BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

Enkripsi Nilai Piksel Pada Citra Digital Dengan Algoritma Piecewise Linear Chaotic Map

Robby Wijaya

Program Studi Sistem Informasi, STMIK TIME, Medan, Indonesia
Email: robbyhuang98@email.com
Email Penulis Korespondensi: robbyhuang98@email.com

Abstrak−Proses perekaman, penyimpanan dan sharing citra digital sangat mudah dilakukan saat ini. Untuk memproteksi informasi di dalam citra, citra dapat dienkripsi dengan mengacak citra ke bentuk citra yang tidak dapat dimengerti. Algoritma Piecewise Linear Chaotic Map digunakan dalam penelitian untuk melakukan proses enkripsi terhadap citra. Caranya adalah algoritma Piecewise Linear Chaotic Map membangkitkan bilangan acak, dan bilangan acak tersebut digunakan untuk mengacak nilai piksel citra dengan menggunakan fungsi XOR. Aplikasi menerapkan metode Piecewise Linear Chaotic Map untuk mengenkripsi nilai piksel pada citra digital, sehingga hanya pihak tertentu saja yang mengetahui kunci yang dapat mengakses citra digital.

Kata Kunci: Citra Digital; Enkripsi; Piecewise Linear Chaotic Map

Abstract−The process of recording, storing and sharing digital images is very easy to do nowadays. To protect the information in the image, the image can be encrypted by scrambling the image into an unintelligible image form. The Piecewise Linear Chaotic Map algorithm is used in research to encrypt images. The trick is that the Piecewise Linear Chaotic Map algorithm generates random numbers, and these random numbers are used to randomize image pixel values using the XOR function. The application implements the Piecewise Linear Chaotic Map method to encrypt pixel values in digital images, so that only certain parties who know the key can access digital images.

Keywords: Digital Image; Encryption; Piecewise Linear Chaotic Map

1. PENDAHULUAN

Dalam dunia digital saat ini, keamanan citra digital menjadi semakin penting karena pengiriman sering dilakukan melalui jaringan terbuka. Kemanan citra digital dibutuhkan pada banyak aplikasi, seperti sistem pencitraan medis, citra militer, konferensi video rahasia dan bidang lainnya. Banyak metode enkripsi telah dikembangkan untuk memenuhi permintaan terhadap keamanan citra. Akan tetapi beberapa diantaranya diketahui tidak aman seperti pada jurnal penelitian "Partial Encryption of Compressed Images and Videos" yang membahas mengenai kriptanalisis pada citra dan video yang dikompres dan ditransmisikan melalui aplikasi multimedia dan jaringan nirkabel dan jurnal "On the Security of Image Encryption Method" yang membahasa keamanan dan kriptanalisis terhadap beberapa metode enkripsi citra [1]. Teknik enkripsi citra berbeda dengan teknik enkripsi data karena terdapat beberapa serangan yang mungkin dilakukan pada citra yang berhubungan dengan pengolahan citra, seperti pengubahan warna citra keabuan, pengubahan ukuran citra dan teknik pre-processing lainnya. Oleh karen itu dibutuhkan algoritma yang lebih kuat untuk meminimalkan keberhasilan serangan terhadap skema enkripsi citra digital [2].

Penelitian yang dilakukan oleh Mondal dan Mandal menggunakan logistic map untuk mengacak posisi piksel pada citra graysacle, karena logistic map dapat berjalan pada komputasi yang rendah dan merupakan generator bilangan acak yang ringan. Akan tetapi logistic mapping memiliki kelemahan yaitu distribusi yang tidak merata, keamanan yang rendah dan ruang parameter yang kecil [3]. Penelitian yang dilakukan oleh Wang, Liu dan Lei mengemukakan bahwa Piecewise Linear Chaotic Map (PWLCM) memiliki performa pengacakan yang lebih baik dibandingkan dengan Logistic Map [2]. Enkripsi citra digital merupakan hal yang penting untuk mengamankan informasi yang terkandung pada citra digital. Pengamanan citra dapat dilakukan dengan mengacak intensitas warna citra melalui channel warna Red, Green dan Blue, sehingga warna setiap piksel pada citra berubah dan pada akhirnya citra tidak memiliki makna. Metode chaotic map yang dapat digunakan untuk mengacak citra digital adalah Piecewise Linear Chaotic Map. Metode chaotic map ini diketahui memiliki siklus yang besar dan memiliki distribusi keseragaman yang acak. Piecewise Linear Chaotic Map adalah chaos map yang terdiri dari beberapa segmen linier. Pemilihan metode Piecewise Linear Chaotic Map dalam penelitian ini karena metode ini memiliki densitas pengacakan dan fungsi korelasi yang baik.

2. METODOLOGI PENELITIAN

2.1 Implementasi

Implementasi adalah bermuara pada aktivitas, aksi, tindakan, atau adanya mekanisme suatu sistem. Implementasi bukan sekedar aktivitas, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh- sungguh berdasarkan acuan norma tertentu untuk mencapai tujuan kegiatan, sehingga implementasi tidak berdiri sendiri tetapi dipengaruhi oleh objek berikutnya. Implementasi adalah perluasan aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana, birokrasi yang efektif [4].

Implementasi dapat diartikan sebagai pelaksanaan atau penerapan [5]. Implementasi bermuara pada aktivitas, aksi, tindakan, atau adanya mekanisme suatu sistem. Implementasi bukan sekedar aktivitas, tetapi suatu kegiatan yang

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

terencana dan untuk mencapai tujuan kegiatan. Menurut Guntur Setiawan, "Implementasi adalah perluasan aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana, birokrasi yang efektif [6].

2.2 Algoritma

Algoritma berasal dari nama ilmuwan muslim dari Uzbekistan, Abu Ja'far Muhammad bin Musa Al- Khuwarizmi (780-846M). Pada awalnya kata algoritma adalah istilah yang merujuk kepada aturan-aturan aritmetika untuk menyelesaikan persoalan dengan menggunakan bilangan numerik arab. Pada abad ke-18, istilah ini berkembang menjadi algoritma, yang mencakup semua prosedur atau urutan langkah yang jelas dan diperlukan untuk menyelesaikan suatu permasalahan. Pemecahan sebuah masalah pada hakikatnya adalah menemukan langkah-langkah tertentu yang jika dijalankan efeknya akan memecahkan masalah tersebut [7].

Pemecahan sebuah masalah pada hakekatnya adalah menemukan langkah-langkah tertentu yang jika dijalankan efeknya akan memecahkan masalah tersebut. Misalnya, dalam masalah menelepon. Sewaktu akan menelepon di telepon umum, maka urutan langkah-langkah tertentu mesti dilakukan. Urutan langkah-langkah tersebut secara garis besar adalah [8]:

1. Angkat gagang telepon
2. Masukkan koin
3. Tekan nomor yang akan dihubungi
4. Bicara
5. Letakkan gagang telepon

Definisi algoritma adalah susunan langkah penyelesaian suatu masalah secara sistematis dan logis. Terdapat dua kata yang menjadi perhatian dalam definisi ini, yaitu sistematis dan logis [9]. Suatu pekerjaan dapat diselesaikan dengan menggunakan algoritma yang berbeda dengan kumpulan instruksi (set of instructions) yang berbeda dengan perbedaan waktu akses, efisiensi tempat, usaha dan sebagainya. Dua buah resep yang berbeda untuk membuat salad kentang dapat dijadikan contoh, resep pertama mengupas kulit kentang terlebih dahulu sebelum memasak kentang tersebut, sementara resep lainnya dilakukan dengan langkah yang terbalik, dan kedua resep akan mengulangi kedua langkah tersebut dan akan dihentikan pada saat salad kentang siap untuk dimakan [10]. Beberapa kriteria atau syarat algoritma secara umum adalah sebagai berikut [11]:

1. Algoritma harus tidak ambigu (unambigous)
2. Algoritma harus tepat (precise)
3. Algoritma harus pasti (definite)
4. Algoritma harus berhingga (finite)

Serangkaian langkah dalam algoritma harus dapat dilaksanakan pada rentang waktu tertentu seperti yang telah diuraikan sebelumnya. Pertimbangan dalam pemilihan algoritma adalah [12]:

1. Algoritma haruslah benar, artinya algoritma akan memberikan keluaran yang dikehendaki atau diharapkan dari sejumlah masukan yang diberikan. Suatu algoritma bukan algoritma yang baik jika memberikan keluaran yang salah, tidak peduli sebagus apapun struktur dari algoritma tersebut.
2. Algoritma harus mampu memberikan hasil yang sedekat mungkin dengan nilai yang sebenarnya.
3. Algoritma harus efisien.

2.3 Piecewise Linear Chaotic Map (PWLCM)

Teori chaotic map (pengacakan) sudah menjadi topik penelitian yang atraktif di dalam bidang keamanan informasi. Karakteristik yang menarik dari chaos (acak) adalah sensitifitasnya terhadap nilai awal (initial value). Jika nilai awal sistem chaos diubah sedikit saja, misalnya sebesar 10^{-10}, maka bila sistem chaos tersebut diiterasikan sejumlah kali, hasil iterasinya berbeda signifikan dengan sebelumnya. Sensisitivitas ini sangat berguna di dalam kriptografi karena bersesuaian dengan prinsip diffusion dari Shannon dalam merancang sebuah algoritma kriptografi. Dengan prinsip diffusion ini, maka pengubahan satu bit nilai awal chaos dapat menyebabkan cipherteks tetap tidak berhasil didekripsi [13].

Random number generator (RNG) adalah suatu peralatan komputasional yang dirancang untuk menghasilkan suatu urutan nilai yang tidak dapat ditebak polanya dengan mudah, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak (random). RNG ini tidak dapat diterapkan dalam prakteknya. Bilangan acak yang dihasilkan oleh komputer sekalipun tidak benar-benar acak dan kebanyakan bilangan acak yang diterapkan dalam kriptografi juga tidak benar-benar acak, tetapi hanya berupa acak semu. Ini berarti bahwa bilangan acak yang dihasilkan itu dapat ditebak susunan atau urutan nilainya. Dalam kriptografi, bilangan acak sering dibangkitkan dengan menggunakan pembangkit bilangan acak semu (pseudo random number generator) [14].

Bilangan acak adalah deretan nilai yang acak dan tidak dapat diprediksi secara keseluruhan. Untuk menghasilkan bilangan acak merupakan hal yang sulit, kebanyakan pembangkit bilangan acak (random bit / random number generator) mempunyai beberapa bagian yang dapat diprediksi dan berhubungan. Kebanyakan RNG mengulang string yang sama setelah melakukan n putaran, sedangkan ada beberapa RNG lainnya menghasilkan nilai acak dengan berfokus pada suatu area tertentu dan mendistribusikannya secara seragam [14].

Piecewise Linear Chaotic Map (PWLCM) adalah chaos map yang terdiri dari beberapa segmen linier. Piecewise Linear Chaotic Map memiliki densitas pengacakan dan fungsi korelasi yang baik [15]. Bila dibandingkan

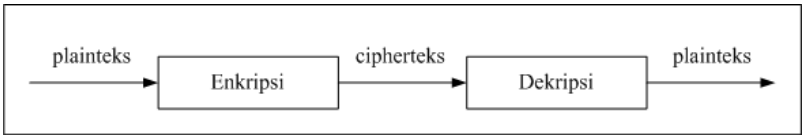
ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

dengan Logistic Map, Piecewise Linear Chaotic Map memiliki range yang lebih luas, karena Logistic Map hanya akan acak apabila nilai parameter alpha mendekati nilai 4, sedangkan nilai parameter pada Piecewise Linear Chaotic Map dapat ditentukan antara nilai 0 hingga 0.5. Rumus pengacakan yang dihasilkan oleh Piecewise Linear Chaotic Map dapat dilihat pada persamaan 1 berikut [16].

$$x(n) = F[x(n-1)] = \begin{cases} x(n-1)x\frac{1}{p} & if\ 0 \le x(n-1) < p \\ [x(n-1)-p]x\frac{1}{0{,}5-p} & if\ p \le x(n-1)0{,}5 \\ F[1-x(n-1)] & if\ 0{,}5 \le x(n-1) < 1 \end{cases} \quad (1)$$

2.4 Enkripsi dan Dekripsi

Pesan asli yang dirahasiakan dinamakan plainteks (plaintext, artinya teks jelas yang dapat dimengerti), sedangkan pesan hasil penyandian disebut cipherteks (ciphertext, artinya teks tersandi). Pesan yang telah disandikan dapat dikembalikan lagi ke pesan aslinya hanya oleh orang yang berhak (orang yang mengetahui metode penyandian dan memiliki kunci penyandian). Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption), sedangkan proses mengembalikan cipherteks menjadi plainteks disebut dekripsi (decryption). Gambar 1 memperlihatkan diagram kedua proses yang dimaksud [17].



Gambar 1. Proses Enkripsi dan Proses Dekripsi

Algoritma kriptografi yang berfungsi untuk mengamankan data, terdiri dari tiga fungsi dasar [18], yaitu:

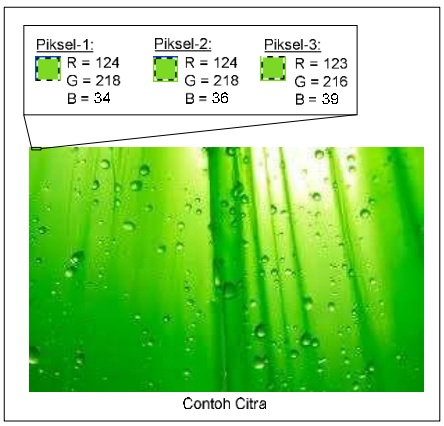
1. Enkripsi, merupakan proses untuk merubah plaintext menjadi ciphertext dengan menambahkan kunci.
2. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan.
3. Kunci, yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi.

Dengan demikian, keamanan suatu pesan tergantung pada kunci yang digunakan dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidak menjadi masalah apabila seseorang mengetahui algoritma yang digunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan [19].

3. HASIL DAN PEMBAHASAN

3.1 Proses Enskripsi Citra

Algoritma Piecewise Linear Chaotic Map digunakan dalam penelitian untuk melakukan proses enkripsi terhadap citra. Cara untuk menggunakannya adalah algoritma Piecewise Linear Chaotic Map membangkitkan bilangan acak, dan bilangan acak tersebut digunakan untuk mengacak nilai piksel citra dengan menggunakan fungsi XOR. Sebagai contoh, misalkan proses enkripsi Piecewise Linear Chaotic Map dilakukan pada citra pada gambar2 berikut.



Gambar 2. Contoh Citra

Proses enkripsi Piecewise Linear Chaotic Map terhadap citra digital pada gambar 2 adalah sebagai berikut:

1. Nilai parameter p yang digunakan = 0.3678 (dibatasi antara 0.1 hingga 0.5 sesuai ketentuan pada Piecewise Linear Chaotic Map).

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

2. Kunci pengacakan x(0) = y = 0.785697415
3. Proses enkripsi terhadap piksel-1 (R = 124, G = 218 dan B = 34) adalah sebagai berikut:
   a. Enkripsi nilai R = 124
      1) x(0) = 0.785697415
      2) Hitung nilai acak x(1)
         x(1) = F(x(0)) = F(0.785697415)
         Oleh karena 0.5 <= 0.785697415 < 1, maka
         x(1) = F(1 - 0.785697415)
         x(1) = F(0.214302585)
         Oleh karena 0 <= 0.214302585 < 0.3678, maka
         x(1) = 0.214302585 * 1/0.3678
         x(1) = 0.5826606444
      3) Nilai kunci = x(1) * 255 = 0.5826606444 * 255 = 149
      4) Operasi XOR antara nilai R dan nilai kunci:
         R = 124 XOR 149 = 233
   b. Enkripsi nilai G = 218
      1) x(1) = 0.5826606444
      2) Hitung nilai acak x(2)
         Oleh karena 0.5 <= 0.5826606444 < 1, maka
         x(2) = F(1 - 0.5826606444)
         x(2) = F(0.4173393556)
         Oleh karena 0.3678 <= 0.4173393556 < 0.5, maka
         x(2) = (0.4173393556 - 0.3678) * 1/(0.5 - 0.3678)
         x(2) = 0.3747303752
      3) Nilai kunci = x(2) * 255 = 0.3747303752 * 255 = 96
      4) Operasi XOR antara nilai G dan nilai kunci:
         G = 218 XOR 96 = 186
   c. Enkripsi nilai B = 34
      1) x(2) = 0.3747303752
      2) Hitung nilai acak x(3)
         Oleh karena 0.3678 <= 0.3747303752 < 0.5, maka
         x(3) = (0.3747303752 - 0.3678) * 1/(0.5 - 0.3678)
         x(3) = 0.052423413
      3) Nilai kunci = x(3) * 255 = 0.052423413 * 255 = 13
      4) Operasi XOR antara nilai B dan nilai kunci:
         B = 34 XOR 13 = 47
   d. Hasil enkripsi piksel-1, R = 124, G = 218 dan B = 34, dienkripsi menjadi R = 233, G = 186 dan B = 47.
4. Proses enkripsi terhadap piksel-2 (R = 124, G = 218 dan B = 36) adalah sebagai berikut:
   a. Enkripsi nilai R = 124
      1) x(3) = 0.052423413
      2) Hitung nilai acak x(4)
         x(4) = F(x(3)) = F(0.052423413)
         Oleh karena 0 <= 0.052423413 < 0.3678, maka
         x(4) = 0.052423413 * 1/0.3678
         x(4) = 0.1425323899
      3) Nilai kunci = x(4) * 255 = 0.1425323899 * 255 = 36
      4) Operasi XOR antara nilai R dan nilai kunci:
         R = 124 XOR 36 = 88
   b. Enkripsi nilai G = 218
      1) x(4) = 0.1425323899
      2) Hitung nilai acak x(5)
         x(5) = F(x(4)) = F(0.1425323899)
         Oleh karena 0 <= 0.1425323899 < 0.3678, maka
         x(5) = 0.1425323899 * 1/0.3678
         x(5) = 0.3875268893
      3) Nilai kunci = x(5) * 255 = 0.3875268893 * 255 = 99
      4) Operasi XOR antara nilai G dan nilai kunci:
         G = 218 XOR 99 = 185
   c. Enkripsi nilai B = 36
      1) x(5) = 0.3875268893
      2) Hitung nilai acak x(6)
         x(6) = F(x(5)) = F(0.3875268893)

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

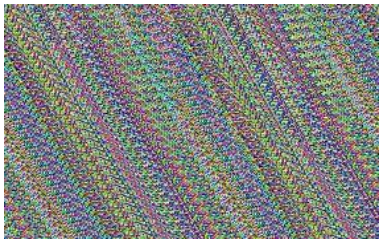
Oleh karena 0.3678 <= 0.3875268893 < 0.5, maka
x(6) = (0.3875268893 - 0.3678) * 1/(0.5 - 0.3678)
x(6) = 0.1492200401

3) Nilai kunci = x(6) * 255 = 0.1492200401 * 255 = 38
4) Operasi XOR antara nilai B dan nilai kunci:
B = 36 XOR 38 = 2

d. Hasil enkripsi piksel-2, R = 124, G = 218 dan B = 36, dienkripsi menjadi R = 88, G = 185 dan B = 2.

5. Ulangi proses di atas hingga semua piksel citra terenkripsi.

Hasil enkripsi citra dengan algoritma Piecewise Linear Chaotic Map dapat dilihat pada gambar 3.



Gambar 3. Hasil Citra Terenkripsi

3.2 Proses Deskripsi Citra

Proses dekripsi citra sama dengan proses enkripsi citra. Proses dekripsi tetap melakukan pembangkitan nilai acak dan menggunakannya untuk mendekripsi nilai piksel citra. Apabila nilai parameter p dan nilai kunci y yang digunakan sama dengan nilai pada proses enkripsi, maka proses dekripsi akan berhasil mengembalikan citra terenkripsi kembali ke citra awal. Proses dekripsi terhadap citra hasil enkripsi dari sub bab proses enkripsi citra adalah sebagai berikut:

1. Nilai parameter p = 0.3678
2. Kunci dekripsi x(0) = y = 0.785697415
3. Proses dekripsi terhadap piksel-1 (R = 233, G = 186 dan B = 47) adalah sebagai berikut:
   a. Dekripsi nilai R = 233
      1) x(0) = 0.785697415
      2) Hitung nilai acak x(1)
         x(1) = F(x(0)) = F(0.785697415)
         Oleh karena 0.5 <= 0.785697415 < 1, maka
         x(1) = F(1 - 0.785697415)
         x(1) = F(0.214302585)
         Oleh karena 0 <= 0.214302585 < 0.3678, maka
         x(1) = 0.214302585 * 1/0.3678
         x(1) = 0.5826606444
      3) Nilai kunci = x(1) * 255 = 0.5826606444 * 255 = 149
      4) Operasi XOR antara nilai R dan nilai kunci:
         R = 233 XOR 149 = 124
   b. Dekripsi nilai G = 186
      1) x(1) = 0.5826606444
      2) Hitung nilai acak x(2)
         Oleh karena 0.5 <= 0.5826606444 < 1, maka
         x(2) = F(1 - 0.5826606444)
         x(2) = F(0.4173393556)
         Oleh karena 0.3678 <= 0.4173393556 < 0.5, maka
         x(2) = (0.4173393556 - 0.3678) * 1/(0.5 - 0.3678)
         x(2) = 0.3747303752
      3) Nilai kunci = x(2) * 255 = 0.3747303752 * 255 = 96
      4) Operasi XOR antara nilai G dan nilai kunci:
         G = 186 XOR 96 = 218
   c. Dekripsi nilai B = 47
      1) x(2) = 0.3747303752
      2) Hitung nilai acak x(3)
         Oleh karena 0.3678 <= 0.3747303752 < 0.5, maka
         x(3) = (0.3747303752 - 0.3678) * 1/(0.5 - 0.3678)
         x(3) = 0.052423413
      3) Nilai kunci = x(3) * 255 = 0.052423413 * 255 = 13
      4) Operasi XOR antara nilai B dan nilai kunci:

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

B = 47 XOR 13 = 34

d. Hasil dekripsi piksel-1, R = 233, G = 186 dan B = 47 menjadi R = 124, G = 218 dan B = 34.

4. Proses dekripsi terhadap piksel-2 (R = 88, G = 185 dan B = 124) adalah sebagai berikut:
   a. Dekripsi nilai R = 88
      1) x(3) = 0.052423413
      2) Hitung nilai acak x(4)
         x(4) = F(x(3)) = F(0.052423413)
         Oleh karena 0 <= 0.052423413 < 0.3678, maka
         x(4) = 0.052423413 * 1/0.3678
         x(4) = 0.1425323899
      3) Nilai kunci = x(4) * 255 = 0.1425323899 * 255 = 36
      4) Operasi XOR antara nilai R dan nilai kunci:
         R = 88 XOR 36 = 124
   b. Dekripsi nilai G = 185
      1) x(4) = 0.1425323899
      2) Hitung nilai acak x(5)
         x(5) = F(x(4)) = F(0.1425323899)
         Oleh karena 0 <= 0.1425323899 < 0.3678, maka
         x(5) = 0.1425323899 * 1/0.3678
         x(5) = 0.3875268893
      3) Nilai kunci = x(5) * 255 = 0.3875268893 * 255 = 99
      4) Operasi XOR antara nilai G dan nilai kunci:
         G = 185 XOR 99 = 218
   c. Dekripsi nilai B = 2
      1) x(5) = 0.3875268893
      2) Hitung nilai acak x(6)
         x(6) = F(x(5)) = F(0.3875268893)
         Oleh karena 0.3678 <= 0.3875268893 < 0.5, maka
         x(6) = (0.3875268893 - 0.3678) * 1/(0.5 - 0.3678)
         x(6) = 0.1492200401
      3) Nilai kunci = x(6) * 255 = 0.1492200401 * 255 = 38
      4) Operasi XOR antara nilai B dan nilai kunci:
         B = 2 XOR 38 = 36
   d. Hasil dekripsi piksel-2, R = 88, G = 185 dan B = 2 menjadi R = 124, G = 218 dan B = 36.
5. Ulangi proses di atas hingga semua piksel citra terdekripsi.

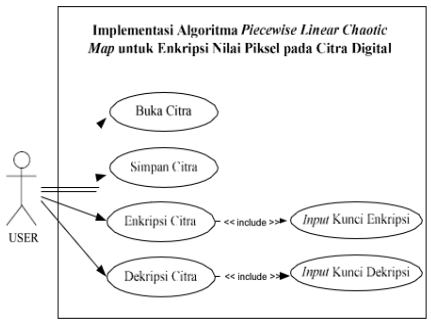
Aplikasi hasil rancangan dapat digunakan untuk mengacak dan mengamankan citra digital dengan menggunakan metode Piecewise Linear Chaotic Map. Kelebihan yang dimiliki oleh aplikasi adalah sebagai berikut:

1. Pengguna dapat memasukkan kunci enkripsi, berupa nilai parameter p dan nilai y. Citra terenkripsi tidak akan dapat didekripsi apabila kunci enkripsi tidak diketahui.
2. Walaupun citra terenkripsi mengalami distorsi pada bagian tertentu, tetapi citra masih dapat didekripsi.

Di samping kelebihan yang dimiliki oleh aplikasi, terdapat pula kelemahan yang dimiliki oleh aplikasi sebagai berikut:

1. Aplikasi tidak dapat melakukan proses enkripsi terhadap file lain, selain file citra..
2. Aplikasi dapat berjalan pada sistem operasi windows dan tidak dapat dijalankan pada sistem operasi lainnya, seperti sistem operasi android atau iOS.

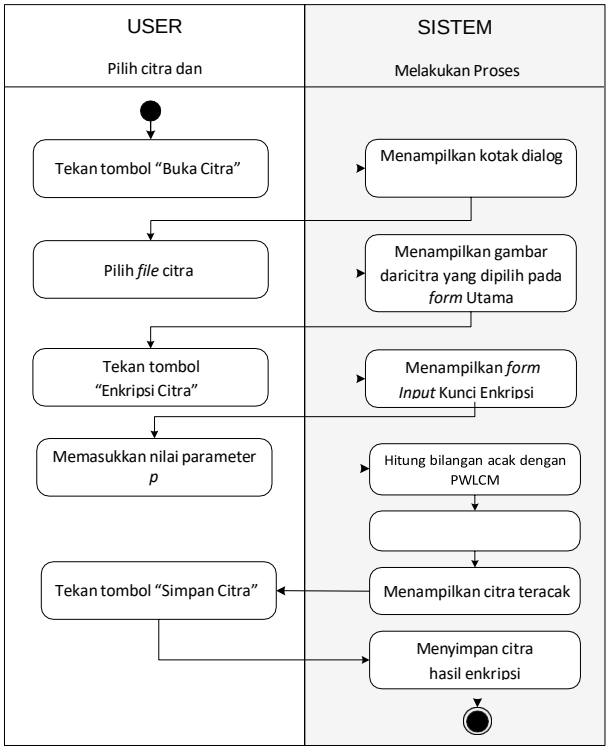
Unified Modeling Language (UML) digunakan untuk memodelkan sistem. Diagram UML yang digunakan adalah use case dan activity diagram. Use case adalah salah satu diagram Unified Modeling Language (UML) yang dapat digunakan untuk menganalisis dan memodelkan sistem. Gambar 4 menunjukkan interaksi antara pengguna dan sistem di dalam diagram use case.



Gambar 4. Diagram Use Case Aplikasi

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

Proses enkripsi citra di dalam aplikasi dapat digambarkan dengan activity diagram seperti terlihat pada gambar 5.



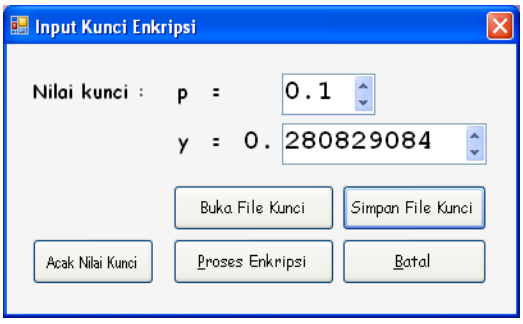
Gambar 5. Activity Diagram dari Proses Enkripsi.

Berikut adalah hasil implementasi dari perancangan aplikasi Piecewise Linear Chaotic Map untuk enkripsi nilai piksel pada citra digital:

1. Sebagai contoh, dipilih file citra dengan nama file "05. Chedi.jpg", maka file citra akan ditampilkan pada form utama, seperti terlihat pada gambar

Gambar 6. Citra pada Form Utama.

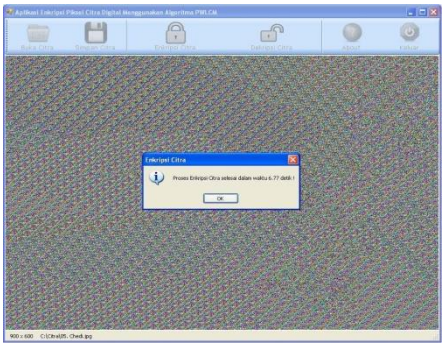
2. Untuk mengenkripsi citra, pilih dan tekan tombol "Enkripsi Citra" pada form Utama, dan form Input Kunci Enkripsi Form Input Kunci Enkripsi berfungsi untuk menerima input nilai kunci yang akan digunakan untuk proses enkripsi.



Gambar 7. Form Input Kunci Enkripsi

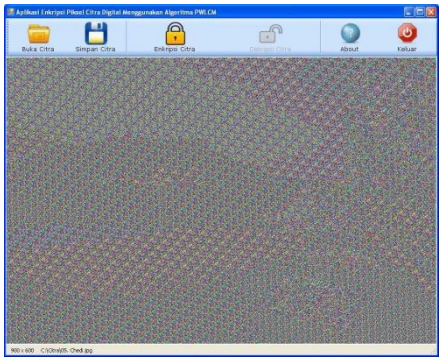
3. Masukkan kunci berupa nilai p = 0.1 dan nilai y = 0.280829084 klik proses enkripsi maka proses enkripsi akan berjalan

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr



Gambar 8. Citra Hasil Enkripsi

4. Misalkan dimasukkan kunci dekripsi yang berbeda, yaitu nilai p = 0.1 dan nilai y = 0.280829085, atau memiliki selisih nilai kunci 0.000000001 dengan nilai kunci enkripsi 0.280829084, maka hasil dekripsi citra sebagai berikut



Gambar 9. Hasil Dekripsi Citra dengan Kunci Berbeda

4. KESIMPULAN

Setelah menyelesaikan penelitian mengenai perancangan aplikasi Piecewise Linear Chaotic Map untuk enkripsi nilai piksel pada citra digital, beberapa hal yang dapat disimpulkan adalah sebagai berikut: Aplikasi menerapkan metode Piecewise Linear Chaotic Map untuk mengenkripsi nilai piksel pada citra digital, sehingga hanya pihak tertentu saja yang mengetahui kunci yang dapat mengakses citra digital Proses dekripsi harus menggunakan kunci yang sama dengan proses enkripsi untuk mengembalikan citra terenkripsi ke citra awal. Walaupun citra terenkripsi mengalami distorsi pada bagian tertentu, tetapi citra masih dapat didekripsi.

REFERENCES

[1] Li, S., and Zheng, X., 2014, On The Security of an Image Encryption Method, China; Xi'an Jiaotong University.
[2] Wang Y., Liu Z., and Lei P., 2014 Cryptographic Properties Analysis of Piecewise Logistic Map, Chongqing, China; Chongqing University of Posts and Telecommunications
[3] Mondal and Mandal, 2016, A Light Weight Secure Image Encryption Scheme Based on Chaos & DNA Computing. Jharkhand, India; Jurnal of King Saud University Computer and Information Sciences
[4] B. Mesterjon, dan L.N. Zulita, Implementasi Metode Selection Sort untuk Menentukan Nilai Prestasi Siswa Kelas 3 dan Kelas 4 SD Negeri 107 Seluma, Bengkulu: Universitas Dehasen, 2015.
[5] Kamus Besar Bahasa Indonesia (KBBI), Pengertian Implementasi, http://kbbi.web.id/implementasi, 2020.
[6] Ario, Implementasi Peraturan Presiden nomor 26 tahun 2009 tentang Penerapan E-KTP Berbasis NIK di Samarinda, Jakarta: E-journal Ilmu Pemerintahan, 2016.
[7] Tarigan, Analisis Dan Implementasi Algoritma Linear Search Pada Permainan Word Scramble, Medan:USU, 2015.
[8] Yulita, Algoritma dan Pemrograman, Yogyakarta: STMIK Amikom, 2018.
[9] Sitorus, Algoritma dan Pemrograman, Yogyakarta: Andi, 2015.
[10] Sigiro. Analisis Dan Implementasi Penyelesaian Game Minesweeper Menggunakan Algoritma Greedy BestFirst Search. Medan: Universitas Sumatera Utara, 2016.
[11] Wahid, Dasar-Dasar Algoritma & Pemrograman, Yogyakarta: Andi, 2017.
[12] Utami dan Sukrisno, 10 Langkah Belajar Logika dan Algoritma Menggunakan Bahasa C dan C++ di GNU/Linux. Yogyakarta: Andi, 2019.
[13] R. Munir, Algoritma Enkripsi Citra Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map, Bandung: ITB, 2015.
[14] Tjahjono, dkk, Implementasi Unique Code Nominal Transfer Menggunakan Metode Linear Congruential Generator untuk Order Deposit, Pasuruan: Universitas Merdeka, 2016.
[15] X. Wang, and D. Chen, A Parallel Encryption Algorithm Based on Piecewise Linear Chaotic Map, Harbin,China: Hindawi Publishing Corporation, 2018.
[16] A. Awad, and A. Saadane, New Chaotic Permutation Methods for Image Encryption, Orleans, France:IAENG

ISSN 2774-3659 (Media Online)
Vol 3, No 1, Desember 2022
DOI 10.47065/bulletincsr.v3i1.206 | Hal 161−169
https://hostjournals.com/bulletincsr

International Journal of Computer Science, 2015.
[17] R. Munir, Matematika Diskrit, Bandung: Informatika, 2014.
[18] D. Ariyus, Kriptografi, Yogyakarta: Andi, 2015.
[19] R. Munir, Kriptografi, Bandung: Informatika, 2016.