ISSN 2085-4552

Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi *Chaos Map* Dan Teknik Selektif

Arinten Dewi Hidayat[1], Irawan Afrianto[2]
Teknik Informatika, Universitas Komputer Indonesia (UNIKOM), Bandung, Indonesia
arinz_jfa@email.unikom.ac.id[1], irawan.afrianto@email.unikom.ac.id[2]

Diterima 29 Mei 2017
Disetujui 16 Juni 2017

Abstract*— Many organizations use design applications to draw the products they create. The drawings are digital files that have various formats of type and size. The images sometimes have to be protected because they are secret designs, such as the design of military vehicles, weapons and other designs. In order to secure digital data, cryptography is one of the solution, including if the data to be secured in the form of digital images. Algorithms that can be used to perform cryptography in digital image one of them is chaos map using Arnold cat map, logistics map and application of selective technique. Chaos was chosen for three reasons: sensitivity to initial conditions, random behavior, and no repetitive periods. While the application of selective technique means only encrypt some elements in the image but the effect of the whole image is encrypted. Cryptography in the image is also implemented because the organization using an intranet network to deliver its design drawings from one division to another. This allows for data tapping or exploitation of digital images while inside the intranet network. So it is necessary to develop a cryptographic system on the intranet network that has the ability to secure digital images that are in the network. The results obtained from black box testing, white box and network security testing show that the built system has been able to secure digital images when sent over the organization's intranet network.

***Index Terms*—Cryptography, Image, Chaos Map Algorithm, Selective Technique, Intranet.**

I. PENDAHULUAN

Saat ini perkembangan perusahaan-perusahaan yang bergerak dibidang desain semakin meningkat. Desain-desain yang dikembangkan pun telah menggunakan aplikasi-aplikasi pengolah gambar/citra guna mempercepat dan mempermudah proses desain gambar. Sehingga gambar-gambar yang dihasilkan berupa citra digital yang memiliki format umum seperti *Bitmap* (BMP), *Joint Photographic Group Experts* (JPEG), *Graphics Interchange Format* (GIF), dan *Portable Network Graphics* (PNG) [10].

Salah satu hal dipertimbangkan oleh perusahaan-perusahaan tersebut adalah bagaimana cara untuk melindungi dan mengamankan file-file gambar desain tersebut hingga tahap produksi. Hal ini dikarenakan banyaknya terjadi penyalahgunaan serta pencurian desain-desain produk terjadi. Apalagi jika desain-desain gambar yang dihasilkan merupakan desain-desain yang bersifat rahasia, seperti desain senjata, teknologi kendaraan militer dan sebagainya. Oleh karena itu dibutuhkan suatu sistem yang dapat melindungi data gambar tersebut sehingga hanya pengguna tertentu saja yang dapat menggunakan gambar tersebut.

Kriprografi pada citra digital menjadi salah satu solusi dalam pengamanan file-file gambar, sehingga lebih terlindungi dan memiliki akses yang terbatas. Kriptografi dapat dikembangkan dengan memanfaatkan algortima-algoritma yang ada guna mengamankan data-data pada citra digital.

Solusi terhadap keamanan citra digital dari penyadapan atau serangan adalah dengan mengekripsinya. Enkripsi citra merupakan teknik untuk melindungi citra dengan cara menyandikan citra (*plain-image*) sehingga tidak dapat dikenali lagi (*chiper-image*) [1]. *Chaos* dipilih karena karakteristik yaitu sensitivitas terhadap kondisi awal, berkelakuan acak, dan tidak memiliki periode berulang. *arnold cat map* digunakan untuk mengacak susunan *pixel-pixel*, sedangkan *logistic map* digunakan sebagai pembangkit *keystream*. Adapun pendekatan teknik selektif yaitu hanya mengenkripsi sebagian elemen di dalam citra namun efeknya keseluruhan citra terenkripsi [1].

Dikarenakan posisi bagian / divisi desain dan divisi produksi letaknya berjauhan, maka organisasi menfasilitasi pengiriman citra desain tersebut menggunakan jaringan intranet. Dikarena sifat jaringan intranet yang banyak pennguna , maka citra desain yang dikirimkan melalui jaringan intranet di organisasi tersebut dilengkapi dengan kritografi pada citra-citra digital yang dikirimkan, dengan harapan data-data citra digital akan menjadi lebih aman dan terlindungi dari kegiatan-kegiatan eksploitasi yang berda di jaringan komputer.

II. LANDASAN TEORI

A. *Kriptografi*

Kriptografi adalah ilmu yang berdasarkan pada teknik matematika yang erat kaitanya dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah bukan hanya penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [5].

Proses penyandian *plainteks* menjadi *cipherteks* disebut enkripsi dan proses mengembalikai *cipherteks* menjadi *plainteks* disebut dekripsi [6].

Gambar 1. Konsep kriptogtafi

B. *Citra Digital*

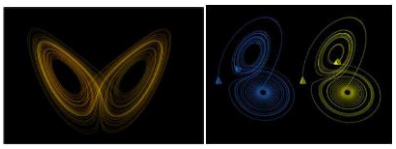
Citra digital adalah citra yang dapat diolah oleh komputer. Dalam konteks lebih luas, pengolahan citra digital mengacu pada pemrosesa setiap data dua dimensi. Citra digital merupakan sebuah larik (*array*) yang berisi nilai-nilai real maupun komplek yang direpresentasikan dengan deret bit tertentu. Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut *pixel*, yaitu elemen terkecil dari sebuah citra [10]. Salah satu bentuk citra digital adalah citra biner, yaitu citra yang hanya mempunyai dua nilai derajat keabuan: hitam dan putih. *Pixel – pixel* objek bernilai 1 dan *pixel-pixel* latar belakang bernilai 0. Pada waktu menampilkan gambar, 0 adalah putih dan 1 adalah hitam. Jadi, pada citra biner, latar belakang berwarna putih sedangkan objek berwarna hitam [11].

C. *Intranet*

Merupakan suatu konsep *Local Area Network* (LAN) yang mengadopsi teknologi internet, sehingga didalam intranet harus memiliki komponen-komponen yang membangun internet seperti protokol TCP/IP, alamat IP dan protokol lainnya, klien dan juga server [12].

D. *Chaos Map*

Teori chaos menggambarkan kebiasaan dari suatu sistem dinamis, yang keadaannya selalu berubah seiring dengan berubahnya waktu, dan sangat sensitif terhadap kondisi awal dirinya sendiri. Teori chaos ini juga sering disebut dengan sebutan *butterfly effect*.



Gambar 2. *Butterfly Effect*

Dikarenakan oleh sensitivitas yang dimiliki teori chaos terhadap keadaan awal dirinya, teori chaos memiliki sifat untuk muncul secara chaos (kacau). Bahkan perubahan keadaan awal sekecil (10^-100) saja akan membangkitkan bilangan yang benar-benar berbeda. Hal ini sangat berguna dan dapat diterapkan di dalam dunia kriptografi sebagai pembangkit kunci acak yang nantinya akan diolah sebagai sarana dalam melakukan proses enkripsi. Semakin acak bilangan yang dihasilkan, semakin baik pula tingkat keamanan dari suatu chiperteks [3].

E. *Arnold Cat Map (ACM)*

Merupakan fungsi chaos dwimatra dan bersifat reversible. Fungsi chaos ini ditemukan oleh Vladimir Arnold pada tahun 1960, dan kata “cat” muncul karena dia menggunakan citra seekor kucing dalam eksperimennya .ACM mentransformasikan koordinat (x,y) di dalam citra yang berukuran N x N ke koordinat baru (x’ ,y’). Persamaan iterasinya adalah :

$$\begin{bmatrix} X\,\text{i-1} \\ Y\,\text{i-1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} X\,\text{i} \\ Y\,\text{i} \end{bmatrix} \bmod N \qquad (1)$$

Dalam hal ini (xi , yi) adalah posisi pixel di dalam citra, (x i-1 , y i-1) posisi pixel yang baru setelah iterasi ke-I; b dan c adalah integer positif sembarang.

Determinan matriks $\begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}$ harus sama dengan 1 agar hasil transformasinya bersigat area-preserving, yaitu tetap berada di dalam area citra yang sama. ACM termasuk pemetaan yang bersifat satu ke satu karena setiap posisi pixel selalu ditransformasikan ke posisi lain secara unik. ACM diiterasikan sebanyak m kali dan setiap iterasi menghasilkan citra yang acak. Nilai b, c, dan jumlah iterasi m dapat dianggap sebagai kunci rahasia.

Proses yang terjadi di dalam setiap iterasi ACM adalah pergeseran (*shear*) dalam arah y, kemudian dalam arah x, dan semua hasilnya (yang mungkin berada di luar area gambar) dimodulokan dengan N agar tetap berada di dalam area gambar (*area preserving*) [2].

F. *Logistic Map*

Persamaan logistik merupakan contoh pemetaan polinomial derajat dua, dan seringkali digunakan sebagai contoh bagaimana rumitnya sifat chaos (kacau) yang dapat muncul dari suatu persamaan yang sangat sederhana. Persamaan ini dipopulerkan oleh seorang ahli biologi yang bernama Robert May pada

tahun 1976, melanjutkan persamaan logistik yang dikembangkan oleh Pierre Francois Verhulst.

Secara matematis, persamaan logistik dapat dinyatakan dengan persamaan:

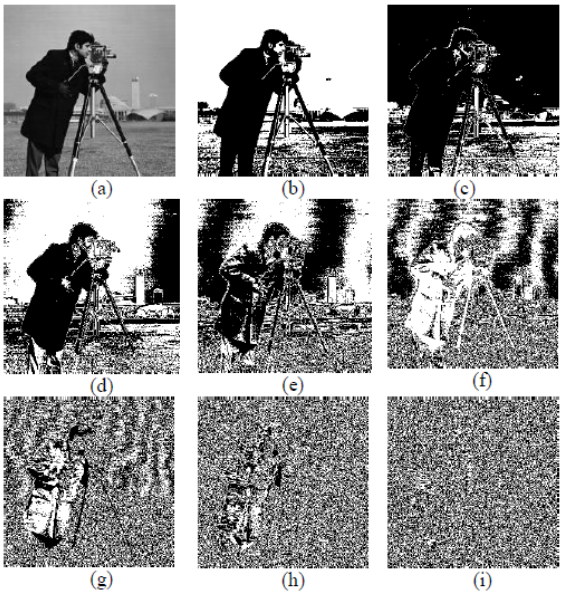
$$X_{i+1} = r_{xi} (1- xi) \quad (2)$$

nilai-nlai xi adalah bilangan riil di dalam selang (0, 1), sedangkan r adalah parameter fungsi yang menyatakan laju pertumbuhan yang nilainya di dalam selang (0, 4). Logistic Map akan bersifat chaos bilamana $0 \leq r \leq 4$. Untuk memulai iterasi Logistic Map diperlukan nilai awal x0. Perubahan sedikit saja pada nilai awal ini (misalnya sebesar 10-10) akan menghasilkan nilai-nilai chaos yang berbeda secara signifikan setelah Logistc Map diiterasi sejumlah kali. Di dalam sistem kriptografi simetri, nilai awal chaos, x0, dan parameter μ berperan sebagai kunci rahasia. Nilai-nilai acak yang dihasilkan dari persamaan (3) tidak pernah berulang kembali sehingga *logistic map* dikatakan tidak mempunyai periode [2].

G. *Enkripsi Selektif*

Pengubahan bit *Most Significant Bit* (MSB) menjadi dasar enkripsi selektif citra digital. Dengan hanya mengenkripsi bit MSB maka proses enkripsi menjadi lebih efisien, sebab tidak semua data citra dienkripsi dengan *stream cipher*.

Setiap pixel direpresentasikan dalam sejumlah byte, susunan bit pada setiap byte adalah b7 b6 b5 b4 b3 b2 b1 b0. Bit – bit paling kiri adalah bit paling berarti (MSB), sedangkan bit – bit paling kanan adalah least significant bits atau LSB. Jika setiap bit ke-1 dari setiap pixel pada citra abu-abu diekstrasi dan diplot ke dalam setiap *bitplane image* maka akan diperoleh citra seperti pada gambar 3 [4].



Gambar 3. Mekanisme Enkripsi Selektif

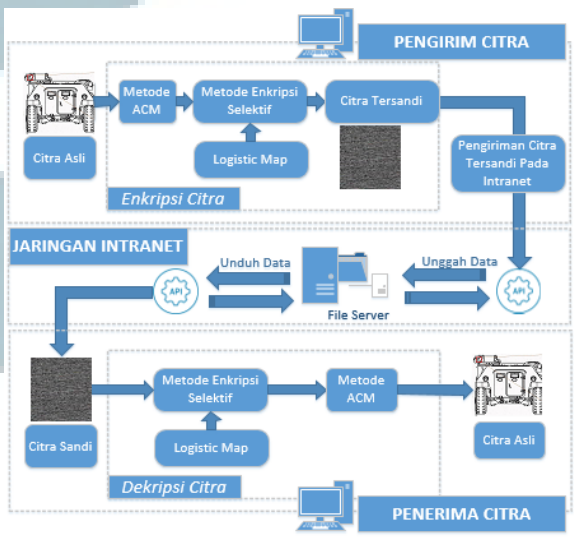
III. ANALISIS DAN PERANCANGAN SISTEM

A. *Gambaran Umum Sistem*

Sistem yang akan dibangun pada penelitian ini adalah sistem kriptografi citra digital , dimana pengirim mengirimkan gambar yang telah di enkripsi sebelumnya menggunakan algoritma *Chaos Map* dan penerapan teknik selektif, selanjutnya citra dalam bentuk *cipher image* dikirim melalui sistem jaringan intranet dan penerima citra bertugas mengembalikan *cipher image* ke bentuk semula (*plain image*).

Sistem yang dikembangkan merupakan sistem yang bekerja di lingkungan jaringan intranet organisisasi, dimana antara divisi desain dan divisi produksi berada pada lokasi yang berjauhan sehingga membutuhkan suatu akses jaringan komputer intranet guna memfasilitasi pengiriman data citra desain yang diperlukan.

Aplikasi pada sisi pengirim citra melakukan enkripsi pada citra yang akan dikirimkan dan meneruskannya (unggah file) ke server jaringan intranet melalui suatu API (*Application Programming Interface*). Sementara pada sisi penerima citra , melakukan proses unduh menggunakan API guna mendapatkan data citra yang dikirm dan melakukan proses dekripsi guna dapat melaihat citra asli yang dikirimkan. Ilustrasi sistem yang dibangun dapat dilihat pada gambar 4.



Gambar 4. Gambaran Umum Sistem Kriptografi

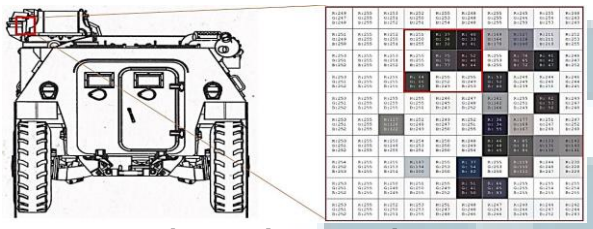
B. *Analisis Algoritma*

Analisis algoritma digunakan untuk mengetahui alur proses dari algoritma yang digunakan untuk dapat diterapkan ke dalam aplikasi yang dibangun. Pembangunan aplikasi ini menggunakan metode

kombinasi *chaos map* yaitu *arnold cat map* dan *logistic map* serta penerapan teknik selektif

C. *Analisis Algoritma Arnold Cat Map*

Pada tahap ini dilakukan operasi permutasi citra dengan ACM yang bertujuan mengacak susunan pixel-pixel di dalam citra. Berikut langkah pengacakan menggunakan citra bimau berukuran 50 x 50. Pengacakan citra dilakukan pada 9 bit tetangga yang diambil dari citra. Gambar merupakan citra dengan nilai RGB.



Gambar 5. Nilai RGB pada citra

Parameter *Arnold Cat Map* yang diinputkan m = 2, b = 2, dan c = 3, kemudian dengan transformasi ACM dan menghasilkan iterasi pertama m=1.

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} Xi \\ Yi \end{bmatrix} Mod\ (N)$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ 14 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 10 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 17 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 13 \end{bmatrix} Mod\ (3) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

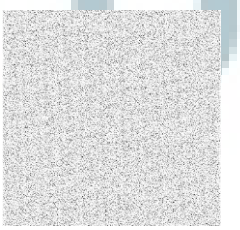
Iterasi 1

	0	1	2
0	1	5	9
1	4	8	3
2	7	2	6

Iterasi 2

	0	1	2
0	1	8	6
1	4	2	9
2	7	5	3

Hasil dari iterasi ACM pada citra dapat dilihat pada gambar 6 berikut:



Gambar 6. Hasil Iterasi ACM Pada Citra

D. *Analisis Pembangkitan Kunci Algoritma Logistic Map*

Untuk mengenkripsi bit-bit MSB dengan stream cipher diperlukan barisan bit kunci rahasia yang menjadi *keystream*. Bit-bit ini dibangkitkan dari fungsi logistic map dengan mengiterasikan persamaan (3) subbab 2.2.11. Nilai awal logistic map (x0) berperan sebagai kunci enkripsi. Namun, keluaran dari logistic map tidak dapat langsung di-XOR-kan dengan bit-bit plainteks karena masih berbentuk bilangan riil antara 0 dan 1.

X1 = 4.0x0(1-x0) = 4.0(0.456)(1 – 0.456) = 0.992256
X2 = 4.0x1(1-x1) = 4.0(0.992256)(1 – 0.992256) = 0.030736
X3 = 4.0x2(1-x2) = 4.0(0.030736)(1 – 0.030736) = 0.119166
...
X100 = 4.0x99(1-x99) = 4.0(0.914379)(1 – 0.914379) = 0.313162

Agar barisan nilai chaotik dapat dipakai untuk enkripsi dan dekripsi dengan stream cipher, maka nilai – nilai chaos tersebut dikonversikan ke nilai integer. Selanjutnya, 1 bit MSB diekstraksi dari nilai integer tersebut. Bit MSB inilah yang menjadi bit kunci untuk enkripsi.

Transformasi yang sederhana adalah dengan mengambil bagian desimal dari bilangan riil, membuang angka nol yang tidak signifikan, lalu mengekstrak t digit integer. Karena nilai-nilai pixel berada di dalam rentang integer [0,255], maka sebelum di-XOR-kan keystream di modulus-kan dengan 256. Jadi pada contoh ini ki = 4358 mod 256 = 6. Pada citra digital yang digunakan, telah mengambil 9 bit tetangga dengan nilai RGB, dan mengiterasikan persamaan ACM pada citra sehingga pixel pada citra telah teracak. Selanjutnya enkstraksi 4 bit MSB dari setiap pixel citra, nyatakan setiap 4 bit tersebut sebagai pi(i = 1, 2, 3,….,n) n = N x N.

Transformasi dengan mengambil bagian desimal dari bilangan riil, membuang angka nol yang tidak signifikan, lalu mengekstrak t digit integer. Ambil nilai desimal dan ekstrak 4 digit yang akan menjadi nilai keystream yang akan di-XOR-kan dengan pi, kemudian moduluskan dengan 256.

X1 = 0.89344 = 8934 mod 256 = 230
230 = 11100110 ; 4 Bit MSB nya adalah k1 = 1110
X2 = 0.361778 = 3617 mod 256 = 33
33 = 00100001 ; 4 Bit MSB nya adalah k2 = 0010
X3 = 0.877399 = 8773 mod 256 = 69
69 = 01000101 ; 4 Bit MSB nya adalah k3 = 0100
X4 = 0.408765 = 4087 mod 256 = 247
247 = 11110101 ; 4 Bit MSB nya adalah k4 = 1111

E. *Analisis Teknik Enkripsi Selektif*

Pixel-pixel citra di dalam struktur citra bitmap berukuran sejumlah byte. Pada citra 8-bit satu pixel berukuran 1 byte (8-bit, sedangkan pada citra 24-bit satu pixel berukuran 3 byte (24 bit). Di dalam susunan byte terdapat bit yang paling tidak berarti (LSB) dan bit yang paling berarti (MSB).

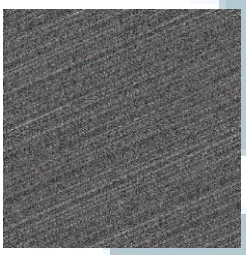
Pengubahan 1 bit LSB tidak mempengaruhi nilai byte secara signifikan, namun pengubahan 1 bit MSB dapat mengubah nilai byte secara signifikan. Secara visual efek perubahan bit-bit MSB pada seluruh pixel

citra menyebabkan citra tersebut menjadi rusak sehingga citra tidak dapat dipersepsi dengan jelas. Inilah yang menjadi dasar enkripsi citra yang bertujuan membuat citra tidak dapat dikenali lagi karena sudah berubah menjadi bentuk yang tidak jelas [4].

Tabel 1. Perubahan bit MSB

4 Bit MSB	Nilai RGB	Nilai RGB (Biner)	CI (4 Bit MSB *Chiper*)	Nilai RGB Setelah nilai 4 bit MSB diganti	Nilai RGB *Chiper*
P_1	R: 37 G: 38 B: 32	= 00100101 = 00100110 = 00100000	1100	= 11000101 = 11000110 = 11000000	R: 197 G: 198 B: 192
P_2	R: 40 G: 33 B: 41	= 00101000 = 00100001 = 00101001	0000	= 00001000 = 00000001 = 00001001	R: 8 G: 1 B: 9
P_3	R: 169 G: 164 B: 170	= 10101001 = 10101000 = 10101010	1110	= 11101001 = 11101000 = 11101010	R: 233 G: 232 B: 234

Hasil citra yang telah dienkripsi dapat dilihat pada gambar 7.

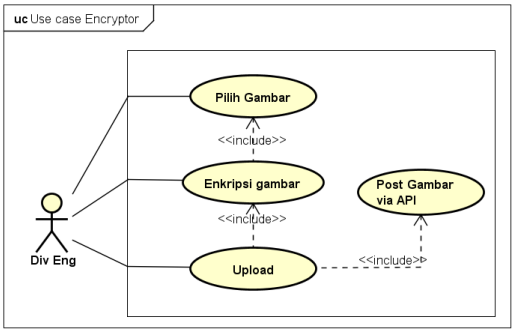


Gambar 7. Hasil Citra Yang Telah Dienkripsi

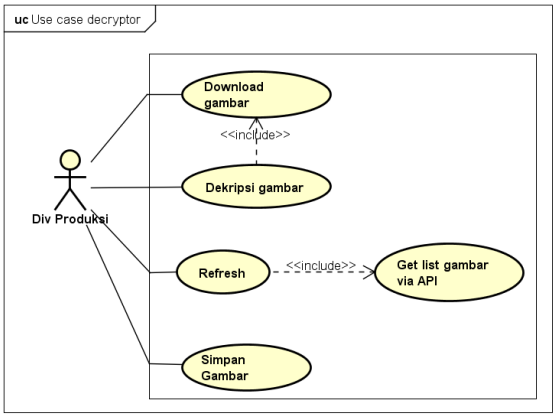
F. *Diagram Use Case*

Diagram *use case* menggambarkan suatu urutan interaksi antara satu atau lebih aktor dan sistem. Diagram use case merepresentasikan sebuah interaksi antar user sebagai aktor dengan sistem. Seseorang atau sebuah aktor adalah sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu [8].

Diagram use case dari sistem kriptografi citra digital ini terbagi menjadi 2 yaitu, diagram *use case* pada aplikasi *encryptor* (gambar 8) dan diagram *use case* pada aplikasi *decryptor* (gambar 9).



Gambar 8. Diagram Use Case *Encryptor*

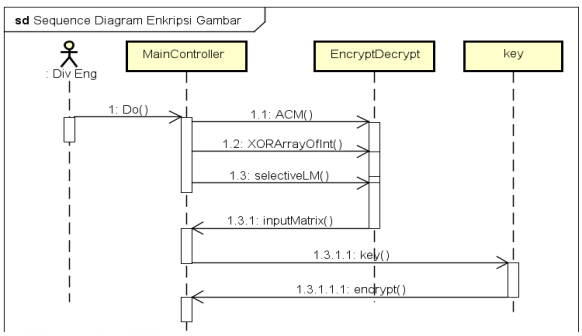


Gambar 9. Diagram Use Case *Decryptor*

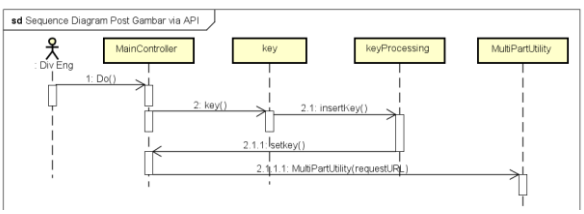
G. *Diagram Sequence*

Sequence diagram menggambarkan interaksi antar objek di dalam dan diluar sistem (termasuk pengguna, display, dan sebagainya) berupa pesan yang digambarkan terhadap waktu. *Sequence* diagram terdiri dari dimensi vertikal (waktu) dan dimensi horizontal (objek yang terkait) yang biasanya digunakan untuk menggambarkan skenario atau rangkaian langkah-langkah yang dilakukan sebagai respon dari sebuah event untuk menghasilkan output tertentu.

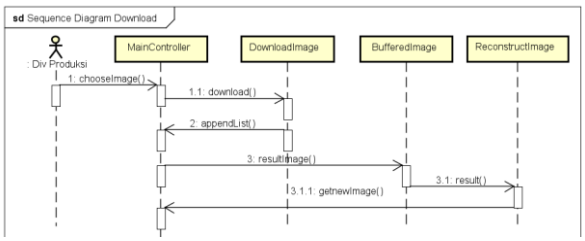
Adapun *sequence* diagram untuk enkripsi dapat dilihat pada gambar 10, *sequence* diagram kirim gambar via API pada gambar 11 dan *sequence* diagram untuk unduh dan dekripsi dapat dilihat pada gambar 12 dan 13.



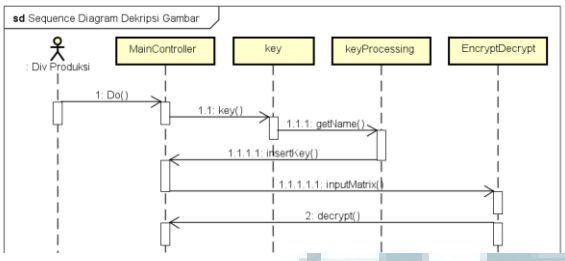
Gambar 10. *Sequence* Diagram Enkripsi Citra



Gambar 11. *Sequence* Diagram Post Citra via API



Gambar 12. *Sequence* Diagram Download Citra via API

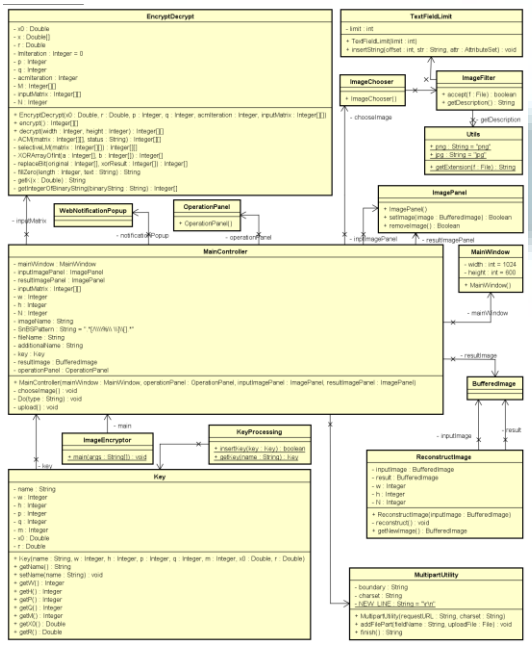


Gambar 13. *Sequence* Diagram Dekripsi Citra

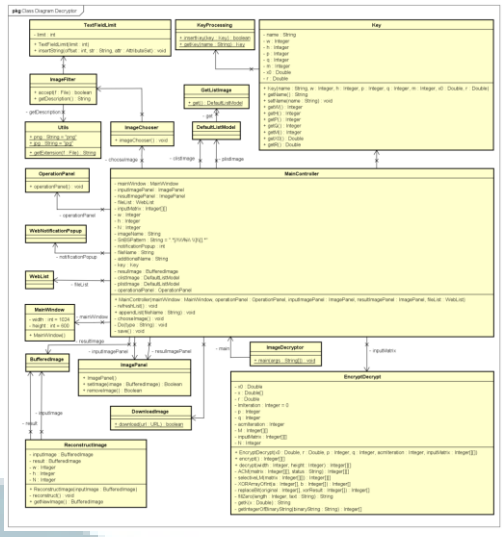
H. Diagram Class

Diagram *class* digunakan untuk menampilkan kelas-kelas dan paket-paket di dalam sistem. Diagram *class* memberikan gambaran sistem secara statis.. Diagram *class* sangat membantu dalam visualisasi struktur kelas dari suatu sistem [9].

Diagram *class* pada aplikasi sistem keamanan enkripsi citra digital terbagi menjadi 2, yaitu diagram *class* untuk *encryptor* (gambar 14) dan diagram *class* untuk *decryptor* (gambar 15).



Gambar 14. Diagram Class *Encryptor*



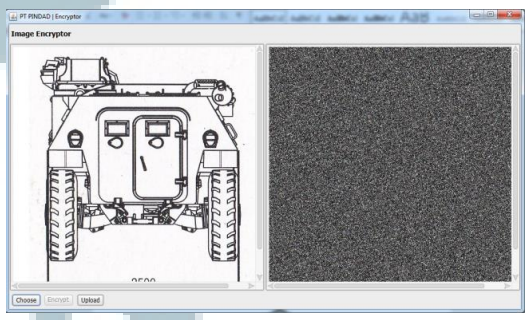
Gambar 15. Diagram Class *Decryptor*

IV. IMPLEMENTASI DAN PENGUJIAN SISTEM

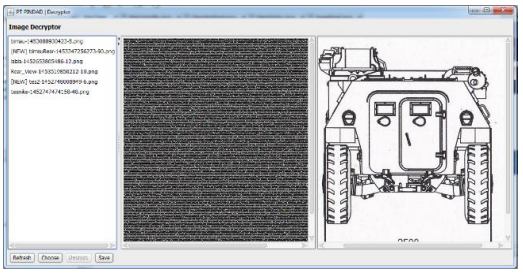
A. Implementasi

Hasil dari penelitian ini adalah sistem kritografi citra yang di*install* pada komputer pengguna, baik sebagai *encryptor* maupun *decryptor*.

Antarmuka sistem kritografi citra dapat dilihat pada gambar 16 untuk mekanisme enkripsi citra, sedangkan gambar 17 menunjukkan mekanisme dekripsi citra.



Gambar 16. Antarmuka Enkripsi Citra



Gambar 17. Antarmuka Dekripsi Citra

B. Pengujian Sistem

Setelah melakukan tahap implementasi, maka tahapan selanjutnya adalah pengujian sistem yang dibuat. Pengujian ini dilakukan untuk mengetahui

apakah rancangan dan implementasi yang telah dilakukan berjalan sesuai dengan prosedur yang diinginkan atau tidak.

B 1. Pengujian Blackbox

Pengujian *blackbox* bertujuan mengukur kinerja dari perangkat lunak apakah fungsinya dapat berjalan dengan baik atau tidak [7]. Berdasarkan rencana pengujian yang disusun, maka dilakukan pengujian seperti yang dicantumkan pada tabel 2.

Tabel 2. Pengujian *blackbox*

Aktivitas yang dilakukan	Yang diharapkan	Pengamatan	Kesimpulan
Memilih gambar yang akan di enkripsi	Gambar berhasil ditampilakn ada panel image	Berhasil Menampilkan gambar	Diterima
Mengenkripsi gambar yang telah dipilih	Menampilkan hasil enkripsi pada panel image enkripsi	Berhasil menampilkan gambar *cipher image*	Diterima
Mendekripsi gambar yang dipilih	Menampilkan gambar *cipher* pada panel image	Berhasil menampilkan *plain image*	Diterima

B.2. Pengujian Whitebox

Pengujian *whitebox* digunakan untuk mengetahui logika yang dibuat pada sebuah perangkat lunak apakah berjalan dengan baik atau tidak [7].

Pengujian *whitebox* akan digunakan pada algoritma *Chaos Map* dan teknik selektif, untuk mengukur kinerja logika berdasarkan *pseudocode* yang telah dibuat pada tahap analisis.

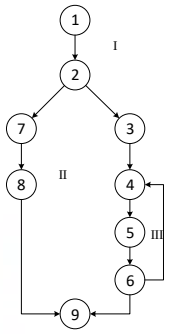
1. Langkah pertama ubah *pseudocode* menjadi *flowchart*
2. Ubah *flowchart* menjadi *flowgraph* ke dalam bentuk yang lebih sederhana.
3. Tahap pengujian, dimana tahap pengujian ini dilakukan dengan 5 cara yaitu, menghitung *region*, menghitung *cyclomatic complexity*, menghitung *independent path*, menggunakan *graph matriks*, dan menghitung *predicate node*.

Pengujian *whitebox* dimulai dengan pengujian *generate* XOR yang dilakukan pada algoritma teknik selectif yang meng-XOR-kan nilai 4-bit MSB dengan *keystream* yang dibangkitkan dari *logistic map*. Tabel 3 merupakan *source code* pengujian *generate* XOR, yang akan menghasilkan *flowgraph* pada gambar 18.

Tabel 3. *Sourcecode generate XOR*

Line	Source

```
1  Integer[] result;
2    if (a.length == b.length) {
3           result = new Integer[a.length];
4           for (int i = 0; i < a.length; i++) {
5                   result[i] = a[i] ^ b[i]; }
6           return result;
7           } else {
8           return null;
9  }
```



Gambar 18. *Flowgraph Generate XOR*

Tahap selanjutnya adalah menghitung *region* hingga *predicate note*.

Hitung Region = 3
Hitung *cyclomatic complexity* yaitu sebagai berikut:

$V_{(G)}$ = Edge – Node + 2
= 10 – 9 + 2
= 3

Berdasarkan pada hasil *cyclomatic complexity* maka didapat dua *independent path* yaitu :

Path 1 = 1-2-3-4-5-6-9
Path 2 = 1-2-7-8-9
Path 3 = 1-2-3-4-5-6-4-5-6-9

Graph matriks generate XOR dapat dilihat pada tabel 4.

Tabel 4. *Graph matriks generate XOR*

Node	1	2	3	4	5	6	7	8	9	Sum
1		1								0
2			1				1			1
3				1						0
4					1					0
5						1				0
6				1					1	1
7								1		0
8									1	0
9										0
Total										2

$V_{(G)}$ = Jumlah *Graph Matriks* + 1
= 2 + 1
= 3

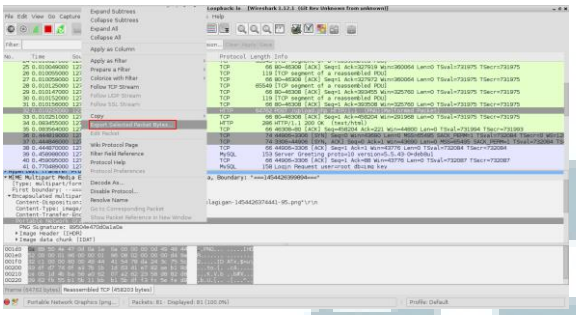
Predicate Node

$V_{(G)}$ = Jumlah node yang memiliki jalur lebih dari 1 jalur
= 2 + 1

= 3

B.3. Pengujian Keamanan Citra

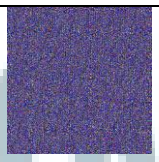
Pengujian keamanan citra terenkripsi mengunakan mekanisme *Man In The Middle Attack* (MITM) yaitu adanya komputer di intranet yang bertindak sebagai penyerang dengan menggunakan aplikasi *wireshark* untuk melakukan tindak penyadapan terhadap data citra yang dikirimkan seperti yang terlihat pada gambar 19.



Gambar 19. *Penyadapan dengan Wireshark*

Hasil yang diperoleh dari penyadapan yang dilakukan oleh aplikasi *wireshark* dapat dilihat pada tabel 5.

Tabel 5. *Pengujian Keamanan Dengan Wireshark*

Citra Uji	**Jenis**	**Pengamatan Pada Wireshark**
 Senjata.jpg	Tidak Terekripsi	
 Senjata.jpg	Terekripsi	

V. SIMPULAN

Berdasarkan hasil analisis, perancangan dan implementasi maka penelitian ini telah dapat menghasilkan hal-hal sebagai berikut.

1. Sistem keamanan citra digital yang menggabungkan algoritma chaos yaitu *arnold cat map* dan *logistik map* dan penerapan teknik selektif mampu memengkripsi citra dengan baik.
2. Pengguna aplikasi ini tidak perlu menyisipkan kunci karena sistem membangkitkan kunci bersama dengan nama yang diinputkan pada citra yang telah dienkripsi.
3. Pengujian *blackbox* menunjukkan bahwa fungsionalitas sistem berjalan dengan baik.
4. Pengujian *Whitebox* pada setiap metode, dihasilkan nilai *cyclomatic complexity* yang sama yaitu 3. Maka dapat disimpulkan bahwa pengujian *whitebox* pada proses *generate* XOR berjalan dengan baik, karena setiap pengujian menghasilkan nilai yang sama.
5. Pengujian pengiriman citra di intranet menunjukkan citra yang telah terenkripsi tidak dapat dilihat aslinya seperti halnya yang belum terenkripsi.

Sementara untuk pengembangan sistem selanjutnya, terdapat beberapa hal yang perlu dilakukan yaitu :

1. Pengembangan tampilan sistem yang lebih interaktif.
2. Citra yang akan dikirim tidak hanya satu , melainkan beberapa citra.
3. Diharapkan pada pengembangan selanjutnya algoritma chaos yang digunakan tidak hanya *arnold cat map* dan *logistic map*, melainkan beberapa algoritma chaos lainnya.

UCAPAN TERIMA KASIH

Terima kasih diucapkan kepada PT.PINDAD Bandung, yang telah bersedia menjadi mitra penelitian yang dilakukan..

DAFTAR PUSTAKA

[1] Munir, R.,. “Analisis Keamanan Algortima Enkripsi Citra Digital Menggunakan Kombinasi *Chaos Map* dan Penerapan Teknik Selektif”, Jurnal Teknik Informatika (JUTI) Vol 10, Nomor 2, 2012.

[2] Munir, R. “Algortima Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi dan Teknik Subtitusi Menggunakan *Arnold Cat Map* dan Logistic Map”., Jurnal Seminar Nasional Pendidikan Nasinal (SENAPATI 2012), 2012.

[3] Susanto, A. “Penerapan Teori Chaos di Dalam Kriptografi”. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2008-2009/Makalah2/MakalahIF3058-2009-b031.pdf. Diakses 16 Januari 2016.

[4] Munir, R. “Algoritma Enkripsi Citra Digital Dengan Kombinasi *Chaos Map* Dan Penerapan Teknik Selektif Terhadap Bit-Bit MSB”. Jurnal Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2012), 2012.

[5] Sadikin, R. “Kriptografi Untuk Keamanan Jaringan”, Yogyakarta, Penerbit Andi, 2012.

[6] Wahana Komputer. "Kriptografi Dalam Memahami Model Enkripsi Dan Security Data”, Yogyakarta, Penerbit Andi, 2003.

[7] Irwan, M. “Blackbox Testing and Whitebox Testing”, http://tkjpnup.blogspot.co.id/2013/12/black-box-testing-dan-white-box-testing.html. Diakses 14 Desember 2015.

[8] Sutopo, A.H., “Analsis dan Desain Berorintasi Objek”, Yogtyakarta, J&J Learning, 2002

[9] Irwanto, D., “Perancangan Object Oriented Software dengan UML, Yogyakarta, Penerbit Andi, 2006

[10] Kadir Abdul, Susanto Adhi, Teori dan Aplikasi Pengolahan Citra, Yogyakarta, Penerbit Andi, 2013.

[11] Munir, R., “Pengolahan Citra Digital” , Bandung, Penerbit Informatika, 2004.

[12] Nurkamid, Mukhamad. "Analisa Keefektifan Jaringan Local Area Network (intranet) Universitas Muria Kudus." *Jurnal Sains dan Teknologi* , Vol.4 no. 2 : hal.143-150, 2013.