma Eucledian pada persamaan (2). Dari sini dapat disimpulan bahwa periode gambar digital yang terdiri atas 101x101 *pixel* (seperti pada Gambar 6.) adalah 25.



Gambar 8. Grafik Hubungan Periode (Sumbu Y) terhadap Ukuran Gambar Digital (Sumbu X) [2]

Perhatikan bahwa Gambar 8. menunjukkan hubungan antara periode terhadap ukuran gambar digital. Meskipun nilai periode ini cenderung meningkat seiring dengan bertambahnya ukuran gambar, namun terdapat ketidakteraturan yang cukup signifikan sehingga cenderung sukar untuk menentukan rumus yang dapat mendefinisikan hubungan periode dan ukuran gambar digital.

IV. Enkripsi pada Gambar Digital

Persamaan (4) yang menunjukkan algoritma Arnold Cat Map dapat digeneralisasi menjadi

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ n \qquad (6)$$

dengan p dan q bilangan bulat positif, dan n adalah ukuran gambar digital dalam *pixel*. Perhatikan bahwa determinan dari matriks transformasi tetaplah bernilai 1 sehingga secara geometris tidak terjadi perubahan luas pada gambar digital. Dari persamaan (6) dapat disimpulkan bahwa algoritma Arnold Cat Map membutuhkan 3 buah parameter yaitu p,q, dan jumlah iterasi yang dilakukan.

Proses Enkripsi dari sebuah gambar digital berukuran n x n pixel, dengan parameter p,q dan jumlah iterasi k dapat dilakukan dalam beberapa tahap. Tahap pertama yaitu pembacaan warna dari gambar digital. Tahap kedua yaitu proses pengacakan posisi pixel pada gambar digital dengan menggunakan persamaan (6). Tahap ketiga yaitu iterasi tahap 1 dan tahap 2 sebanyak k kali terhadap gambar digital.

```
1  {pembacaan gambar digital dari file eksternal}
2  src[n][n] ← open(image_source)
3
4  {iterasi gambar digital}
5  i traversal [1 .. k]
6      row traversal [0 .. n - 1]
7          col traversal [0 .. n - 1]
8
9              {pengaplikasian algoritma Arnold Cat Map}
10             enc_row ← (row + p * col) mod n
11             enc_col ← (q * row + (p * q + 1) * col) mod n
12             encrypt[enc_row][enc_col] ← src[row][col]
13
14     src ← encrypt
15
16 {isi dari encrypt[n][n] adalah hasil dari enkripsi gambar digital}
```

Gambar 9. Potongan *Souce Code* Algoritma Cat Map
Sumber: Dokumentasi Penulis

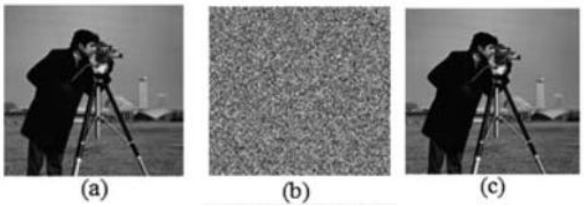
Proses enkripsi dari algorima Arnold Cat Map dapat dituliskan dalam bentuk *pseudocode* terlihat pada Gambar 9. Pada baris 2 dilakukan tahap 1 dari proses enkripsi yaitu pembacaan file eksternal. Hasil dari pembacaan ini akan disimpan dalam sebuah array src berukuran n x n. Nilai yang disimpan dalam array ini dapat berupa kode warna dari tiap pixel pada gambar digital.

Baris kelima menunjukkan tahap ketiga yaitu proses iterasi yang dilakukan sebanyak k kali terhadap tahap kedua yang ditunjukkan oleh baris keenam hinnga ke-14. Proses penyusunan pixel dengan menggunakan algoritma Arnold Cat Map ini dilakukan terhadap setiap pixel pada array src, sehingga dilakukan iterasi di sepanjang *row* dari array src (baris ke-6) dilanjutkan dengan iterasi di sepanjang *column* dari array src (baris ke-7).

Koordinat tiap *pixel* pada gambar digital didefinisikan sebagai indeks *row* dan *column* pada array. Baris ke-10 hingga baris ke-12 adalah proses penerapan algoritma Arnold Cat Map menggunakan persamaan (6). Pada baris ke-10, dilakukan perhitungan terhadap koordinat sumbu x setelah pengaplikasian persamaan (6), sedangkan pada baris ke-11, dilakukan perhitungan terhadap koordinat sumbu y setelah pengaplikasian persamaan (6). Hasil array dengan koordinat baru yang didapat pada perhitungan baris ke-10 dan ke-11 kemudian diisi dengan nilai yang disimpan pada array src koordinat mula-mula sebelum diaplikasikan algoritma Arnold Cat Map. Setelah iterasi terhadap seluruh elemen array src berhasil dilakukan, dilakukan terminasi dengan mengganti nilai array src menjadi array hasil enkripsi (terlihat pada baris ke-14). Alhasil, setelah dilakukan iterasi sebanyak k kali, akan didapatkan array n x n yang berisi hasil enkripsi dengan menggunakan algoritma Arnold Cat Map terhadap array src.

Proses dekripsi dari algoritma Arnold Cat Map ini memanfaatkan sifat periodik dari algoritma Arnold Cat Map ini.

Untuk mendapatkan gambar yang sama seperti semula dilakukan iterasi sebanyak periode gambar digital dikurangi oleh k. Proses ini membutuhkan parameter p, q, dan k seperti pada proses enkripsi.



Gambar 10(a). Gambar Mula-Mula, Gambar 10(b). Gambar Hasil Enkripsi, dan Gambar 10(c). Gambar Hasil Dekripsi [3]

Pada Gambar 10(b). dapat dilihat contoh dari penggunaan algoritma Arnold Cat Map pada gambar berukuran 266 x 256 pixel. Gambar ini dienkripsi dengan iterasi sebanyak 30 kali, dengan nilai p = 10 dan q = 7 sebagai kunci dekripsi. Gambar 10(c). menunjukkan hasil dekripsi dari gambar digital yang sama dengan Gambar 10(a).

Keunggulan algoritma Arnold Cat Map adalah tidak mengubah informasi pada gambar digital. Namun, proses dekripsi dari gambar hasil enkripsi algoritma ini cenderung mudah untuk dipecahkan dengan menggunakan teknik *brute force*. Oleh karena itu, enkripsi gambar digital menggunakan algoritma Arnold Cat Map ini biasa dikombinasikan dengan algoritma lain yang berfungsi mengubah nilai dari *pixel*.

V. KESIMPULAN

Algoritma Arnold Cat Map dapat digunakan untuk melakukan enkripsi dan dekripsi terhadap suatu gambar digital. Dalam prosesnya, Algoritma Arnold Cat Map mengubah posisi setiap *pixel* pada gambar digital tanpa mengubah nilai dari *pixel* tersebut. Enkripsi gambar digital menggunakan algoritma Arnold Cat Map saja tidak cukup. Diperlukan kombinasi dengan algoritma enkripsi lainnya untuk meningkatkan keamanan data yang dienkripsi.

VI. UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan karena atas berkatNya, makalah berjudul “Aplikasi Algoritma Arnold Cat Map dalam Enkripsi Gambar Digital” dapat selesai tepat waktu. Saya ucapkan terima kasih kepada orangtua atas dukungannya selama ini. Terima kasih juga saya ucapkan kepada Bapak Jundhi Santoso, Bapak Rinaldi Munir, dan Ibu Harlili sebagai dosen pengajar Matematika Diskrit atas bimbingannya selama 1 semester ini sehingga makalah ini dapat diselesaikan.

REFERENSI

[1] Munir, Rinaldi. 2006. *Diktat Kuliah IF2120 Matematika Diskrit (Edisi Keempat)*. Bandung: Institut Teknologi Bandung.

[2] Anton, Howard, dan Chris Rorres. 2010. *Elementary Linear Algebra (Tenth Edition)*. John Wiley & Sons, Inc.

[3] Keshari, Sudir dan Modani, (2011). *Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission*, Vol 2, Issue 1. ISSN: 0976-8491

[4] Hariyanto, Eko dan Robbi Rahim, (2016), Arnold’s Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research (IJSR)*, Vol 5, Issue 10. ISSN: 2319-7064

[5] Abdul, Nidaa dan Mohsin Abbas, (2016), Image Encryption based on Independent Component Analysis and Arnold’s Cat Map. *Egyptian Informatics Journal*, Vol 17, Page 139-146, Issue 1. DOI: 10.1016/j.eij.2015.10.001

[6] Struss, Katherine. 2009. *A Chaotic Image Encryption*. Morris: University of Minnesota.

[7] Gupta, Priyanka, Sonia Singh dan Isha Mangal, (2014), Image Encryption Based On Arnold Cat Map and S-Box. *International Journal of Advanced Research in Computer Science and Software Engineer*, Vol 4, Issue 8. ISSN: 2277 128X

[8] https://www.scribd.com/doc/62777487/Teori-Dasar-Kriptografi diakses pada 2 Desember 2017 pukul 21.30 WIB

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2017

Rika Dewi, 13517147