Jurnal Infosecure Vol.4 No.2, Oktober 2023
p-ISSN: 2087-1023
MTI-UNLA

Pengamanan Data Sensitif pada Citra Digital Menggunakan Enkripsi Parsial Berdasarkan Chaos Mapping

Erik Arvan Wahyudi[1], Arief Zulianto[2], Mokhamad Hendayun[3], Hendra Sandhi Firmansyah[4]

Magister Teknik Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3,4]

[1]erik.arvan@widyatama.ac.id

[2]ariefzul@unla.ac.id

[3]hendayun@unla.ac.id

[4]hendrasf@unla.ac.id

Abstrak— Di era digital saat ini, citra digital banyak berperan penting dalam pertukaran informasi. Namun dalam citra digital tersebut kemungkinan terdapat informasi sensitif, yang dapat menjadi sumber dari *Personally Identifiable Information* (PII). Oleh karena itu, area yg berisi informasi sensitif tersebut perlu diamankan. Pada proposal usulan penelitian ini, penulis mengusulkan pengamanan area sensitif tersebut dengan menggunakan ekripsi secara parsial pada area sensitif saja, tanpa mengenkripsi citra secara keseluruhan. Skema enkripsi yang diusulkan menggunakan dua jenis pengacakan yang berdasarkan pemetaan *chaos*, pertama pengacakan posisi piksel dengan menggunakan Arnold Cat Map (ACM), yang kedua pengacakan warna pada piksel dengan menggunakan Tribonacci Cat Map (TCM)**.**

Kata kunci— citra digital, PII, enkripsi parsial, ACM, TCM

I. PENDAHULUAN

Saat ini kita banyak bertukar data yang berisikan informasi sensitif dalam bentuk citra digital. Salah satu contoh adalah kita mengirim foto sebagai bentuk bukti identitas digital ketika mengisi aplikasi *online*, atau tanda nomor kendaraan bermotor yang tertangkap pada cctv di jalan raya. Otoritas pemerintah dan berbagai organisasi bisnis menyimpan dan menggunakan data-data tersebut. Secara luas, informasi sensitif yang terdapat pada citra digital tersebut dapat menjadi sumber dari *Personally Identifiable Information* (PII) atau informasi pribadi. PII mencakup setiap informasi yang dapat digunakan secara unik untuk mengidentifikasi, menghubungi, atau menemukan satu orang individu atau dapat digunakan dengan sumber lain untuk mengidentifikasi satu individu secara unik [1]. Implikasinya, PII dapat digunakan atau dijual untuk memfasilitasi pencurian identitas. PII dapat dieksploitasi dalam berbagai bentuk, dari pencurian identitas, *spamming* dan *phishing* sampai ke spionase dunia maya.

Terdapat sejumlah pilihan untuk perlindungan PII, yang mana masing-masing memiliki kelebihan dan kekurangan yang berbeda dan kurang lebih sesuai untuk situasi tertentu. Teknologi berikut termasuk kedalam kategori *Data Leak Prevention* (DLP) atau pencegahan kebocoran data, antara lain *Hashing*, *Masking*, *End-to-end encryption*, *Strong encryption*, *format-preserving encryption*, *Basic (vaulted) tokenization, In-memory (vaultless) tokenization* [2]. Tantangan dalam perlindungan PII terutama pada citra digital adalah bagaimana citra dapat digunakan untuk berbagai kepentingan tanpa menampilkan/mengakses area sensitif yang selanjutnya disebut Region of Interest (ROI), akan tetapi bila diperlukan oleh pihak yang berwenang, ROI bisa ditampilkan/diakses kembali.

Enkripsi dapat memenuhi banyak kebutuhan dalam perlindungan PII, tapi enkripsi citra secara keseluruhan menyebabkan citra tidak bisa digunakan sama sekali walaupun informasi yang diperlukan berada di luar area sensitif (Non-ROI). Oleh karena itu penulis mengusulkan skema enkripsi parsial hanya pada ROI, sedangkan Non-ROI tidak terenkripsi sehingga tetap bisa diakses. Jenis enkripsi yang digunakan harus memenuhi syarat berikut, yaitu tidak mengubah dimensi area yang dienkripsi karena area enkripsi sebagian atau secara keseluruhan dikelilingi oleh area yang tidak dienkripsi, dan syarat berikutnya adalah mempertahankan format citra antara lain dengan menjaga rentang nilai piksel yang dienkripsi tidak boleh keluar dari rentang nilai warna (0-255) agar citra hasil enkripsi tetap dapat ditampilkan di aplikasi pemuat citra yang umum digunakan, tanpa harus menggunakan aplikasi khusus.

Pada penelitian ini penulis mengusulkan skema enkripsi parsial pada citra yang memiliki area sensitif, dengan hanya mengenkripsi area ROI dan tanpa mengenkripsi area Non-ROI. Dengan demikian citra

enkripsi parsial yang dihasilkan masih tetap dapat digunakan dan informasi sensitif pada area ROI tetap terlindungi. Adapun sistem kriptografi citra yang digunakan pada penelitian ini adalah kombinasi dua pemetaan chaos, yaitu pengacakan posisi piksel dengan menggunakan pemetaan dua dimensi *Arnold Cat Map* (ACM) dan pengacakan nilai piksel dengan menggunakan pemetaan tiga dimensi *Tribonacci Cat Map* (TCM), kombinasi tersebut tidak merubah dimensi area enkripsi dan juga tetap mempertahankan format citra, sehingga area ROI hasil proses enkripsi masih dapat digabungkan kembali dengan area Non-ROI, dan citra terenkripsi parsial yang dihasilkan masih dapat ditampilkan oleh aplikasi pemuat citra yang umum digunakan tanpa harus menggunakan aplikasi khusus.

Makalah ini disusun sebagai berikut: bagian 1 berisikan pendahuluan, bagian 2 membahas penelitian terkait, bagian 3 memperkenalkan skema yang diusulkan, dan pada bagian terakhir dibahas mengenai metode yang akan digunakan untuk pengujian hasil penelitian

II. PENELITIAN TERKAIT

Personally Identifiable Information (PII) atau informasi pribadi dikenal juga sebagai data pribadi adalah segala informasi yang mengidentifikasikan seseorang. Undang-undang Negara Republik Indonesia Nomor 27 tahun 2022, pasal 1 (1) mendefinisikan data pribadi sebagai "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik", pasal 4 (1) memisahkan jenis data pribadi menjadi data bersifat spesifik dan data bersifat umum. Data spesifik seperti yang dijabarkan pada pasal 4 (2) antara lain berupa data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data kekurangan pribadi, dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Sedangkan data bersifat umum dijabarkan pada pasal 4 (3) terdiri dari nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang [3].

Pedoman privasi yang dikeluarkan oleh *The Organisation for Economic Co-operation and Development* (OECD) mengeluarkan pedoman privasi yang banyak diterima secara luas [4], dalam wilayah hukum Republik Indonesia perlindungan data pribadi diatur dalam Undang-Undang nomor 27 tahun 2022, Undang-undang tersebut selain mendefinisikan data pribadi seperti yang disebutkan sebelumnya, mengatur secara pengelolaan data pribadi, diantaranya pengaturan hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi, hingga ketentuan pidana atas pelanggaran terhadap undang-undang tersebut.

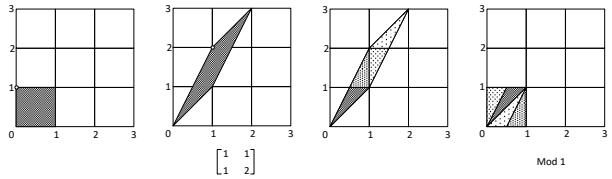
Kata kriptografi (*cryptography*) berasal dari bahasa Yunani, yang berasal dari kata *κρυπτός* (romanji *cryptós*) yang artinya "rahasia" atau "tersembunyi" dan *γράφειν* (romanji *gráphein*) yang artinya "tulisan". Jadi menurut asal katanya kriptografi artinya "tulisan rahasia" atau "tulisan tersembunyi". Tujuan mendasar dari kriptografi adalah untuk secara memadai menangani keempat bidang yaitu (1) privasi atau kerahasiaan (*privacy* or *confidentiality*) (2) integritas data (data integrity) (3) autentikasi (*authentication*) dan (4) non-repudiasi (non-*repudiation*) baik dalam teori maupun praktik [5]. Kebanyakan skema kriptografi konvensional seperti AES, DES, TDES, IDEA, RSA dirancang untuk melindungi data tekstual secara lebih efisien. Akan tetapi skema enkripsi tersebut tidak ideal untuk diterapkan pada citra digital, dikarenakan karakteristik khusus citra digital seperti kapasitas yang masal, redudansi tinggi, korelasi antar piksel yang tinggi, serta ukuran file yang relatif besar [6]. Selain itu, terkadang aplikasi citra juga memiliki prasyarat sendiri seperti pemrosesan *real-time*, mempertahankan akurasi, konsistensi format citra, dan juga kompresi untuk transmisi data [7].

Som, dkk., pada tahun 2013 mengusulkan enkripsi parsial yang mengenkripsi 4-bit MSB dari 8-bit piksel citra *grayscale* yang kemudian digabungkan Kembali dengan 4-bit LSB menjadi citra sandi, penelitian ini mengutamakan kecepatan proses enkripsi [8]. Pada tahun 2016 Ayoup, dkk. mengusulkan ESIE yang membagi citra jadi sejumlah blok, setelah seluruh blok dienkripsi, blok dengan entropi tertinggi (ROI) dilakukan proses enkripsi tambahan, tujuan dari penelitian ini adalah dengan memperkuat keamanan pada area ROI dengan proses enkripsi tambahan [9]. Sedangkan pada tahun 2022 Singh, dkk mengusulkan enkripsi citra efisien dengan menggunakan algoritma YOLO untuk mendeteksi area ROI, kemudian dari semua area ROI yang dideteksi digabungkan dari satu blok ROI yang akan dienkripsi, karena penggabungan tersebut maka area Non-ROI di antara area ROI tersebut ikut terenkripsi [10].

Sistem *chaos* adalah sistem deterministik nonlinear yang memiliki berbagai karakteristik, seperti kepekaan tinggi terhadap kondisi awal, deterministik, ergodisitas. Peta kaotis sering menghasilkan urutan *pseudorandom* yang sangat kompleks, yang sulit diprediksi atau dianalisis, yang dapat memberikan tingkat keamanan tinggi pada algoritma enkripsi [6]. Jameel, dkk. melakukan perbandingan berbagai metode enkripsi citra yang mengacu pada parameter keamanan citra antara lain sensitivitas kunci, keseragaman histogram, informasi entropi dan analisis diferensial. Dari hasil penelitian tersebut disimpulkan teknik *chaos* memiliki nilai ketidakpastian yang paling tinggi dan memberikan tingkat keamanan yang paling tinggi [11]. Selain itu metode kriptografi berbasis *chaos* juga memberikan beberapa keuntungan seperti peningkatan fleksibilitas, keamanan yang tinggi, biaya komputasi yang lebih sedikit, daya komputasi yang lebih sedikit, dan kemudahan implementasi [12]. Pada tahun 1998, Fridrich mengusulkan skema enkripsi citra berbasis chaos yang

terdiri dari dua fase, yaitu substitusi/kofusi dan difusi. Pada fase pertama dilakukan dengan permutasi posisi seluruh piksel menggunakan pemetaan *chaos* 2D atau 3D, pada fase kedua nilai piksel diubah secara berurutan, yang mana perubahan nilai piksel bergantung dari akumulasi efek piksel sebelumnya [13]. Sejak itu, banyak algoritma enkripsi citra diusulkan berdasarkan skema Fridrich, diantaranya adalah: Abdullah , dkk. menggunakan *Arnold Cat Map* pada fase konfusi dan kombinasi *Henon* dan *Logistic Map* pada fase difusi [14], Mondal, dkk. menggunakan Baker Map pada proses permutasi dan difusi [6], Abbasi, dkk. *menggunakan Non-Coupled Map Lattice*(Non-CML) pada fase permutasi dan kombinasi DNA XOR dan RNA coon pada fase difusi [15], sedangkan Maiti, dkk. menggunakan transformasi *fibonaci* pada fase permutasi dan transformasi *Tribonacci* pada fase difusi [16].

Pada tahun 1960an, dengan menggunakan gambar seekor kucing, Vladimir Arnold menunjukkan bagaimana pemetaan yang baru ditemukannya mengacak gambar menjadi pola kacau sebelum kembali lagi ke gambar awal. Sejak itu itu pemetaan tersebut dikenal sebagai *Arnold's Cat Map* (ACM) [17]. Ketika transformasi ACM diterapkan pada piksel citra digital, posisi piksel tersebut secara acak berpindah posisi, namun jika iterasi diteruskan maka posisi semua piksel akan kembali ke posisi semula secara bersamaan.

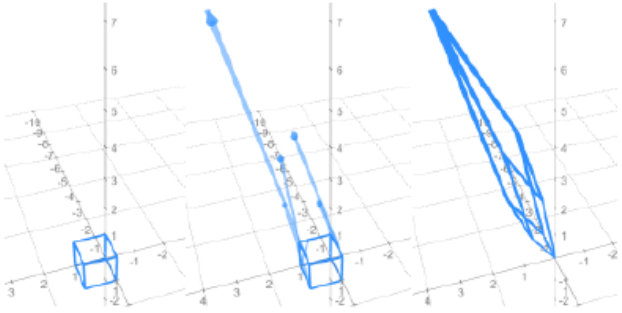


Gambar. 1 Pemetaan ACM

Pemetaan *chaos Arnold's Cat Map* (ACM) yang diperkenalkan oleh Vladimir Arnold pada tahun 1960an, banyak digunakan pada fase permutasi dari ekripsi citra berbasis chaos [9],[14],[18],[19]. Hall, pada tesis yang berjudul *Arnold'S Cat Map: An Exposition*, menyebutkan 5 sifat dasar ACM, yaitu: *Invertible*, *Diagonalizable*, *Continuous*, *Area Preserving*, dan *Ergodic* [20]. Diskrit ACM merupakan versi diskrit dari ACM dimana pemetaan bukan pada satuan kotak, tapi diperluas ke bidang N×N, sedangkan *Generalized* ACM adalah bentuk umum ACM yang mana matriks pembentuknya tidak ditentukan secara unik seperti aslinya akan tetapi berupa persamaan, yang dapat menghasilkan periode yang berbeda untuk N yang sama. Pada bidang N^2, bentuk umum ACM adalah

$$\begin{bmatrix} x_t \\ y_t \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} x_{t-1} \\ y_{t-1} \end{bmatrix} (mod\ N) \quad (1)$$

Karena determinan dari matriks bentuk umum selalu bernilai 1 (det(A)=1*(1+pq)-p*q=1+pq-pq=1), maka pemetaan bersifat area *preserving* dan periodik untuk setiap titik awal. Chen, dkk. meneliti periode untuk nilai p dan q yang berbeda pada modulus N yang sama. dari hasil percobaannya, untuk modulus N=887, terdapat 886 cat map dengan periode tertinggi 1774, dan 127584 dengan periode 888 [21]. Karena variasi periode yang cukup beragam tersebut membuat bentuk umum ACM lebih disukai dari pada pemetaan aslinya untuk diterapkan pada proses enkripsi citra digital, khususnya fase permutasi, bentuk umum ACM diterapkan untuk mengacak posisi piksel pada area N×N. Nilai p dan q digunakan pada persamaan sebelumnya untuk mengacak seluruh piksel secara bersamaan sejumlah iterasi t.



Gambar. 2 Pemetaan TCM

Linnea Fransson pada tesisnya yang berjudul *Tribonacci Cat Map : A discrete chaotic mapping with Tribonacci matrix*, tertarik dengan hubungan antara Arnold Cat Map dengan deret Fibonacci yang menimbulkan pertanyaan apakah bisa deret *Tribonacci* bisa membuat pemetaan yang sama kuat dalam 3 dimensi [22]. Hasil dari penelitian tersebut adalah *Tribonacci Cat Map* (TCM) yang dapat dijadikan alternatif adaptasi pemetaan 3 dimensi dari Arnold Cat Map. Pemetaan TCM merupakan pemetaan pada ruang N×N×N, dengan kata lain pemetaan 3D, sehingga sesuai untuk diterapkan pada fase difusi enkripsi citra digital, khususnya citra warna RGB, yang mana setiap piksel memiliki tiga kanal warna (*Red, Green, Blue*). Pada enkripsi warna, dimensi citra tidak menjadi modulus untuk enkripsi, tapi menggunakan modulus N=256, dikarenakan rentang warna yang bernilai dari 0 sampai 255. Dengan terkuncinya penggunaan modulus pada N=256, maka jika menggunakan TCM orisinal maka akan didapatkan periode 512. Oleh karena itu dengan menggunakan bentuk umum TCM berikut:,

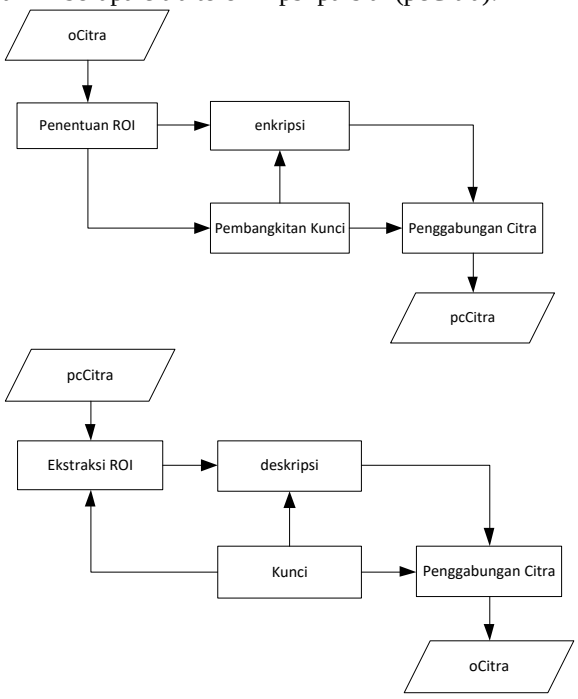
$$\begin{bmatrix} R_t \\ G_t \\ B_t \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 \\ a & a+1 & a+1 \\ a+1 & b & b+1 \end{bmatrix} \begin{bmatrix} R_{t-1} \\ G_{t-1} \\ B_{t-1} \end{bmatrix} (mod\ 256) \quad (2)$$

kita bisa mendapatkan periode yang bervariasi dengan kombinasi nilai a dan b yang berbeda. Dimana pada proses enkripsi, kanal warna (R,G,B) dari seluruh piksel diacak dengan menggunakan kunci yang berupa nilai a dan b, serta jumlah iterasi t.

III. Skema Enkripsi Parsial pada Citra Digital

Skema enkripsi yang diusulkan terbagi menjadi empat poin utama yaitu penentuan ROI dari Citra asal (oCitra) dan pembangkitan kunci, kemudian enkripsi setiap ROI (aROI) dengan menggunakan kunci yang dibangkitkan

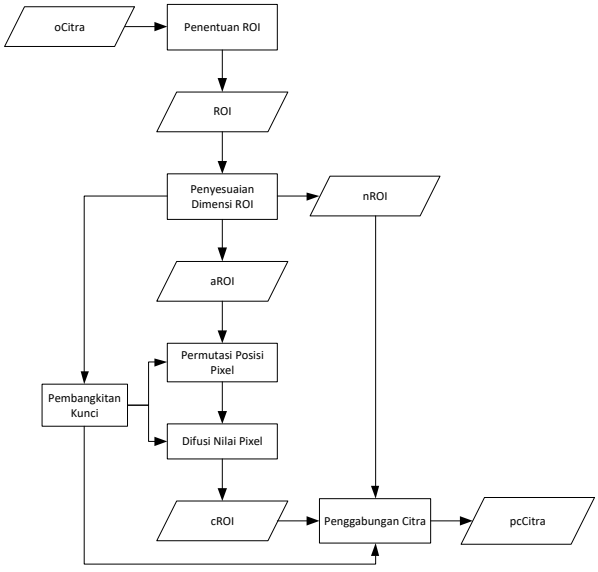
dan tahap terakhir penggabungan kembali ROI terenkripsi (cROI) dengan Non-ROI (nROI) untuk mendapatkan hasil akhir berupa citra terenkripsi parsial (pcCitra).



Gambar. 3 Proses enkripsi dan dekripsi

Untuk proses dekripsi, tahap pertama adalah ekstraksi cROI dari pcCitra menggunakan kunci pada tahap enkripsi, kemudian proses dekripsi setiap cROI dengan menggunakan kunci untuk mendapatkan aROI, tahap terakhir adalah penggabungan aROI dengan nROI untuk mendapatkan oCitra.

A. Enkripsi



Gambar. 4 Detail proses enkripsi

Proses enkripsi diawali dengan penentuan ROI dari oCitra, pada setiap ROI dilakukan pengaturan ulang ukuran menyesuaikan dengan skala yang ditentukan, tahap berikutnya adalah pembangkitan kunci untuk tahap permutasi dan difusi untuk setiap aROI, setelah itu proses enkripsi yang terdiri dari proses permutasi dan difusi pada setiap aROI dengan menggunakan kunci pada tahap sebelumnya, tahap terakhir adalah penggabungan kembali cROI dengan nROI untuk mendapatkan hasil akhir berupa citra terenkripsi parsial(pcCitra).

1) Penentuan ROI: Untuk penentuan ROI bias dilakukan dengan dua cara, pertama adalah dengan menentukan ROI secara manual, yang kedua adalah dengan menggunakan algoritma pengenalan objek seperti YOLOv3(*You Only Look Once*). Dikarenakan keterbatasan waktu, pada penelitian ini penentuan ROI dilakukan secara manual. Hasil dari proses ini adalah koordinat titik awal dan akhir untuk setiap mROI

2) Penyesuaian Dimensi ROI: Pada tahap Penyesuaian Dimensi ROI dilakukan penyesuaian dimensi ROI berdasarkan rasio antara panjang dan lebar untuk setiap ROI, dengan langkah-langkah sebagai berikut:

Algoritma 1 PenyesuaianDimensi

```
xmin  = min(ROI.awal.x , ROI.akhir.x)
ymin = min(ROI.awal.y , ROI.akhir.y)
panjang  = absolut(ROI.akhir.x - ROI.awal.x)
lebar = absolut(ROI.akhir.y - ROI.awal.y)
Nmin = min(panjang , lebar)
Nmax = max(panjang , lebar)

if Nmax <= 1.5 * Nmin then
   Nmin = Nmax
else
   Nmax = roundup( Nmax / Nmin ) *  Nmin
end if

if panjang >= lebar then
   panjang = Nmax
   lebar = Nmin
else
   panjang = Nmin
   lebar = Nmax
end if

kunci.x = xmin
kunci.y = ymin
kunci.panjang = panjang
kunci.lebar = lebar
kunci.N = Nmin

aROI.pixel(1:panjang,1:lebar)                    =
oCitra.pixel(xmin:xmin+panjang, ymin:ymin+lebar)
```

3) Pembangkitan Kunci: Setiap aROI memiliki satu set kunci yang terdiri dari 11 kunci sebagai berikut x, y, panjang, lebar, N, p, r, tp, a, b, td. Nilai x, y, panjang, lebar dan N didapat dari proses sebelumnya, sedangkan

nilai lainya didapat dengan menggunakan random number generator. Nilai p dan q yang digunakan pada proses permutasi memiliki rentang nilai {0,1,2,…,N-1}, nilai a dan b yang digunakan untuk proses difusi memiliki rentang nilai {0,1,2,…,253}, sedangkan tp dan td adalah jumlah iterasi masing-masing proses berupa nilai integer.

Algoritma 2 pembangkitanKunci

```
kunci.p = random(N-1)
kunci.r = random(N-1)
kunci.tp = random(integer)
kunci.a = random(253)
kunci.b = random(253)
kunci.td = random(integer)
```

4) Fase Permutasi: Pada fase permutasi posisi koordinat piksel aROI diacak dengan menggunakan pemetaan bentuk umum ACM dengan parameter panjang, lebar, p, q, N, dan t (tp) diambil dari set kunci, dengan mengunakan persamaan matriks (1)

Algoritma 3 permutasi

```
panjang = kunci.panjang
lebar = kunci.lebar
N = kunci.N
p = kunci.p
q = kunci.q
t = kunci.tp
A = [[1,p]
     [p,1+p*q]]
A = A ^ t
A = mod(A,N)
m = matriks[[1:N]
            [1:N][1:2]]
for i = 1 to N
   for j = 1 to N
      T = [[i,j]]
      T = mod((A * T), N)
      m(i,j) = T
   next
next
for i = 1 to panjang
   ik = floor( i / N ) * N
   for j = 1 to lebar
      jk = floor( j / N ) * N
      im = m(mod(i, N), mod(j, N), 1)
      jm = m(mod(i, N), mod(j, N), 2)
      cROI.pixel(i, j) = aROI.pixel(ik+im, jk+jm)
   next
next
```

5) Fase Difusi: Pada fase difusi nilai setiap piksel (R,G,B) pada cROI hasil permutasi diacak menggunakan bentuk umum TCM dengan parameter pajang, lebar, a, b, dan t (td) diambil dari set kunci, dengan menggunakan persamaan (2)

Algoritma 4 difusi

```
panjang = kunci.panjang
lebar = kunci.lebar
a = aROI.a
b = aROI.b
t = aROI.td

B = [ [1,1,1]
      [a,a+1,a+1]
      [a+1,b,b+1]]
B = B ^ t
B = mod(B,256)

for i = 1 to panjang
 for j = 1 to lebar
    D = cROI.piksel(i,j)
    D = mod((B * D), 256)
    cROI.pixel(i,j) = D
 next
next
```

6) Tahap Penggabungan: Tahap terakhir adalah tahap penggabungan yang mana cROI digabungkan kembali dengan oCitra pada koordinat (x,y) yang diambil dari kunci untuk menghasilkan pcCitra yang merupakan Citra yang terenkripsi parsial.

Algoritma 5 penggabungan

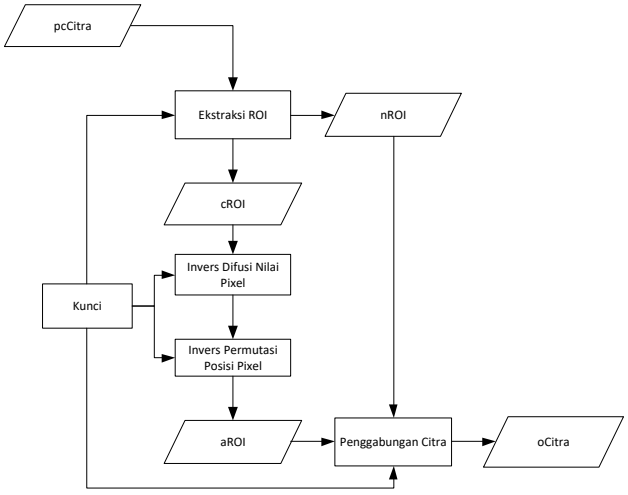
```
x = kunci.x
y = kunci.y
panjang = kunci.panjang
lebar = kunci.lebar

pcCitra = oCitra

pcCitra.pixel ( x : x + panjang, y : y + lebar ) =
cROI.pixel ( 1 : panjang , 1 : lebar )
```

Hasil akhir dari proses enkripsi adalah pcCitra yang merupakan citra terenkripsi parsial, dan sejumlah set kunci yang terdiri dari(x, y, panjang, lebar, N, p, r, tp, a, b, td) sesuai dengan jumlah cROI pada pcCitra.

B. Dekripsi



Gambar. 5 Detail proses dekripsi

Satu pcCitra bisa memiliki satu atau lebih pasangan cROI dan set kunci untuk membukanya. Proses dekripsi cROI pada pcCitra diawali dengan ekstraksi cROI

menggunakan koordinat dari set kunci cROI tersebut, kemudian cROI tersebut didekripsi menggunakan kunci dari set kunci untuk mendapatkan aROI, tahap terakhir adalah penggabungan aROI dengan pcCitra pada koordinat dari set kunci. oCitra yang merupakan citra asal bisa didapatkan jika setiap cROI pada pcCitra telah terdekripsi.

1) Ekstraksi cROI dari pcCitra: Proses ekstraksi cROI dari pcCitra, dimulai dengan mengambil komponen x, y, panjang dan lebar dari set kunci. cROI disalin dari pcCitra pada koordinat (x, y) sampai (x + panjang, y + lebar).

Algoritma 6 ekstraksi

```
x = kunci.x
y = kunci.y
panjang = kunci.panjang
lebar = kunci.lebar

cROI.pixel ( 1 : panjang , 1 : lebar ) = pcCitra.pixel
( x : x + panjang ,  y : y + lebar )
```

2) Fase Invers Difusi: Pada fase invers difusi nilai setiap piksel (R,G,B) pada cROI dikembalikan ke nilai asal dengan menggunakan bentuk umum TCM dengan parameter pajang, lebar, a, b, dan t (td) diambil dari set kunci, dan matriks yang digunakan adalah matriks *invers* dari TCM.

Algoritma 7 invdifusi

```
panjang = kunci.panjang
lebar = kunci.lebar
a = aROI.a
b = aROI.b
t = aROI.td

iB = [[ a+1 , -1 , 0 ]
      [ a^2-ab+a+1 , b-a , -1 ]
      [ -a^2+ab-2a-1 , a-b+1 , 1 ]]
iB = iB ^ t
iB = mod(iB,256)

for i = 1 to panjang
 for j = 1 to lebar
    iD = cROI.piksel(i,j))
    iD = mod((iB * iD), 256)
    cROI.pixel(i,j) = iD #hasil invers difusi iD
dimasukan ke cROI
  next
next
```

3) Fase Invers Difusi: Pada fase *invers* difusi nilai setiap piksel (R,G,B) pada cROI dikembalikan ke nilai asal dengan menggunakan bentuk umum TCM dengan parameter pajang, lebar, a, b, dan t (td) diambil dari set kunci, dan matriks yang digunakan adalah matriks *invers* dari TCM.

Algoritma 8 invpermutasi

```
panjang = kunci.panjang
lebar = kunci.lebar
N = kunci.N
p = kunci.p
q = kunci.q
t = kunci.tp
iA = [[ 1+pq , -p ]
      [ -q , 1 ]]
iA = iA ^ t
iA = mod( iA , N )

m = matriks[ [1:N]
             [1:N]
             [1:2]]

for i = 1 to N
 for j = 1 to N
    T = [[i,j]]
    T = mod(( A * T ), N)
    m(i,j) = T
 next
next

for i = 1 to panjang
 ik = floor( i / N ) * N
 for j = 1 to lebar
    jk = floor( j / N ) * N
    im = m(mod( i, N), mod( j, N), 1)
    jm = m(mod( i, N), mod( j, N), 2)
    aROI.pixel(i,j) = cROI.pixel( ik + im, jk + jm )
 next
next
```

4) Tahap Penggabungan: Tahap terakhir adalah tahap penggabungan yang mana aROI digabungkan kembali dengan pcCitra pada koordinat (x, y) yang diambil dari kunci.

Algoritma 9 penggabungan

```
x = kunci.x
y = kunci.y
panjang = kunci.panjang
lebar = kunci.lebar

oCitra.pixel ( x : x + panjang , y : y + lebar ) =
aROI.pixel ( 1 : panjang , 1 : lebar )
```

Hasil dari proses dekripsi belum tentu berupa citra asal jika belum semua cROI didekripsi, citra asal baru bisa didapatkan jika semua cROI telah didekripsi

REFERENSI

[1] NIST, "Guide to protecting the confidentiality of personally identifiable information (pii)," Tech. Rep., 2010.

[2] Y. Rozenberg, "Challenges in pii data protection," Computer Fraud Security Bulletin, vol. 2012, pp. 5–9, 2012.

[3] "Undang-undang nomor 27 tahun 2022," 2022. [Online]. Available: https://jdih.kominfo.go.id/produk hukum/view/id/832/t/undangundang+nomor+27+tahun+2022

[4] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/9789264196391-en

[5] A. Menezes, J. Katz, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, ser. Discrete Mathematics and Its Applications. CRC Press, 1996. [Online]. Available: https://books.google.co.id/books?id=nSzoG72E93MC

[6] B. Mondal, P. Kumar, and S. Singh, "A chaotic permutation and diffusion based image encryption algorithm for secure communications," Multimedia Tools and Applications, vol. 77, 2018.

[7] Y. Mao and G. Chen, Chaos-Based Image Encryption. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 231–265. [Online]. Available: https://doi.org/10.1007/3-540-28247-5 8

[8] S. Som and S. Sen, "A non-adaptive partial encryption of grayscale images based on chaos," Procedia Technology, pp. 663–671, 2013.

[9] A. M. Ayoup, A. H. Hussein, and M. A. A. Attia, "Efficient selective image encryption," Multimedia Tools and Applications, vol. 75, p.17171–17186, 2016.

[10] K. Singh, O. Singh, N. Baranwal, and A. Singh, "An efficient chaosbased image encryption," Sustainable Energy Technologies and Assessments, vol. 53, pp. 1–10, 2022.

[11] E. A. Jameel and S. A. Fadhel, "Digital image encryption techniques: Article review," Technium: Romanian Journal of Applied Sciences and Technology, vol. 4, pp. 24–35, 2022.

[12] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security, vol. 21, pp. 917–935, 2022.

[13] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, vol. 08, no. 06, pp. 1259–1284, 1998.

[14] H. Abdullah and H. Abdulkareem, "Image encryption using hybrid chaotic map," International Conference on Current Research in Computer Science and Information Technology (ICCIT), pp. 121–125, 2017.

[15] A. A. Abbasi, M. Mazinani, and R. Hosseini, "Evolutionary-based image encryption using biomolecules and non-coupled map lattice," Optics Laser Technology, vol. 140, 2021.

[16] C. Maiti, B. C. Dhara, S. Umer, and V. Asari, "An efficient and secure method of plaintext-based image encryption using fibonacci and tribonacci transformations," IEEE Access, vol. 11, 2023.

[17] V. I. Arnold and A. Avez, "Ergodic problems in classical mechanics," 1968.

[18] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," Optik, vol. 193, 2019.

[19] Chaudhary, Nirmal, Shahi, T. Bahadur, Neupane, and Arjun, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," Journal of Imaging, vol. 8, 2022. [Online]. Available: https://www.mdpi.com/2313-433X/8/6/167

[20] G. M. C. Hall, "Arnold's cat map: An exposition (master's thesis)," Master's thesis, College of Arts and Sciences, Department of Mathematics, 2022.

[21] F. Chen, K. wo Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete arnold cat map," Theoretical Computer Science, vol. 552, pp. 13–25, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514005805

[22] L. Fransson, "Tribonacci cat map: A discrete chaotic mapping with tribonacci matrix (master's thesis)," Master's thesis, Department Of Mathematics, 2021. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-104706