

**IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA
DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN
METODE ARNOLD CAT MAP DAN LOGISTIC MAP**

SKRIPSI

Digunakan Sebagai Syarat Maju Ujian Diploma IV
Politeknik Negeri Malang

Oleh:
ANGGI KURNIAWAN NIM. 1341180028



**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
JUNI 2017**

**IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA
DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN
METODE ARNOLD CAT MAP DAN LOGISTIC MAP**

SKRIPSI

Digunakan Sebagai Syarat Maju Ujian Diploma IV
Politeknik Negeri Malang

Oleh:
ANGGI KURNIAWAN NIM. 1341180028



**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
JUNI 2017**

HALAMAN PENGESAHAN

IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP DAN LOGISTIC MAP

Disusun oleh:

ANGGI KURNIAWAN NIM. 1341180028

Skripsi ini telah diuji pada tanggal 8 Juni 2017

Disetujui oleh:

1. Penguji I : Dr.Eng. Cahya Rahmad,ST .,M.Kom
NIP. 19720202 200501 1 002
.....
2. Penguji II : Indra Dharma Wijaya,ST .,MMT
NIP. 19730510 200801 1 010
.....
3. Pembimbing I : Dr.Eng. Rosa Andrie A.,ST .,M.T
NIP. 19801010 200501 1 001
.....
4. Pembimbing II : Irawati Nurmala Sari,S.Kom.,M.Sc
NIP.
.....

Mengetahui,

Ketua Jurusan
Teknologi Informasi

Rudy Ariyanto, ST., MCs.
NIP. 19711110 199903 1 002

Ketua Program Studi
Teknik Informatika

Ir. Deddy Kusbianto P., M.MKom.
NIP. 19621128 198811 1 001

PERNYATAAN

Dengan ini saya menyatakan bahwa Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Malang, 8 Juni 2017

Anggi Kurniawan

ABSTRAK

Anggi Kurniawan. “Implementasi Enkripsi Dan Dekripsi Pada Citra Digital Dokumen Hasil Scan Menggunakan Metode *Arnold Cat Map* Dan *Logistic Map*”. **Pembimbing:** (1) Dr. Eng. Rosa Andrie A., S.T., M.T (2) Irawati Nurmala Sari, S.Kom., M.Sc

Skripsi, Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang, 2017.

Kemajuan Teknologi Informasi memberikan kemudahan dalam bertukar informasi dan menyimpanan informasi. Informasi selain disimpan dalam bentuk tulisan, juga dapat disimpan dalam bentuk citra digital. Pengiriman informasi melalui saluran publik seperti internet sangat rawan terhadap penyadapan. Selain itu, penyimpanan citra di dalam media *storage* rawan terhadap pengaksesan oleh pihak-pihak yang tidak memiliki otoritas. Oleh Karena itu, diperlukan keamanan pada citra digital dokumen hasil *scan*. Penelitian ini mengembangkan enkripsi citra menggunakan metode *Arnold cat map* dan *logistic map*. Keamanan dilakukan dengan cara mengacak *pixel* dengan menggunakan *Arnold Cat Map* (ACM), kemudian memilih hanya empat bit MSB dari setiap *pixel* untuk dilakukan operasi XOR dengan *keystream* yang dibangkitkan dari *Logistic Map*. Metode ini akan menghasilkan citra digital yang terenkripsi.

Analisa keamanan meliputi keberhasilan proses enkripsi dan dekripsi, sensititas kunci, kecepatan proses, tipe file penyimpanan, analisa histogram, dan analisa entropi. Analisa dilakukan untuk mengetahui tingkat keamanan yang diberikan dan bisa dikembangkan pada masa mendatang. Hasil analisa menunjukkan bahwa metode yang diterapkan dapat melakukan proses enkripsi dan dekripsi dengan baik. Hasil dekripsi memiliki kesamaan 100% dengan citra input. Kecepatan proses dipengaruhi oleh ukuran dan jumlah iterasi yang digunakan. Tipe data penyimpanan yang terbaik yaitu yang bersifat loss less. Histogram masih belum menunjukkan datar (*flat*) pada semua citra pengujian. Hasil enkripsi memiliki tingkat keamanan dari *entropy attack* sebesar 99%.

Kata Kunci : Kriptografi, Pengolahan Citra Digital, Arnold Cat Map, Logistic Map, XOR

ABSTRACT

Anggi Kurniawan. “*Implementation Encryption and Decryption for Scanned Image Document Using Arnold Cat Map and Logistic Map Method*”. ***Conseling Lecture:*** (1) **Dr. Eng. Rosa Andrie A., S.T., M.T** (2) **Irawati Nurmala Sari, S.Kom., M.Sc**

Thesis, Informatics Engineering Study Program, Department of Information Technology, State Polytechnic of Malang, 2017.

The improvement of information technology provides an ease in exchanging information. Stored in written form, information can also be stored in digital image form. Information transmitted through a public line such as internet is very vulnerable to be accessed. Aside, storing image in storage media is vulnerable to be accessed by unauthorized parties. Therefore, it is required a security in scanned image. This research develops image encryption using Arnold Cat Map and Logistic Map Method. The security is done by shuffling pixel using Arnold Cat Map (ACM), then select only four bits of MSB from every pixel to do an XOR operation by keystream generated from Logistic Map. This method will produce an encrypted scanned image.

The Security analysis includes the success of the encryption process and decryption process, key sensitivity, processing speed, file format type, histogram analysis, and entropy analysis. The analysis process is required so that one know the security level of the encrypted scanned image and so it can be developed in the future. The result of the analysis showed that the method developed can do the encryption and decryption process well. The result of decryption process has 100% equality as the original image. The process speed is affected by the size of the original image and the number of iterations used. The best file format type is loss less format type. Histogram of the encrypted image haven't showed flat diagram results on all tested images. The result of encryption has security level of entropy attack with 99% value.

Keywords : *Cryptography, Digital Image Processing, Arnold Cat Map, Logistic Map, XOR.*

KATA PENGANTAR

Puji Syukur kami panjatkan kehadirat Allah AWT atas segala rahmat dan hidayah-Nya penulis dapat menyelesaikan laporan akhir dengan judul “IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP DAN LOGISTIC MAP”. Laporan Skripsi ini penulis susun sebagai persyaratan untuk menyelesaikan studi program Diploma IV Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang.

Kami menyadari tanpa adanya dukungan dan kerja sama dari berbagai pihak, kegiatan laporan akhir ini tidak akan dapat berjalan baik. Untuk itu, kami ingin menyampaikan rasa terima kasih kepada:

1. Bapak Rudy Ariyanto, ST., M.Cs., selaku ketua jurusan Teknologi Informasi, Politeknik Negeri Malang.
2. Bapak Ir. Deddy Kusbianto P., M.MKom., selaku ketua program studi Teknik Informatika.
3. Bapak Dr. Eng. Rosa Andrie Asmara, ST., MT. dan Ibu Irawati Nurmala Sari, S.Kom., M.Sc, selaku pembimbing Skripsi.
4. Bapak dan Ibu Dosen Jurusan Teknologi Informasi Politeknik Negeri Malang yang telah memberikan bekal ilmu dan pengetahuan.
5. Kedua orang tua yang telah memberikan bimbingan, kasih sayang, semangat, nasehat, do'a, serta materi sehingga penulis dapat melanjutkan dan menyelesaikan Pendidikan di Perguruan Tinggi ini.
6. Teman-teman seperjuangan bimbingan serta seluruh teman-teman program studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang.
7. Dan seluruh pihak yang telah membantu dan mendukung lancarnya pembuatan skripsi dari awal hingga akhir yang tidak dapat kami sebutkan satu persatu.

Penulis menyadari bahwa dalam penyusunan laporan skripsi ini, masih banyak terdapat kekurangan dan kelemahan yang dimiliki penulis baik itu sistematika penulisan maupun penggunaan bahasa. Untuk itu penulis

mengharapkan saran dan kritik dari berbagai pihak yang bersifat membangun demi penyempurnaan laporan ini. Semoga Tuhan Yang Maha Esa memberikan balasan yang berlipat ganda atas semua bantuan dan dukungan yang diberikan. Semoga laporan ini berguna bagi pembaca secara umum dan penulis secara khususnya. Akhir kata, penulis ucapkan banyak terima kasih.

Malang, 8 Juni 2017

Penulis

DAFTAR ISI

	Halaman
HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN.....	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN	xiii
BAB I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan	2
1.4 Batasan Masalah	2
1.5 Sistematika Penulisan	3
BAB II. LANDASAN TEORI	5
2.1 Scanner.....	5
2.2 Enkripsi dan Dekripsi	5
2.2 Citra Digital	6
2.3 Arnold Cat Map	6
2.4 Logistic Map	7
2.5 Enkripsi Pada Metode Arnold Cat Map dan Logistic Map.....	7
2.6 Dekripsi pada Metode Arnold Cat Map dan Logistic Map.....	9
2.7 Visual Basic .NET	9
2.8 Bilinier Interpolation.....	10
2.9 Pengujian Citra.....	11
2.10 Penyimpanan Citra.....	13
BAB III. METODOLOGI PENELITIAN.....	16
3.1 Study Literatur	16
3.2 Analisa	17
3.3 Perancangan Sistem	17
3.4 Implementasi.....	19
3.5 Pengujian Sistem Analisa Hasil Laporan Akhir	20
3.6 Penarikan Kesimpulan	23
BAB IV. ANALISIS DAN PERANCANGAN	24
4.1 Dekripsi Sistem.....	24
4.2 Kebutuhan Perangkat Keras dan Perangkat Lunak.....	24
4.3 Analisa Pengguna.....	25
4.4 Batasan Sistem.....	25
4.5 Desain Sistem.....	25
4.6 Racangan User Interface	46

BAB V. IMPLEMENTASI.....	48
5.1 Pembuatan Aplikasi	48
5.2 Pembuatan Menu Utama.....	48
5.3 Pembuatan Pembangkit Kunci	50
5.4 Hasil Aplikasi.....	53
BAB VI. PENGUJIAN DAN PEMBAHASAN	55
6.1 Pengujian Sistem.....	55
6.2 Pengujian Hasil	59
BAB VII. KESIMPULAN	80
7.1 Kesimpulan	80
7.2 Saran	81
DAFTAR PUSTAKA	81
LAMPIRAN	82

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Diagram Proses Enkripsi	8
Gambar 2.2 Diagram Proses Dekripsi	9
Gambar 3.1 Langkah-Langkah Penelitian Diagram Proses Dekripsi	16
Gambar 3.2 Skema Enkripsi dan Dekripsi	18
Gambar 3.3 Pengembangan menggunakan Siklus Prototype	19
Gambar 4.1 <i>Use Case Diagram</i>	26
Gambar 4.2 <i>Flowchart</i> Enkripsi Citra.....	30
Gambar 4.3 <i>Flowchart</i> Dekripsi Citra	31
Gambar 4.4 Ilustrasi Citra Simulasi	32
Gambar 4.5 Ilustrasi Citra Simulasi Hasil Permutasi Arnold Cat Map	36
Gambar 4.6 Simulasi Hasil Citra Terenkripsi	39
Gambar 4.7 Hasil Citra Teracak.....	43
Gambar 4.8 Ilustrasi Hasil Citra Invers Permutasi Arnold Cat Map	46
Gambar 4.9 Rancang User Interface	47
Gambar 5.1 Menu Utama.....	48
Gambar 5.2 Menu Proses	49
Gambar 5.3 Tampilan Hasil <i>Generate Key</i>	51
Gambar 5.4 Tampilan <i>GroupBox Secret Key</i>	51
Gambar 5.5 Tampilan Kotak Dialog <i>Save a Secret Key</i>	52
Gambar 5.6 Tampilan Tempat File <i>Secret Key</i> Tersimpan.....	52
Gambar 5.7 Tampilan Aplikasi Enkripsi dan Dekripsi Citra.....	53
Gambar 5.7 Tampilan Hasil Enkripsi.....	54
Gambar 5.8 Tampilan Hasil Dekripsi	54
Gambar 6.1 Grafik Kecepatan Proses Berdasarkan Ukuran Citra	70
Gambar 6.2 Grafik Kecepatan Proses Berdasarkan Jumlah Iterasi	71
Gambar 6.3 Citra Uji Entropi.....	77

DAFTAR TABEL

	Halaman
Tabel 4.1 Deskripsi Use Case Diagram	26
Tabel 4.2 Nilai Piksel Pada Setiap Koordinat Pada Citra Simulasi	32
Tabel 4.3 Hasil Permutasi Arnold Cat Map	35
Tabel 4.4 Hasil Ekstraksi 4-bit MSB Pada Simulasi Enkripsi	36
Tabel 4.5 Hasil Iterasi Logistic Map	37
Tabel 4.6 Hasil Pembangkitan <i>Keystream</i>	38
Tabel 4.7 Hasil Operasi Pi XOR Ki	38
Tabel 4.8 Hasil Penggantian <i>Ci</i>	39
Tabel 4.9 Hasil Ekstraksi 4-bit MSB Pada Simulasi Dekripsi.....	40
Tabel 4.10 Hasil Iterasi Logistic Map Pada Simulasi Dekripsi	41
Tabel 4.11 Hasil Pembangkitan Keystream Pada Simulasi Dekripsi	41
Tabel 4.12 Hasil Operasi Ci XOR Ki.....	42
Tabel 4.13 Hasil Penggantian <i>Pi</i>	40
Tabel 4.14 Hasil Invers Permutasi Arnold Cat Map	46
Tabel 6.1 Pengujian Sistem.....	55
Tabel 6.2 Pengujian Pesan Error.....	57
Tabel 6.3 Citra Uji Coba	60
Tabel 6.4 Uji Coba Enkripsi Citra.....	62
Tabel 6.5 Analisa Dekripsi Citra berdasarkan tabel 6.4	65
Tabel 6.6 Hasil Uji coba Sensifitas Kunci	66
Tabel 6.7 Hasil Pengujian Kecepatan Proses	68
Tabel 6.8 Uji Coba Kecepatan Proses berdasarkan Jumlah Iterasi	70
Tabel 6.9 Hasil Pengujian Tipe Data Penyimpanan.....	72
Tabel 6.10 Analisa Penyimpanan Citra.....	73
Tabel 6.11 Pengujian Histogram.....	74
Table 6.12 Hasil Uji EntropiBerdasarkan <i>Secret Key</i>	77
Table 6.13 Hasil Uji EntropiBerdasarkaN Warna Citra.....	78

DAFTAR LAMPIRAN

- Lampiran 1 *Source Code* Aplikasi
- Lampiran 2 Lembar Bimbingan
- Lampiran 3 Lembar Persetujuan Maju Ujian
- Lampiran 4 Lembar Revisi
- Lampiran 5 Lembar Verifikasi
- Lampiran 6 Biodata Mahasiswa

BAB I. PENDAHULUAN

Bab ini berisikan tentang ide dan latar belakang penelitian. Sekaligus berisi tentang masalah yang dihadapi, batasan dalam melakukan penelitian, serta tujuan yang ingin dicapai melalui penelitian yang dilakukan.

1.1 Latar Belakang

Perkembangan Teknologi Informasi yang begitu pesat memberikan beberapa kemudahan bagi masyarakat dunia, salah satunya yaitu berbagi atau bertukar informasi. Banyak bermunculan media online seperti portal berita online, website, jejaring sosial yang dapat diakses melalui media *smartphone* semakin memudahkan pengguna untuk bertukar informasi. Proses tukar-menukar citra digitalpun menjadi semakin tinggi dan mudah. Serta penyimpanan data citra digital di internet akan terus berkembang dengan kemajuan teknologi yang ada. Terdapat beberapa instansi yang mengimplementasikan penyimpanan arsip berupa hasil *scanning* dari dokumen ke dalam bentuk citra digital. Hal tersebut sebagai sarana untuk memudahkan dalam pengarsipan dokumen di dalam sebuah komputer.

Dengan pesatnya perkembangan internet memungkinkan antar instansi dalam bertukar informasi dengan saling mengirim dokumen dalam bentuk citra digital melalui media internet. Karena dengan adanya media internet seperti *e-mail* dan media sosial lainnya, ada kemudahan yang didapat yaitu mengurangi biaya pengiriman, mempersingkat waktu pengiriman, dan bisa dilakukan kapan saja.

Disisi lain, dengan teknologi informasi yang semakin berkembang akan meningkatkan kesempatan untuk tindak kejahatan yang lebih beragam. Dengan tingkat keamanan pengguna yang minim, maka akan mempermudah pihak lain untuk mendapatkan informasi yang tersebar di internet/jaringan. Contohnya saja pengiriman citra melalui saluran publik rawan terhadap penyadapan dan penyimpanan citra di dalam media *storage* rawan terhadap pengaksesan oleh pihak-pihak yang tidak memiliki otoritas. Bahkan perangkat penyimpanan online pun bisa dibobol untuk pencurian data pengguna. Hal ini akan sangat berbahaya karena dapat disalah gunakan untuk tindak kejahatan oleh pelakunya.

Berdasarkan permasalahan diatas, kebutuhan terhadap kerahasiaan citra digital menjadi aspek yang harus dipenuhi. Penelitian ini dibuat untuk memberikan

tingkat keamanan terhadap kerahasiaan citra digital dengan teknik kriptografi pada citra digital. Metode yang digunakan pada penelitian ini menggabungkan dua fungsi *chaos* yaitu *Arnold Cat Map* dan *Logistic Map*. *Arnold Cat Map* (ACM) digunakan untuk mengacak susunan *pixel-pixel*, sedangkan *Logistic Map* digunakan sebagai pembangkit *keystream*, sehingga informasi terhadap citra digital terahasiakan. Teknik ini bisa digunakan sebelum melakukan pengiriman data yang berupa citra digital secara rahasia, maupun sebelum citra digital di unggah ke media penyimpanan online ataupun disimpan pada media *storage*. Hal ini bertujuan agar pihak ketiga tidak dapat mengetahui informasi citra yang ada dan meminimalkan kebocoran informasi yang mengakibatkan tindak kejahanatan terhadap data.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka dapat dirumuskan beberapa permasalahan sebagai berikut:

- a. Bagaimana cara mengatasi pencurian dokumen hasil *scan*?
- b. Bagaimana meningkatkan keamanan pada penyimpanan dokumen yang berbentuk citra digital?
- c. Bagaimana mencegah kebocoran informasi yang terkandung dalam dokumen yang berbentuk citra digital?

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah membuat aplikasi yang bisa digunakan untuk meningkatkan kemanan informasi pada dokumen hasil *scan* dan dapat melakukan penyimpanan citra digital secara aman dengan cara melakukan enkripsi citra digital pada dokumen menggunakan metode *Arnold Cat Map* dan *LogisticMap*.

1.4 Batasan Masalah

Batasan masalah yang diangkat dalam laporan skripsi ini dapat dipaparkan sebagai berikut:

- a. Penelitian terbatas pada citra digital dari hasil *scan* dokumen.
- b. Penilitian menggunakan metode *Arnold Cat Map* dan *Logistic Map* untuk melakukan enkripsi dan dekripsi.
- c. Penilitian menggunakan kunci simetris.

- d. Proses pengacakan menggunakan citra berbasis *bitmap*.
- e. Citra *inputan* berupa citra dengan ukuran $N \times N$.

1.5 Sistematika Penulisan

Penulisan laporan skripsi dibagi menjadi tujuh bab, yaitu:

1.5.1 Judul Laporan Akhir

Pada bagian ini memberitahukan tentang judul yang akan dibuat sebagai penelitian tentang implementasi enkripsi digital pada citra dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map* sebagai salah satu upaya pengamanan dokumen yang berbentuk citra digital.

1.5.2 BAB I. PENDAHULUAN

Bab ini berisikan uraian yang memuat tentang segala yang melatar belakangi dilakukannya pembuatan penelitian dan yang menjadi dasar permasalahan, yang terdiri atas latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metodologi, dan sistematika penulisan.

1.5.3 BAB II. LANDASAN TEORI

Pembahasan dalam bagian ini berkisar mengenai landasan teori yang menjadi referensi utama dalam melaksanakan penelitian. Teori – teori tersebut adalah teori mengenai implementasi enkripsi digital pada citra dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map*.

1.5.4 BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan dan menguraikan tentang metodologi yang digunakan penulis dalam mengimplementasikan aplikasi enkripsi dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map* serta pengujian yang dilakukan untuk mencapai tujuan penelitian.

1.5.5 BAB IV. ANALISIS DAN PERANCANGAN

Bab ini menjelaskan dan menguraikan tentang analisa dan perencanaan pembuatan keseluruhan aplikasi dan penelitian yang dilakukan, serta melakukan analisa hasil yang didapat.

1.5.6 BAB V. IMPLEMENTASI

Bab ini menjelaskan tentang bagaimana aplikasi dibuat dan berjalan berdasarkan analisa dan perancangan yang dilakukan sebelumnya. Dimana aplikasi diharapkan dapat melakukan enkripsi dan dekripsi citra digital pada citra dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map* dengan baik.

1.5.7 BAB VI. PENGUJIAN DAN PEMBAHASAN

Bab ini berisikan tentang tampilan yang diusulkan seperti form input dan output dalam aplikasi yang mengimplementasikan enkripsi digital pada citra dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map*. Selain itu dilakukan juga pembahasan tentang analisa hasil yang diperoleh dari aplikasi yang dibuat.

1.5.8 BAB VII. PENUTUP

Bab ini dibagi menjadi dua sub bab, kesimpulan yang menjawab permasalahan yang dihadapi dan saran yang berisikan solusi alternatif untuk permasalahan yang terjadi pada laporan skripsi.

1.5.9 DAFTAR PUSTAKA

Berisikan catatan semua sumber yang digunakan dalam penulisan laporan skripsi.

1.5.10 LAMPIRAN

Berisikan segala dokumen yang digunakan pada penelitian pada kegiatan penulisan skripsi.

BAB II. LANDASAN TEORI

Bab ini berisikan tentang teori yang digunakan sebagai dasar melakukan penelitian. Teori tersebut kemudian dipakai untuk mendukung pembuatan aplikasi, rancangan metode, serta pengujian yang dilakukan dalam penelitian.

2.1 Scanner

Scanner adalah sebuah alat pemindai salah satu perangkat input pada komputer, merupakan suatu alat yang berfungsi untuk menduplikat objek layaknya seperti mesin fotokopi ke dalam bentuk digital.

Scanner dapat menduplikat objek tersebut menggunakan sensor cahaya yang terdapat di dalamnya. Sensor yang terdapat pada scanner tersebut mendeteksi struktur, tulisan, dan gambar dari objek yang discan lalu dikirimkan ke komputer dalam bentuk digital [1].

Fungsi Scanner yaitu perangkat yang berkerja dengan memindahkan sebuah data atau beberapa objek yang terdapat di atas lensa scanner ke dalam memori penyimpanan komputer. Jadi jika diatas lensa scanner terdapat sebuah kertas yang berisi teks ataupun gambar, maka data tersebut akan di pindahkan ke dalam komputer dengan secara keseluruhan [2].

2.2 Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti (*unintelligible*). Karena teknik *cipher* merupakan suatu sistem yang telah siap untuk di automatisasi, maka teknik ini digunakan dalam sistem keamanan komputer dan jaringan.

Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit,

catatan penting dalam komputer, maupun password untuk mengakses sesuatu [3].

Sedangkan dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi [4].

2.2 Citra Digital

Citra digital adalah gambar dua dimensi yang ditampilkan pada layar komputer sebagai himpunan/diskrit nilai digital. Citra Digital dibentuk oleh kumpulan titik yang dinamakan piksel (*pixel* atau “*picture element*”) [5].

Sebuah citra digital dapat mewakili oleh sebuah matriks yang terdiri dari M kolom N baris, dimana perpotongan antara kolom dan baris disebut piksel (*piksel = picture element*), yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah $f(x,y)$, yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk persamaan matriks 2.1 sebagai berikut:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & \dots & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix} \quad (2.1)$$

Berdasarkan persamaan tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas $f(x,y)$, dimana harga x (baris) dan y (kolom) merupakan koordinat posisi dan $f(x,y)$ adalah nilai fungsi pada setiap titik (x,y) yang menyatakan besar intensitas citra atau tingkat keabuan atau warna dari piksel di titik tersebut. Pada proses digitalisasi (sampling dan kuantitas) diperoleh besar baris M dan kolom N hingga citra membentuk matriks $M \times N$ dan jumlah tingkat keabuan piksel G [6].

2.3 Arnold Cat Map

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.

Arnold Cat Map mentransformasikan koordinat (x, y) di dalam citra yang berukuran $N \times N$ ke koordinat baru (x', y') . Persamaan iterasinya sebagai berikut:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc + 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \quad (2.2)$$

dalam hal ini (x_i, y_i) 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. ACM termasuk pemetaan yang bersifat satu-kesatu 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 [7].

2.4 Logistic Map

Logistic Map adalah sistem *chaos* yang paling sederhana yang berbentuk persamaan iteratif sebagai berikut:

$$x_{i+1} = r x_i (1 - x_i) \quad (2.3)$$

dengan $0 \leq x_i \leq 1$, $i = 0, 1, 2, \dots$ dan $0 \leq r \leq 4$. Nilai awal (*seed*) persamaan iterasi adalah x_0 . Persamaan (3) bersifat deterministik sebab jika dimasukkan nilai x_0 yang sama maka dihasilkan barisan nilai *chaotik* (x_i) yang sama pula. Sifat algoritma *Chaos* yang paling penting adalah sensitivitasnya pada perubahan kecil nilai awal. Artinya jika terjadi perubahan nilai kunci yang digunakan, maka hasil yang didapatkan tidak akan sama [8]. *Logistic Map* ini yang berperan sebagai pembangkit *keystream*. Bit-bit MSB yang dipilih dari setiap *pixel* di XOR-kan dengan *keystream* yang panjangnya empat bit. Empat-bit *keystream* k_i diperoleh dengan teknik sebagai berikut: nilai *chaos* x_i diambil bagian desimalnya (setelah tanda koma) seukuran panjang angka (*size*) yang diinginkan kemudian diubah menjadi *integer*. Empat bit terakhir dari representasi biner *integer* itulah yang dijadikan sebagai k_i .

2.5 Enkripsi Pada Metode Arnold Cat Map dan Logistic Map

Algoritma enkripsi pada penelitian ini dapat digunakan untuk mengenkripsi citra *grayscale* maupun untuk citra berwarna. Secara garis besar algoritma enkripsi terdiri dari dua bagian. Pertama: pengacakan pixel-pixel citra dengan ACM. Kedua: enkripsi stream cipher, yaitu operasi XOR antara 4-bit *Most Significant Bit* (MSB)

dari setiap pixel dengan 4-bit *keystream*. Berikut tahapan dari proses Enkripsi pada metode *Arnold Cat Map* dan *Logistic Map* [7]:

1. *Input*: citra awal P (plain-image) berukuran N x N, p, q, m (jumlah iterasi ACM), r, x_0 .
2. Langkah-langkah dari proses enkripsi, yaitu:
 - a. Langkah pertama melakukan permutasi, yaitu mengacak pixel-pixel di dalam citra P dengan mengiterasikan ACM sejumlah m kali. Persamaan ACM adalah
$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \pmod{N} \quad (2.4)$$

Parameter *Arnold Cat Map* yaitu p, q, dan m (jumlah iterasi), berperan sebagai kunci rahasia.

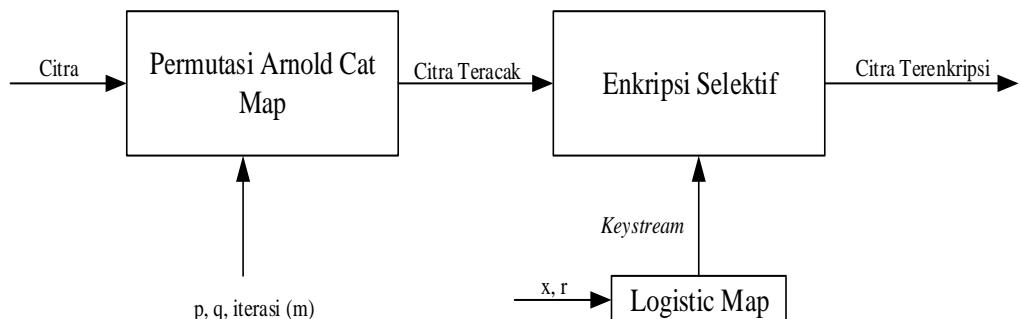
 - b. Langkah kedua Ekstraksi 4-bit *MSB* setiap *pixel* dari citra hasil langkah 1 di atas, nyatakan setiap 4-bit tersebut sebagai p_i ($i = 1, 2, \dots, n$).
Catatan: $n = N \times N$.
 - c. Iterasikan *Logistic Map* untuk memperoleh nilai-nilai *keystream* sesuai dengan paparan di dalam 2.4.
 - d. Enkripsi p_i dengan k_i menggunakan persamaan:

$$c_i = p_i \oplus k_i \quad (2.5)$$

- e. c_1, c_2, \dots, c_n selanjutnya menggantikan 4-bit *MSB* dari setiap *pixel* yang dienkripsi. Hasil enkripsi terhadap seluruh *pixel* adalah citra terenkripsi (*cipher-image*), C.

3. *Output*: citra terenkripsi C (*Cipher-Image*).

Berikut diagram proses enkripsi citra digital:



Gambar 2.1 Diagram Proses Enkripsi

2.6 Dekripsi pada Metode Arnold Cat Map dan Logistic Map

Proses Dekripsi adalah proses mengembalikan citra yang telah terenkripsi ke dalam bentuk citra asli. Berikut tahapan dari proses Dekripsi pada metode *Arnold Cat Map* dan *Logistic Map* [7]:

1. *Input*: citra terenkripsi (*cipher-image*), p, q, m (jumlah iterasi ACM), r, x_0 .
2. Langkah-langkah dari proses dekripsi, yaitu:

- a. Langkah Pertama, Ekstrasi 4-bit *MSB* setiap *pixel* dari *cipher-image* C , nyatakan setiap 4-bit tersebut sebagai c_i ($i = 1, 2, \dots, n$).

Catatan: $n = N \times N$

- b. Langkah kedua, iterasikan *Logistic Map* untuk memperoleh nilai-nilai *keystream* sesuai dengan paparan di dalam 2.4.
- c. Langkah ketiga, Dekripsi c_i dengan k_i menggunakan persamaan:

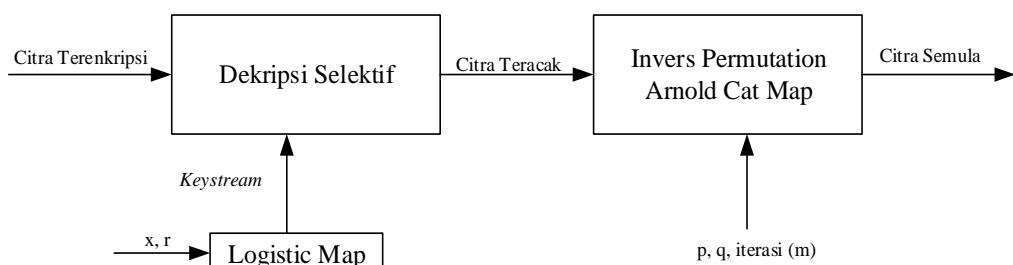
$$p_i = c_i \oplus k_i \quad (2.6)$$

- d. Langkah keempat, p_1, p_2, \dots, p_n . Selanjutnya menggantikan 4-bit *MSB* dari setiap *pixel* yang didekripsi.
- e. Langkah kelima, lakukan *inverse permutation*, yaitu menyusun kembali *pixel-pixel* citra hasil dari langkah 4 dengan persamaan *invers ACM* sebagai berikut:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(N) \quad (2.7)$$

3. *Output*: citra semula P (*plain image*).

Berikut diagram proses dekripsi citra digital:



Gambar 2.2 Diagram Proses Dekripsi

2.7 Visual Basic .NET

Microsoft .NET yang awalnya disebut dengan Next Generation Windows Service (NGWC) merupakan suatu Platform untuk membangun dan menjalankan generasi penerus aplikasi-aplikasi terdistribusi. Microsoft .NET adalah Framework

pengembangan yang menyediakan antarmuka pemrograman baru untuk layanan Windows dan API (Application Programming Interface). Dari definisi lain dari Microsoft .NET adalah strategi Microsoft untuk menghubungkan sistem, infomasi dan alat, sehingga orang dapat berkomunikasi serta berkolaborasi dengan lebih efektif. Teknologi .NET terintegrasi penuh melalui produk-produk Microsoft dan menyediakan kemampuan untuk mengembangkan solusi dengan menggunakan Web service. Platform Microsoft .NET terdiri dari lima komponen utama yang tersusun dalam tiga lapisan. Lapisan paling bawah adalah sistem operasi, lapisan kedua terdiri dari tiga komponen dan lapisan teratas adalah Visual Studio .NET.

Microsoft Visual Studio .NET yakni sebuah kumpulan lengkap dengan tools pengembangan untuk membangun sebuah aplikasi Web ASP .NET, XML Web Services, aplikasi desktop dan aplikasi mobile. Di dalam Visual Studio tersebut bahasa-bahasa pemrograman .NET seperti Visual C++, Visual C# dan Visual J#. Semuanya menggunakan lingkungan pengembangan terintegrasi atau IDE yang sama sehingga kemungkinan untuk saling berbagi tools dan fasilitas.

Visual Basic .NET yakni salah satu bahasa pemrograman yang bisa digunakan untuk membangun aplikasi-aplikasi .NET di platform Microsoft5 .NET. Tidak seperti generasi sebelumnya Visual Basic versi 6.0 ke bawah yang lebih difokuskan untuk pengembangan aplikasi desktop, Visual Basic .NET memungkinkan para pengembang membangun bermacam aplikasi, baik desktop aplikasi web. Seiring dengan perkembangan aplikasi perangkat lunak yang semakin kompleks, saat ini Visual Basic .NET memasuki versi kelima yaitu Visual Basic 2008. Meskipun demikian beberapa alasan dalam praktikum ini menggunakan Visual Basic .NET 2005.

IDE atau juga disebut dengan Integrated Design atau Development Environment merupakan perangkat lunak komputer yang berfungsi untuk membantu pemrograman dalam pengembangan perangkat lunak. Singkatnya, IDE adalah suatu lingkungan pengembangan aplikasi yang terintegrasi lengkap dengan beragam tools atau utilitas pendukung [9].

2.8 Bilinier Interpolation

Bilinear Interpolation-Interpolasi Bilinear menentukan nilai pixel baru berdasarkan rata-rata (dengan memberi bobot) dari 4 piksel dari ukuran 2×2 piksel

tetangga terdekat dalam gambar asli. Metode ini rata-rata memiliki efek anti-aliasing dan karena itu relatif mulus pada bagian tepinya dan tanpa meninggalkan kesan jaggies [10]. Jaggies adalah suatu efek bergerigi yang timbul akibat dari teknik digital yang digunakan untuk menampilkan sebuah gambar.

2.9 Pengujian Citra

Pengujian citra digunakan untuk melakukan analisa terhadap citra asli dan citra pembanding. Dengan analisa yang dilakukan, bisa dilihat perbedaan yang tampak antara citra asli dan citra pembanding. Ada beberapa cara perhitungan yang bisa dilakukan contohnya adalah dengan menggunakan perhitungan NPCR, UACI, MSE, PSNR, Entropi.

2.9.1 NPCR dan UACI

NPCR (*Number of Pixel of Change Rate*) dan UACI (*Unified Averaged Changed Intensity*) adalah salah satu perhitungan yang banyak digunakan untuk melakukan evaluasi kekuatan enkripsi citra digital dengan pendekatan perbedaan citra. Pada enkripsi citra, analisa digunakan untuk melakukan kalkulasi antara matriks piksel penyusun citra *input* dan dengan matriks piksel penyusun citra *output*. Perhitungan ini didesain untuk melakukan tes terhadap perubahan piksel dan rata-rata perubahan intensitas antara citra yang dibandingkan.

Perhitungan NPCR berfokus pada nilai absolut yang terjadi di setiap perubahan citra asli dan citra pembanding. Misal citra asli dan citra pembanding adalah C^1 dan C^2 ; Nilai *pixel* dalam citra asli dan citra pembanding dinotasikan sebagai $C^1(i,j)$ dan $C^2(i,j)$; M adalah panjang citra dan N adalah lebar citra. Rumus dari perhitungan NPCR dijabarkan dengan persamaan 2.8:

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\% \quad (2.8)$$

$$\text{with : } D(i, j) = \begin{cases} 0, & \text{if } C^1(i, j) = C^2(i, j) \\ 1, & \text{if } C^1(i, j) \neq C^2(i, j) \end{cases}$$

Perhitungan UACI berfokus pada rata-rata perbedaan antara 2 citra yang dibandingkan, yaitu citra asli dan citra pembanding. Rumus dari perhitungan UACI dijabarkan dengan persamaan 2.9:

$$UACI = \sum_{i=1}^M \sum_{j=1}^N \frac{|C^1(i, j) - C^2(i, j)|}{255 \times (M \times N)} \times 100\% \quad (2.9)$$

Nilai NPCR memiliki satuan prosentase nilai. Nilai ini mempresentasikan tingkat perbedaan *pixel* citra asli dan citra pembanding. Pada nilai 0%, maka dipastikan citra asli dan citra pembanding adalah identic, namun jika memiliki nilai, maka mulai ada perbedaan. Semakin besar nilai NPCR, maka semakin besar perbedaan citra asli dan citra pembanding.

Nilai UACI berfokus kepada prosentase perubahan citra asli dan citra pembanding. Penilaian sama dengan UACI, jika nilai adalah 0% maka dipastikan citra asli dan citra pembanding adalah identic. Jika memiliki nilai diatas 0% maka pada citra terdapat perbedaan. Semakin besar nilai, maka semakin besar pula perbedaan antara citra tersebut.

2.9.2 MSE dan PSNR

MSE (*Mean Square Error*) dan PSNR (*Peak Signal-to-Noise Ratio*) adalah perhitungan untuk menghitung error dari 2 matriks yang dibandingkan. Hal ini bertujuan untuk membantingkan kualitas dari citra yang dibandingkan. MSE merepresentasikan nilai kumulatif dari error antara citra pertama dan citra kedua. Nilai dari MSE diharapkan adalah serendah mungkin. Rumus dari perhitungan MSE dijabarkan dengan persamaan 2.10:

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (2.10)$$

Dimana nilai *pixel* dalam citra asli dan citra pembanding dinotasikan sebagai $I(i, j)$ dan $K(i, j)$. Setelah nilai MSE diketahui, maka selanjutnya bisa dilakukan perhitungan nilai psnr. Nilai psnr dihitngan dalam ukuran dB(*decibel*). Rumus dari perhitungan PSNR dijabarkan dengan persamaan 2.11:

$$PSNR = 10 \cdot \log 10 \left(\frac{MAX_I^2}{MSE} \right) \quad (2.11)$$

$$= 20 \cdot \log 10 \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (2.12)$$

$$= 20 \cdot \log 10 (MAX_I) - 10 \cdot \log 10 (MSE) \quad (2.13)$$

Dimana MAX_I adalah nilai maksimum piksel dari suatu citra. Dalam penggunaan citra 8 bit maka MAX_I bernilai 255. Dengan demikian bisa dilakukan analisa terhadap nilai pembanding dan rasio perbedaan diantara keduanya. Jika citra pembanding memiliki nilai yang identik, maka MSE akan memberikan nilai 0 dan PSNR adalah tak terbatas (*infinite* atau *undefined*). Jika citra asli dan citra pembanding tidak sama, maka akan muncul nilai pada MSE. Semakin besar nilai MSE, maka akan semakin banyak perbedaan yang terhitung. Nilai MSE tersebut kemudian dikalkulasi untuk menghitung banyak *noise* yang ada. *Noise* tersebut merupakan nilai kerusakan yang ada citra pembanding. Semakin tinggi nilai PSNR, maka semakin rendah *noise* pada citra pembanding. Jika menimbulkan nilai tak terbatas, maka citra asli dan citra pembanding dinyatakan identik.

2.9.3 Entropi

Di dalam teori informasi, entropi menyatakan derajat ketidakpastian di dalam sistem. Entropi pesan m dihitung dengan persamaan 2.14:

$$H(m) = \sum_{i=0}^{2M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (2.14)$$

yang dalam hal ini $P(m_i)$ menyatakan peluang simbol m_i di dalam pesan dan entropi dinyatakan dalam satuan bit. Pesan acak seharusnya memiliki entropi yang ideal sama dengan 8, sedangkan pada pesan yang kurang acak nilai entropinya kurang dari delapan. Jika entropi kurang dari delapan, maka terdapat derajat mampu-prediksi (*predictability*) yang merupakan ancaman bagi keamanan [12].

2.10 Penyimpanan Citra

Citra dapat disimpan dengan berbagai format. Terdapat banyak tipe penyimpanan yang dapat digunakan pada penyimpanan citra. Tentu saja semua tipe penyimpanan memiliki kelebihan dan kekurangan masing-masing sesuai dengan kegunaannya.

2.10.1 JPG

JPG atau JPEG yang merupakan kepanjangan dari *Joint Photographic Experts Assemble* biasa digunakan oleh fotografer profesional. JPG mengompres data gambar dengan mengurangi bagian-bagian dari gambar untuk memblok pixel dari suatu gambar. JPG juga biasa digunakan di internet karena bisa dikompres

hingga ukuran kecil. Data JPG tertentu bisa dikompres dengan rasio perbandingan 2:1 sampai paling tinggi 100:1, tergantung pengaturan yang kamu gunakan. Ada beberapa kekurangan yang dimiliki oleh JPG. Format JPG tidak baik jika digunakan untuk menyimpan gambar artistik karena akan menyebabkan kualitas gambar yang menurun. JPG juga bukan format gambar yang cocok untuk penggunaan tipografi, crips line, atau karya fotografer dengan sudut yang tajam karena objek menjadi blur. Namun, di balik kekurangannya, JPG juga memiliki keunggulan. File JPG akan cocok jika gambar yang ada memiliki banyak warna dan gambar yang memiliki gradien seperti perubahan warna yang perlahan-lahan dari merah ke biru [13].

2.10.2 GIFF

GIF atau *Graphics Interchange Format* merupakan salah satu format gambar yang juga umum digunakan. GIF merupakan format gambar dengan 8-bit warna, berarti mereka dibatasi oleh palet sebanyak 256 jenis warna, yang dapat dipilih dari model RGB dan disimpan ke *Color Look Up Table* (CLUT), atau sederhananya “*Color Table*“. Mereka itu sejatinya adalah palet warna standar, seperti palet. Mereka itu sejatinya adalah palet warna standar, seperti palet “*Web Safe*“. Selain bisa transparansi, GIF juga mendukung animasi gambar yang membatasi tiap formnya pada 256 warna standar. Dan karena sifatnya yang tidak pecah-pecah, GIF bisa digunakan untuk menjaga baris dalam tipografi tetap rapi, dan juga bentuk-bentuk geometri, tapi sebaiknya menggunakan format yang memang diperuntukkan untuk vektor grafis seperti SVG atau AI (Adobe Illustrator). GIF merupakan format grafis yang digunakan pada desain web di mana GIF memiliki kombinasi warna yang lebih sedikit daripada JPG, tetapi mampu menyimpan tetapi mampu menyimpan. Format GIF mendukung penggunaan multiple-bitmap dalam satu file sehingga dapat menghasilkan gambar animasi dan merekam penggunaan *Transparency Masking* [13].

2.10.3 PNG

Portable Network Graphics atau biasa kamu kenal dengan PNG merupakan salah satu alternatif format gambar untuk kepentingan internet karena PNG mendukung transparansi di dalam peramban (*browser*) dan memiliki keindahan tersendiri yang tidak bisa diberikan GIF atau bahkan JPG. PNG yang bisa dikatakan sebagai gabungan JPG dan GIF ini merupakan masuk dalam kelas 24-bit makanya

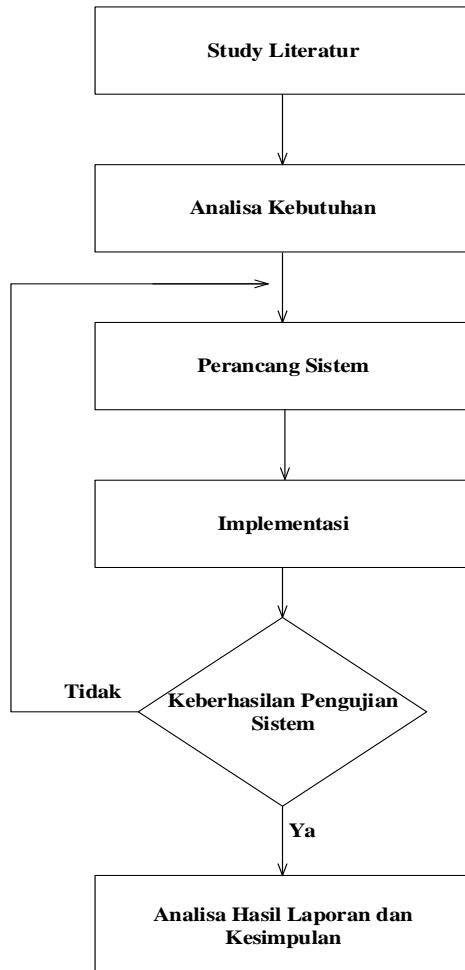
cocok untuk membuat screenshoot, sekaligus PNG juga mendukung kelas 8-bit seperti GIF, dan 24-bit seperti JPG. Format PNG ini diperkenalkan untuk menggantikan format GIF. PNG mempunyai faktor kompresi yang lebih baik dibandingkan dengan GIF (kurang lebih 5%-25% lebih baik dibanding format GIF). Tetapi ada satu fasilitas dari GIF yang tidak terdapat pada PNG format yaitu dukungan terhadap penyimpanan multi format untuk keperluan animasi [13].

2.10.4 TIFF

TIFF atau *Tagged Image Format File* merupakan format gambar terbaik dengan pengertian bahwa semua data dan informasi (data RGB, data CMYK, dan lainnya) yang berkaitan dengan koreksi atau manipulasi terhadap gambar tersebut tidak hilang. Format TIFF biasa digunakan untuk kebutuhan pencetakan dengan kualitas gambar yang sangat tinggi sehingga ukuran berkas untuk format ini biasanya sangat besar, karena dalam file ini gambar tidak dikompresi. Format ini mampu menyimpan gambar dengan kualitas hingga 32 bit. Format berkas TIFF juga dapat digunakan untuk keperluan pertukaran antar platform (PC, Macintosh, dan Silicom Graphic). Format ini juga mudah digunakan untuk transfer antar program [13].

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan langkah – langkah yang dilakukan untuk membuat Aplikasi yang mengimplementasikan enkripsi pada citra digital dokumen hasil *scan* dengan menggunakan metode *Arnold Cat Map* dan *Logistic Map*. Langkah – langkah yang diperlukan antara lain:



Gambar 3.1 Langkah-Langkah Penelitian

3.1 *Study Literatur*

Pada tahap ini penelitian dilakukan dengan mempelajari berbagai literatur melalui pengumpulan dokumen-dokumen, referensi-referensi, buku-buku, sumber dari internet, atau sumber lain yang diperlukan untuk merancang dan mengimplementasikan sistem yang berkaitan dengan penulisan skripsi yang dilakukan.

3.2 Analisa

Tujuan menganalisa antara lain menganalisa kebutuhan dan keperluan dasar yang akan digunakan dalam pembuatan aplikasi yang diinginkan. Hasil perancangan yang diperoleh adalah pembuatan aplikasi yang dapat melakukan enkripsi dan dekripsi pada citra digital menggunakan metode *Arnold Cat Map* dan *Logistic Map*.

3.3 Perancangan Sistem

Perancangan merupakan tahap untuk menggambarkan rancangan yang akan dibangun sebelum dilakukan penulisan *source code* kedalam suatu bahasa pemrograman.

Implementasi Algoritma pada aplikasi yang akan digunakan menggunakan kunci simetris. Kunci simetris adalah penggunaan kunci yang sama pada saat melakukan proses enkripsi dan pada saat proses dekripsi. Sehingga jika dimasukan kunci yang berbeda, maka tidak akan mendekripsi citra digital ke bentuk semula.

Citra yang digunakan dalam penelitian ini adalah citra RGB dengan komposisi 8 bit di tiap warnanya. Pengacakan dengan algoritma *Arnold Cat Map* akan melakukan pengacakan ketiga komponen tersebut. Hal ini dikarenakan Algoritma akan mengacak *pixel*, sehingga komponen RGB akan ikut di dalamnya. Selanjutnya enkripsi *stream cipher*, yaitu operasi XOR antara 4-bit *MSB* dari setiap *pixel* dengan 4-bit *keystream* yang dibangkitkan dari *Logistic Map*.

Adapun sistem yang dibangun hanya digunakan untuk melakukan proses enkripsi dan dekripsi. Sistem tersebut kemudian bisa digunakan untuk penyimpanan secara personal. Hasil citra terenkripsi juga bisa dikirimkan dengan media ke pihak lain, meskipun dengan keamanan yang kurang. Berikut adalah skema Enkripsi dan Dekripsi:

Pada Gambar 3.2 ada dua bagian proses yaitu Proses Enkripsi dan Dekripsi menggunakan metode *Arnold Cat Map* dan *Logistik Map*.

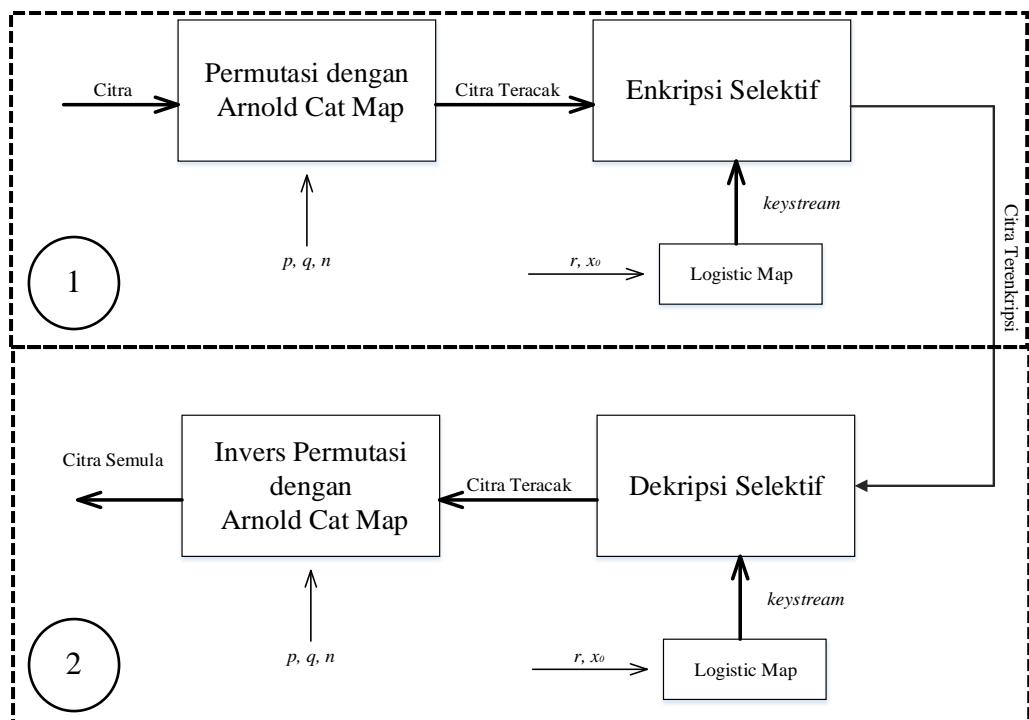
1. Proses Enkripsi

- a. Langkah awal yaitu dengan permutasi menggunakan *Arnold Cat Map* yang membutuhkan p , q , n sebagai kunci menghasilkan citra teracak.

- b. Selanjutnya Citra teracak dienkripsi selektif yang membutuhkan *keystream* yang dibangkitkan dari *Logistic Map* dengan inputan r dan x_0 sehingga akan menghasilkan Citra terenkripsi.

2. Proses Dekripsi

- Langkah awal yaitu mendekripsi selektif yang membutuhkan *keystream* yang dibangkitkan dari *Logistic Map* dengan inputan r, x_0 .
- Selanjutnya proses Invers Permutasi dengan Arnold Cat Map untuk mengembalikan posisi *pixel* semula. Pada proses ini membutuhkan p, q, n sebagai kunci sehingga akan menghasilkan citra semula.

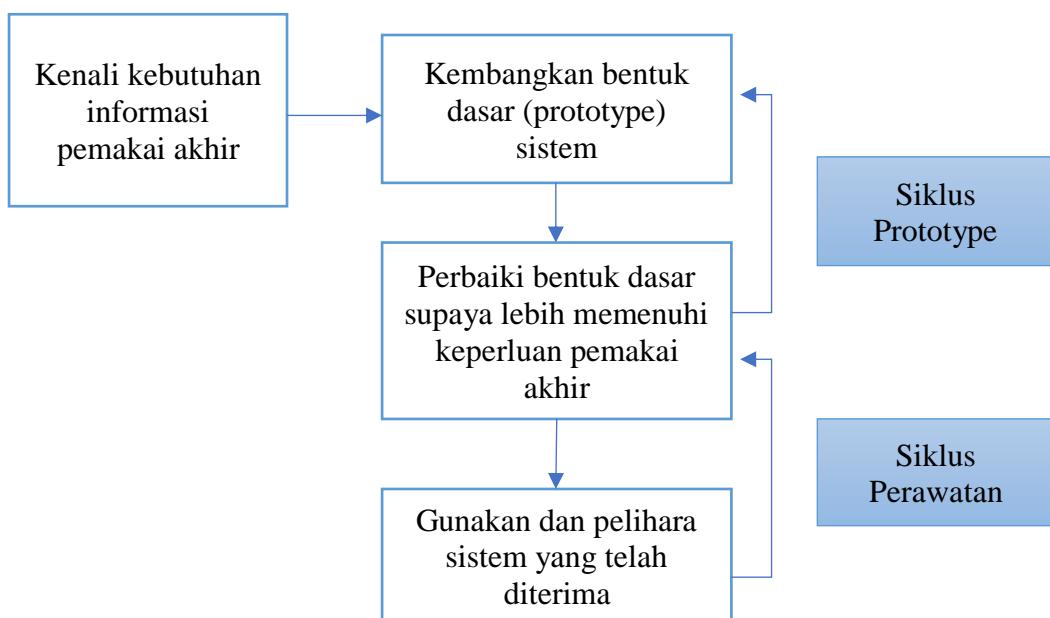


Gambar 3.2 Skema Enkripsi dan Dekripsi

Adapun pendekatan selektif artinya hanya mengenkripsi sebagian elemen di dalam citra namun efeknya keseluruhan citra terenkripsi. Kunci sebaiknya tidak dikirimkan ke pihak lain melalui saluran yang tidak aman. Pengiriman kunci dapat menggunakan saluran yang aman, contohnya dengan cara bertemu langsung atau dengan cara aman lainnya. Dengan demikian, diharapkan agar citra tidak berkoneksi dengan kuncinya secara langsung, sehingga meskipun terdapat pencurian di dalam saluran yang tidak aman, kunci akan aman karena disimpan atau dikirimkan melewati saluran yang aman.

3.4 Implementasi

Implementasi enkripsi dan dekripsi pada citra digital dokumen hasil *scan* menggunakan metode arnold cat map dan logistic map mengacu kepada metode Prototype. Metode *prototype* adalah pengembangan yang cepat dan pengujian terhadap hasil produk (*prototype*) dari aplikasi yang dibangun. Kemudian dikembangkan melalui proses interaksi dan berulang-ulang oleh para ahli sistem informasi dan ahli bisnis. *Prototype* disebut juga dengan desain aplikasi cepat (*rapid application design/RAD*) karena menyederhanakan dan mempercepat desain sistem (O'Brien, 1999:100).



Gambar 3.3 Pengembangan menggunakan Siklus Prototype

Pembangunan sistem informasi memerlukan penyelidikan dan analisis mengenai alasan timbulnya ide atau gagasan untuk membangun dan mengembangkan sistem. Analisis dilakukan untuk melihat berbagai komponen yang dipakai sistem yang sedang berjalan meliputi *hardware*, *software*, jaringan dan sumber daya manusia. Analisis juga mendokumentasikan aktivitas sistem informasi meliputi *input*, pemrosesan, *output*, penyimpanan dan pengendalian (O'Brien, 1999:101). Gambaran pengembangan aplikasi dengan menggunakan prototyping yang diberikan oleh O'Brien (1999:101). Pada gambar 3.3 dijelaskan siklus hidup pengembangan dengan menggunakan prototype. Berikut adalah penjelasan dalam pengembangan yang dilakukan:

- Penyelidikan / Analisa. Pemakai akhir mengenali kebutuhan informasi mereka dan menaksir beberapa kemungkinan pemecahan sistem informasi cadangan.
- Analisa / Rancangan. Pemakai akhir dan/atau analisis sistem menggunakan paket pengembangan penggunaan (*application development packages*) untuk rancangan yang menarik dan menguji bentuk dasar dari bagian sistem informasi yang memenuhi kebutuhan informasi dari *end user*.
- Rancang / Penerapan. Bentuk dasar sistem informasi diuji berulangkali hingga pemakai akhir mendapatkan sistem sampai sistem dapat diterima.
- Penerapan / Pemeliharaan. Sistem informasi yang diterima dapat diubah dengan mudah setelah kebanyakan dokumentasi sistem disimpan dalam penyimpanan.

3.5 Pengujian Sistem Analisa Hasil Laporan Akhir

Pengujian dilakukan untuk memastikan bahwa sistem yang dirancang dapat berjalan seperti yang diharapkan. Strategi pengujian perangkat lunak yang digunakan yaitu:

3.5.1 Pengujian Visual

Pengujian visual digunakan untuk melihat kecocokan citra asli, citra terenkripsi, dan citra terdekripsi. Antara citra Asli dan citra terenkripsi diharuskan memiliki perbedaan yang besar, sedangkan citra asli dan citra terdekripsi diharuskan memiliki persamaan yang besar. Perhitungan untuk perbedaan hasil menggunakan rumus *Number of Pixel Change Rate (NPCR)*, yang mengindikasikan perbedaan *pixel* diantara dua citra. Rumus selanjutnya adalah *Unified Average Changing Intensity(UACI)*, yang digunakan untuk rata-rata intensitas perbedaan *pixel* dari dua citra dan berikut adalah rumus matematika dari NPCR dan UACI:

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\% \quad (3.1)$$

with : $D(i, j) = \begin{cases} 0, & \text{if } C^1(i, j) = C^2(i, j) \\ 1, & \text{if } C^1(i, j) \neq C^2(i, j) \end{cases}$

$$UACI = \sum_{i=1}^M \sum_{j=1}^N \frac{|C^1(i, j) - C^2(i, j)|}{255 \times (M \times N)} \times 100\% \quad (3.2)$$

Hasil yang dinginkan dari perhitungan NPCR adalah setinggi mungkin, sedangkan hasil dari UACI berada disekitar 33% [11].

Pengujian visual yang bisa dilakukan selanjutnya adalah menggunakan perhitungan MSE (Mean Square Error) dan perhitungan PSNR (*Peak Signal to Noise Ratio*). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra pembanding. PSNR adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. Perhitungan MSE dijabarkan dengan persamaan 3.3 dan rumus PSNR dijabarkan dengan persamaan 3.6:

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (3.3)$$

$$PSNR = 10 \cdot \log 10 \left(\frac{MAX_I^2}{MSE} \right) \quad (3.4)$$

$$= 20 \cdot \log 10 \left(\frac{MAX_I}{\sqrt{MSE}} \right) \quad (3.5)$$

$$= 20 \cdot \log 10 (MAX_I) - 10 \cdot \log 10 (MSE) \quad (3.6)$$

Hasil yang diinginkan pada pengujian MSE adalah serendah mungkin. Sedangkan nilai PSNR diharapkan memiliki nilai setinggi mungkin.

3.5.2 Pengujian Sensifitas Kunci

Keamanan adalah fungsi utama dari sistem enkripsi. Citra harus mendapatkan keamanan dari berbagai serangan pada kunci. Salah satu serangan yang memungkinkan adalah mencoba dengan berbagai kunci untuk membongkar keamanan dari citra digital. Sistem enkripsi yang baik adalah sistem yang sensitive terhadap perubahan kunci. Dengan demikian, perubahan kunci akan mengakibatkan dampak yang sangat besar dalam proses enkripsi dan dekripsi citra.

Pengujian yang dilakukan adalah dengan cara melakukan enkripsi citra dengan citra yang sama, namun dengan kunci yang berbeda. Perhitungan dengan menggunakan rumus NPCR untuk citra hasil dengan kunci pertama, dan citra hasil dengan kunci ke dua. Kemudian dilakukan dekripsi dengan pasangan kunci yang berbeda dan dilakukan perhitungan dengan rumus NPCR pada citra terdekripsi. Perhitungan dimaksudkan melihat perbedaan hasil dengan harapan memiliki hasil

yang setinggi mungkin. Dengan demikian diharapkan citra tidak akan terdekripsi dengan kunci yang berbeda.

3.5.3 Pengujian Kecepatan Proses

Pengujian kecepatan dilakukan untuk mengetahui kecepatan proses pada saat proses enkripsi maupun proses dekripsi. Parameter yang digunakan untuk pengujian adalah ukuran citra serta banyaknya jumlah iterasi. Pengujian ini dimaksudkan untuk melihat perbedaan kecepatan pada ukuran citra yang berbeda, serta kecepatan proses banyaknya jumlah iterasi yang dilakukan.

3.5.4 Pengujian Penyimpanan Citra

Pengujian penyimpanan ini dimaksudkan untuk melihat tipe data yang paling baik untuk melakukan proses penyimpanan citra terdekripsi. Seperti yang diketahui, banyak tipe penyimpanan yang bisa digunakan. Pengujian dilakukan menggunakan citra asli yang sama, kemudian dilakukan proses enkripsi. Setelah citra berhasil dienkripsi, kemudian dibuka lagi dan dilakukan proses dekripsi. Kemudian proses pengujian dilakukan dengan perhitungan untuk mengetahui perbedaan citra yang terkena serangan dengan citra asli dengan rumus NPCR. Nilai yang diharapkan dari perhitungan NPCR adalah serendah mungkin.

3.5.5 Analisa Histogram

Di dalam bidang pengolahan citra histogram memperlihatkan distribusi nilai *pixel* di dalam sebuah citra. Histogram digunakan penyerang (*attacker*) untuk melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan *pixel* di dalam histogram. Penyerang berharap nilai *pixel* yang sering muncul di dalam *plain-image* berkorelasi dengan nilai *pixel* yang sering muncul di dalam *cipher-image*. Dengan menganalisis frekuensi kemunculan nilai *pixel*, penyerang mendeduksi kunci atau *pixel-pixel* di dalam *plain-image*.

Agar penyerang tidak dapat menggunakan histogram untuk melakukan analisis frekuensi, maka histogram *plain-image* dan histogram *cipher-image* seharusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan. Oleh karena itu, histogram *cipher-image* seharusnya datar (flat) atau secara statistik memiliki distribusi (relatif) uniform. Distribusi yang (relatif) *uniform* pada *cipher-*

image adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki tingkat keamanan yang bagus [10].

3.5.6 Pengujian Entropi

Pengujian entropi dilakukan dengan cara menghitung derajat ketidakpastian dari citra hasil dekripsi, dengan persamaan Entropi sebagai berikut:

$$H(m) = \sum_{i=0}^{2M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (3.7)$$

Hasil yang diinginkan pada pengujian Entropi adalah memiliki nilai ideal sama dengan 8, Jika entropi kurang dari delapan, maka terdapat derajat mampu-prediksi (*predictability*) yang merupakan ancaman bagi keamanan.

3.6 Penarikan Kesimpulan

Pada tahap terakhir yaitu berupa analisa hasil laporan dan kesimpulan. Setelah melakukan pengujian aplikasi maka penulis akan melakukan analisa hasil laporan dan membuat kesimpulan. Kesimpulan diambil untuk menjawab rumusan masalah yang telah ditentukan.

BAB IV. ANALISIS DAN PERANCANGAN

Bab ini berisikan tentang analisa dan perancangan dalam pembuatan aplikasi. Mulai dari desain sistem sampai alur sistem yang dibangun. Bab ini juga berisikan rencana pengujian yang dilakukan dalam penelitian untuk analisa yang akan dilakukan.

4.1 Dekripsi Sistem

Aplikasi pengamanan citra digital dokumen hasil *scan* merupakan sebuah aplikasi untuk meningkatkan keamanan citra digital dokumen hasil scan dengan melakukan proses enkripsi. Aplikasi tersebut menggunakan metode *Arnold Cat Map* dan *Logistic Map*. Keamanan diawali dengan cara mengacak pixel dengan menggunakan *Arnold Cat Map* (ACM), kemudian memilih hanya empat bit MSB dari setiap *pixel* untuk dilakukan operasi XOR dengan *keystream* yang dibangkitkan dari *Logistic Map*. Metode ini akan menghasilkan citra digital yang terenkripsi.

Aplikasi ini memberikan kemudahan kepada pengguna. Pengguna mendapatkan antarmuka yang mudah dengan menyediakan beberapa tombol yang digunakan untuk melakukan setiap prosesnya. Tombol tersebut berfungsi untuk membuka citra, *generate key*, menyimpan, melakukan enkripsi citra serta melakukan dekripsi citra. Tombol *generate key* memberikan kemudahan dalam menentukan kunci rahasia secara *random*.

Aplikasi ini berbasis desktop. Bahasa pemrograman yang digunakan yaitu VB.NET. Dengan adanya aplikasi ini, diharapkan pengguna mendapatkan keamanan lebih saat mempunyai file citra yang rahasia sehingga informasi tidak bisa diketahui oleh pihak lain yang tidak memiliki kepentingan.

4.2 Kebutuhan Perangkat Keras dan Perangkat Lunak

Aplikasi memiliki kebutuhan dari perangkat keras maupun perangkat lunak yang harus dipenuhi dalam penelitian yang dilakukan.

- a. Kebutuhan Perangkat Keras
 - Komputer / Laptop
- b. Kebutuhan Perangkat Lunak
 - Visual Basic

4.3 Analisa Pengguna

Aplikasi pengamanan citra digital dokumen hasil *scan* ini digunakan untuk proses enkripsi dan dekripsi citra digital. Sistem ini hanya digunakan oleh *user*, *user* dapat melakukan antara lain:

- a. Membuka Gambar.
- b. Memasukan nilai p dan q yang merupakan parameter dari *Arnold Cat Map*.
- c. Memasukan nilai x dan r yang merupakan parameter dari *Logistic Map*.
- d. Memasukan jumlah iterasi.
- e. Melakukan Proses Enkripsi Citra
- f. Melakukan Proses Dekripsi Citra

4.4 Batasan Sistem

Pembuatan Aplikasi Enkripsi citra digital dokumen hasil scan ini memiliki batasan pada pembuatannya sebagai berikut:

- a. Aplikasi berbasis *desktop*.
- b. Menggunakan Bahasa pemrograman VB.NET.
- c. Menggunakan metode *Arnold Cat Map* untuk pengacakan *pixel*.
- d. Menggunakan metode *Logistic Map* untuk pembangkitan *keystream*.
- e. Menggunakan kunci simetris.
- f. Menggunakan citra ukuran $N \times N$ untuk melakukan proses enkripsi dan dekripsi.

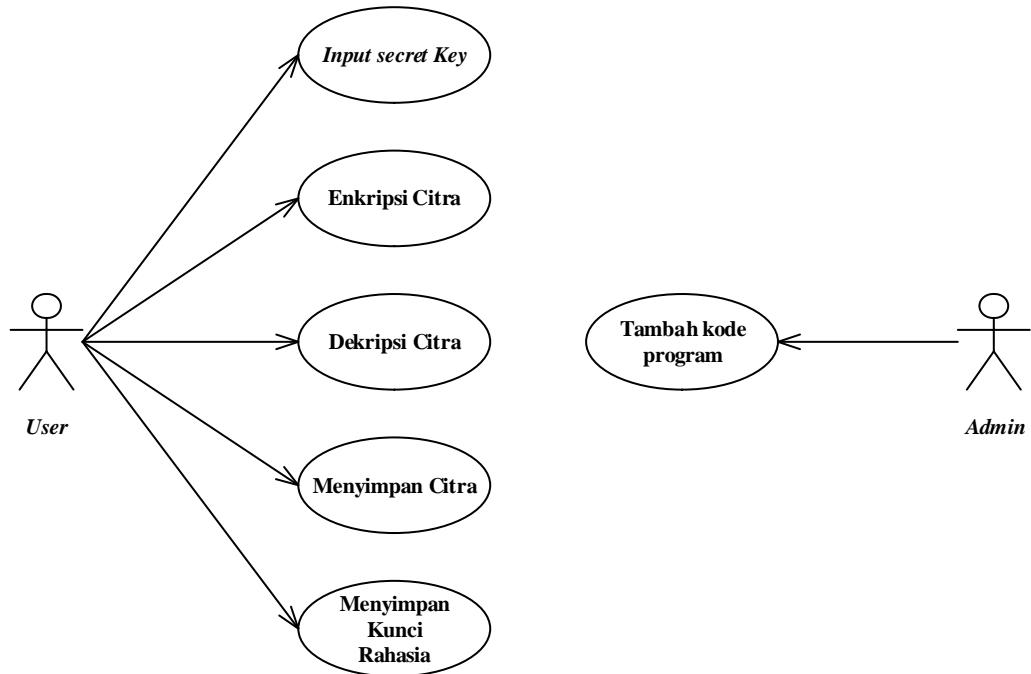
4.5 Desain Sistem

Desain sistem digunakan untuk melakukan perancangan system dari awal samai selesai. Aplikasi yang dibangun harus sesuai dengan desain yang ada dan teori pendukung untuk memperoleh aplikasi yang sesuai kebutuhan.

4.5.1 Use Case Diagram

Diagram use case digunakan untuk menggambarkan secara ringkas siapa yang menggunakan sistem dan apa saja yang bisa dilakukannya. Diagram usecase tidak menjelaskan secara detail tentang penggunaan usecase, namun hanya memberi gambaran singkat hubungan antara *usecase*, aktor, dan sistem. Melalui diagram *usecase* dapat diketahui fungsi-fungsi apa saja yang ada pada sistem (Rosa-

Salahudin, 2011: 130). Kebutuhan fungsional dari sistem dapat digambarkan dengan menggunakan *use case diagram* di bawah ini:



Gambar 4.1 Use Case Diagram

Tabel 4.1 Deskripsi Use Case Diagram

<i>Use Case Name:</i> <i>Input secret key</i>	<i>ID:</i> UC.01 <i>Siklus 1</i>	<i>Importance Level:</i> <i>High</i>		
<i>Primary Actor:</i> <i>User</i>	<i>Use Case Type:</i>			
<i>Stakeholder and Interest:</i> <i>User</i> memasukan <i>secret key</i>				
<i>Brief Description:</i> Menjelaskan proses memasukan <i>secret key</i> .				
<i>Normal flow events:</i> <ol style="list-style-type: none"> 1. <i>User</i> dapat memasukkan <i>secret key</i> secara manual atau dengan cara menekan tombol <i>generate key</i>. 				
<i>Alternative flow:</i> <ol style="list-style-type: none"> 1a. Jika <i>secret key</i> yang dimasukan tidak sesuai dengan <i>requirement</i> dari setiap <i>key</i> maka sistem akan menampilkan notifikasi. 				

<i>Use Case Name:</i> Enkripsi Citra	<i>ID:</i> UC.02 Siklus 2	<i>Importance Level:</i> <i>High</i>		
<i>Primary Actor:</i> <i>User</i>	<i>Use Case Type:</i>			
<i>Stakeholder and Interest:</i> <i>User</i> melakukan proses enkripsi citra				
<i>Brief Description:</i> Menjelaskan proses enkripsi citra.				
<i>Normal flow events:</i> <ol style="list-style-type: none"> 1. <i>User</i> memasukkan citra yang akan dienkripsi. 2. <i>User</i> memasukan kunci untuk enkripsi citra pada <i>textbox secret key</i>. 3. <i>User</i> menekan <i>menu bar “Run”</i> dan memilih menu “<i>Enkripsi</i>”. 4. Sistem melakukan proses enkripsi citra. 				
<i>Alternative flow:</i> <ol style="list-style-type: none"> 1a. Jika citra belum dimasukan, maka sistem akan menampilkan <i>notifikasi</i> bahwa citra tidak tersedia. 2.a Jika kunci tidak dimasukan, maka akan muncul notifikasi bahwa <i>secret key</i> masih belum diisi. 4a. Jika terjadi kesalahan dalam proses enkripsi, maka akan muncul notifikasi kesalahan proses. 				

<i>Use Case Name:</i> Dekripsi Citra	<i>ID:</i> UC.03 Siklus 3	<i>Importance Level:</i> <i>High</i>		
<i>Primary Actor:</i> <i>User</i>	<i>Use Case Type:</i>			
<i>Stakeholder and Interest:</i> <i>User</i> melakukan proses dekripsi citra				
<i>Brief Description:</i> Menjelaskan proses dekripsi citra.				
<i>Normal flow events:</i> <ol style="list-style-type: none"> 1. <i>User</i> memasukkan citra terenkripsi. 2. <i>User</i> memasukan kunci untuk dekripsi citra pada <i>textbox secret key</i>. 				

<p>3. User menekan <i>menu bar</i> “Run” dan memilih menu “Dekripsi”.</p> <p>4. Sistem melakukan proses dekripsi citra.</p>
<p><i>Alternative flow:</i></p> <p>1a. Jika citra belum dimasukan, maka sistem akan menampilkan <i>notifikasi</i> bahwa citra tidak tersedia.</p> <p>2.a Jika kunci tidak dimasukan, maka akan muncul notifikasi bahwa <i>secret key</i> masih belum diisi.</p> <p>4a. Jika terjadi kesalahan dalam proses dekripsi, maka akan muncul notifikasi kesalahan proses.</p>

<i>Use Case Name:</i> Menyimpan Citra	<i>ID:</i> UC.04 Siklus 4	<i>Importance Level:</i> <i>High</i>
<i>Primary Actor:</i> <i>User</i>	<i>Use Case Type:</i>	
<i>Stakeholder and Interest:</i>		
<i>User</i> melakukan penyimpanan citra		
<i>Brief Description:</i> Menjelaskan proses penyimpanan citra.		
<i>Normal flow events:</i>		
<p>1. <i>User</i> melakukan penyimpanan citra dengan cara menekan <i>menu bar</i> “File” dan memilih “save image”.</p> <p>2. <i>User</i> dapat memilih format penyimpanan citra antara lain .jpg, .png, .bmp, .gif, dan .tiff.</p>		
<i>Alternative flow:</i>		
1a. Jika citra belum tersedia, maka sistem akan menampilkan <i>notifikasi</i> bahwa citra tidak tersedia.		

<i>Use Case Name:</i> Menyimpan Kunci rahasia	<i>ID:</i> UC.05 Siklus 5	<i>Importance Level:</i> <i>High</i>
<i>Primary Actor:</i> <i>User</i>	<i>Use Case Type:</i>	

<i>Stakeholder and Interest:</i>
User melakukan penyimpanan kunci rahasia
<i>Brief Description:</i>
Menjelaskan proses penyimpanan kunci rahasia.
<i>Normal flow events:</i>
<ol style="list-style-type: none"> 1. User melakukan penyimpanan citra dengan cara menekan tombol “Save Key”. 2. User dapat memilih lokasi penyimpanan pada dialog yang muncul. 3. User memberikan nama pada file kunci rahasia yang akan disimpan
<i>Alternative flow:</i>
1a. Jika kunci rahasia belum tersedia, maka sistem akan menampilkan <i>notifikasi</i> bahwa citra tidak tersedia.

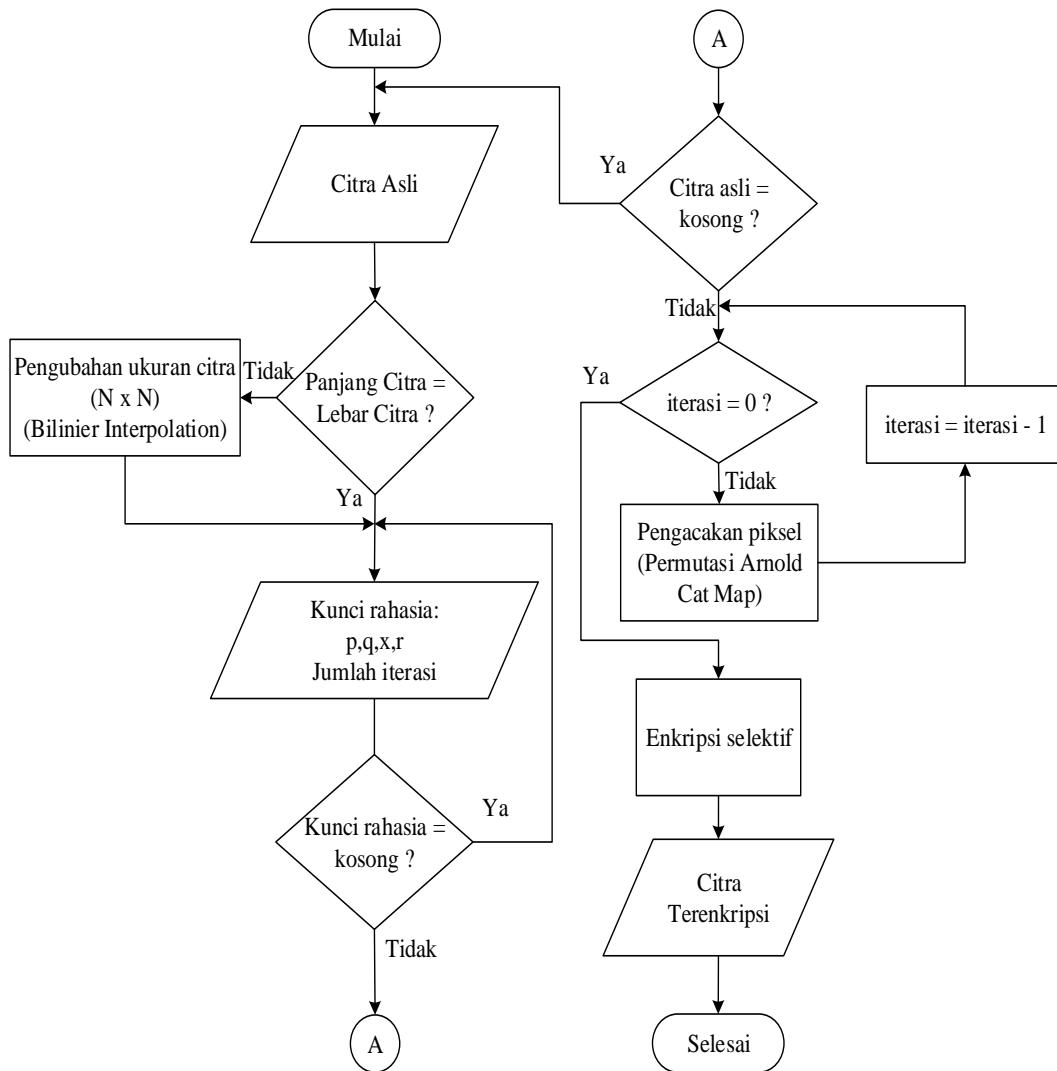
<i>Use Case Name:</i>	<i>ID:</i> UC.06	<i>Importance Level:</i>		
Tambah kode Program	Siklus 6	<i>High</i>		
<i>Primary Actor:</i>	<i>Use Case Type:</i>			
Admin				
<i>Stakeholder and Interest:</i>				
admin melakukan tambah kode program pada aplikasi.				
<i>Brief Description:</i>				
Menjelaskan proses pengembangan aplikasi.				
<i>Normal flow events:</i>				
<ol style="list-style-type: none"> 1. Admin melakukan penambahan kode program dengan menggunakan bahasa pemrograman VB.NET. 				
<i>Alternative flow:</i>				

4.5.2 Flowchart Diagram

Flowchart diagram digunakan menggambarkan bagaimana alur sistem atau untuk menunjukkan langkah-langkah (prosedur-prosedur) suatu sistem yang dibangun.

4.5.2.1 Flowchart enkripsi citra

Proses enkripsi dilakukan setelah proses konversi *bitamp* dari citra asli dan sudah mendapatkan *secret key*. *Bitmap* tersebut tersimpan ke dalam memory sehingga dapat diakses melalui perintah yang ada pada Visual Basic. Akses yang dilakukan adalah pengambilan elemen *pixel* seperti Nilai Red, Nilai Green, dan Nilai Blue pada citra. Kemudian dengan didapatnya akses tersebut, aplikasi dapat melakukan manipulasi *pixel* sesuai dengan metode yang digunakan. *Flowchart* enkripsi dapat dilihat pada gambar 4.2:



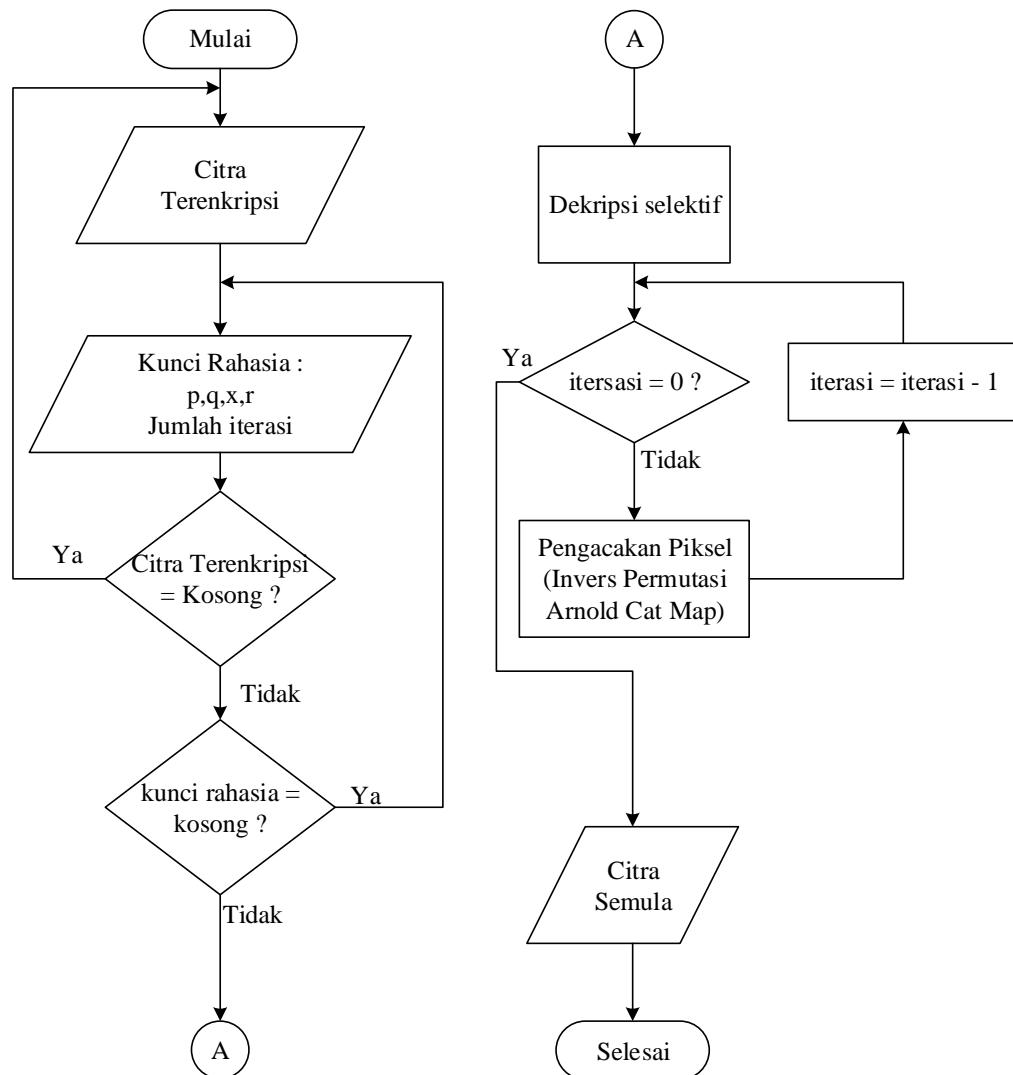
Gambar 4.2 *Flowchart* Enkripsi Citra

Pada gambar 4.2 menjelaskan tentang jalannya proses enkripsi citra. Alur dari proses enkripsi citra diawali dengan melakukan *input* citra. Jika citra yang dimasukan tidak berukuran $N \times N$ maka sistem akan melakukan *resize image*.

Selanjutnya *input* parameter yang dibutuhkan. Jika citra dan kunci masih belum dimasukan maka *user* akan diminta untuk memasukan terlebih dahulu. Proses selanjutnya sistem mengecek berapa jumlah iterasi yang akan dilakukan. Jika jumlah iterasi belum selesai atau tidak sama dengan 0 maka akan dilakukan proses pengacakan *pixel* dengan permutasi *Arnold Cat Map*. Proses diulang sampai iterasi selesai. Kemudian dilakukan enkripsi selektif dengan cara melakukan proses XOR dari 4-bit *MSB* setiap *pixel* dari citra dengan *keystream* yang di bangkitkan dari *Logistic Map*. Hasil dari proses tersebut adalah citra yang terenkripsi.

4.5.2.2 Flowchart dekripsi citra

Proses dekripsi dilakukan setelah proses konversi *bitmap* dari citra terenkripsi dan mendapatkan *secret key* yang sama dengan saat proses enkripsi. *Flowchart* dekripsi dapat dilihat pada gambar 4.3:



Gambar 4.3 Flowchart Dekripsi Citra

Pada gambar 4.3 2 menjelaskan tentang jalannya proses dekripsi citra. Alur dari proses dekripsi citra diawali dengan melakukan *input* citra terenkripsi dan parameter yang di butuhkan. Jika citra terenkripsi dan kunci masih belum dimasukan maka *user* akan diminta untuk memasukan terlebih dahulu. Selanjutnya dilakukan dekripsi selektif dengan cara melakukan proses XOR dari 4-bit *MSB* setiap *pixel* dari citra dengan keystream yang di bangkitkan dari Logistic Map. Proses selanjutnya sistem mengecek berapa jumlah iterasi yang akan dilakukan. Jika jumlah iterasi belum selesai maka akan dilakukan proses pengacakan *pixel* dengan invers permutasi *Arnold Cat Map*. Proses diulang samapi iterasi selesai. Proses tersebut untuk mengembalikan posisi awal *pixel*. Hasil dari proses tersebut adalah citra semula.

4.5.3 Simulasi Proses Enkripsi

Pada simulasi proses enkripsi menggunakan citra berukuran 3 x 3 dengan nilai setiap *pixel* berbeda-beda. Dengan nilai setiap nili *pixel* dimasing-masing koordinat sebagai berikut:

Tabel 4.2 Nilai Piksel Pada Setiap Koordinat Pada citra Simulasi

Koordinat	Nilai Piksel
(0,0)	50
(0,1)	35
(0,2)	65
(1,0)	54
(1,1)	83
(1,2)	75
(2,0)	87
(2,1)	92
(2,2)	58

Berikut simulasi citra:

Koordinat	0	1	2
0	50	35	65
1	54	83	75
2	87	92	58

Gambar 4.4 Ilustrasi Citra Simulasi

Citra pada gambar 4.4 akan disimulasikan untuk proses enkripsi sesuai metode yang diterapkan. Enkripsi menggunakan kunci dengan parameter $p = 5$, $q = 4$, iterasi = 1, $x = 0.7$, $r = 4$.

4.5.3.1 Pengacakan Piksel Dengan *Arnold Cat Map*

Pengacakan *pixel* menggunakan metode *Arnold Cat Map* yang sudah dijelaskan pada persamaan 2.4. Citra masukan adalah citra pada gambar 4.4. Persamaan Arnold Cat Map adalah sebagai berikut:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \quad (4.1)$$

Dari persamaan di atas maka dapat diturunkan rumus untuk mengetahui posisi x baru (x') dan y baru (y'), sebagai berikut:

$$\begin{aligned} \begin{bmatrix} x' \\ y' \end{bmatrix} &= \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \\ &= \begin{bmatrix} 1x_i + py_i \\ qx_i + (pq + 1)y_i \end{bmatrix} \bmod(N) \end{aligned}$$

Jadi, $x' = (x_i + py_i) \bmod (N)$

$$y' = (qx_i + (pq + 1)y_i) \bmod (N)$$

Berikut perhitungan pada setiap koordinat untuk mengetahui lokasi baru hasil pengacakan, dengan nilai parameter $p = 5$, $q = 4$, dan iterasi = 1 (1 kali pengacakan), $N = 3$ (pada citra 3x3):

➤ Koordinat (0,0)

$$x = 0 \text{ dan } y = 0 \text{ maka,}$$

$$\begin{aligned} x' &= (x_i + py_i) \bmod(N) & y' &= (qx_i + (pq + 1)y_i) \bmod (N) \\ &= (0 + 5.0) \bmod 3 & &= (4.0 + (5.4 + 1).0) \bmod 3 \\ &= 0 \bmod 3 & &= 0 \bmod 3 \\ x' &= 0 & y' &= 0 \end{aligned}$$

Jadi, koordinate (0,0) di petakan ke koordinat baru (0,0)

➤ Koordinat (0,1)

$$x = 0 \text{ dan } y = 1 \text{ maka,}$$

$$\begin{aligned} x' &= (x_i + py_i) \bmod(N) & y' &= (qx_i + (pq + 1)y_i) \bmod (N) \\ &= (0 + 5.1) \bmod 3 & &= (4.0 + (5.4 + 1).1) \bmod 3 \\ &= 5 \bmod 3 & &= 21 \bmod 3 \\ x' &= 2 & y' &= 0 \end{aligned}$$

Jadi, koordinate (0,1) di peakan ke koordinat baru (2,0)

➤ Koordinat (0,2)

$x = 0$ dan $y = 2$ maka,

$$\begin{aligned}x' &= (x_i + py_i) \text{ mod}(N) & y' &= (qx_i + (pq + 1)y_i) \text{ mod } (N) \\&= (0 + 5.2) \text{ mod } 3 &&= (4.0 + (5.4 + 1).2) \text{ mod } 3 \\&= 10 \text{ mod } 3 &&= 42 \text{ mod } 3 \\x' &= 1 & y' &= 0\end{aligned}$$

Jadi, koordinate (0,2) di petakan ke koordinat baru (1,0)

➤ Koordinat (1,0)

$x = 1$ dan $y = 0$ maka,

$$\begin{aligned}x' &= (x_i + py_i) \text{ mod}(N) & y' &= (qx_i + (pq + 1)y_i) \text{ mod } (N) \\&= (1 + 5.0) \text{ mod } 3 &&= (4.1 + (5.4 + 1).0) \text{ mod } 3 \\&= 1 \text{ mod } 3 &&= 4 \text{ mod } 3 \\x' &= 1 & y' &= 1\end{aligned}$$

Jadi, koordinate (1,0) di petakan ke koordinat baru (1,1)

➤ Koordinat (1,1)

$x = 1$ dan $y = 1$ maka,

$$\begin{aligned}x' &= (x_i + py_i) \text{ mod}(N) & y' &= (qx_i + (pq + 1)y_i) \text{ mod } (N) \\&= (1 + 5.1) \text{ mod } 3 &&= (4.1 + (5.4 + 1).1) \text{ mod } 3 \\&= 6 \text{ mod } 3 &&= 25 \text{ mod } 3 \\x' &= 0 & y' &= 1\end{aligned}$$

Jadi, koordinate (1,1) di petakan ke koordinat baru (0,1)

➤ Koodinat (1,2)

$x = 1$ dan $y = 2$ maka,

$$\begin{aligned}x' &= (x_i + py_i) \text{ mod}(N) & y' &= (qx_i + (pq + 1)y_i) \text{ mod } (N) \\&= (1 + 5.2) \text{ mod } 3 &&= (4.1 + (5.4 + 1).2) \text{ mod } 3 \\&= 11 \text{ mod } 3 &&= 46 \text{ mod } 3 \\x' &= 2 & y' &= 1\end{aligned}$$

Jadi, kcoordinat (1,1) di petakan ke koordinat baru (2,1)

➤ Koordinat (2,0)

$x = 2$ dan $y = 0$ maka,

$$x' = (x_i + py_i) \text{ mod}(N) \quad y' = (qx_i + (pq + 1)y_i) \text{ mod } (N)$$

$$\begin{aligned}
 &= (2 + 5.0) \bmod 3 && = (4.2 + (5.4 + 1).0) \bmod 3 \\
 &= 2 \bmod 3 && = 8 \bmod 3 \\
 x' &= 2 && y' = 2
 \end{aligned}$$

Jadi, koordinate (2,0) di petakan ke koordinat baru (2,2)

➤ Koordinat (2,1)

$x = 1$ dan $y = 2$ maka,

$$\begin{aligned}
 x' &= (x_i + py_i) \bmod(N) && y' = (qx_i + (pq + 1)y_i) \bmod (N) \\
 &= (1 + 5.2) \bmod 3 && = (4.1 + (5.4 + 1).2) \bmod 3 \\
 &= 11 \bmod 3 && = 46 \bmod 3
 \end{aligned}$$

$$x' = 2 \quad y' = 1$$

Jadi, koordinate (1,1) di petakan ke koordinat baru (2,1)

➤ Koordinat (2,2)

$x = 2$ dan $y = 2$ maka,

$$\begin{aligned}
 x' &= (x_i + py_i) \bmod(N) && y' = (qx_i + (pq + 1)y_i) \bmod (N) \\
 &= (2 + 5.2) \bmod 3 && = (4.2 + (5.4 + 1).2) \bmod 3 \\
 &= 12 \bmod 3 && = 50 \bmod 3
 \end{aligned}$$

$$x' = 0 \quad y' = 2$$

Jadi, koordinate (2,2) di petakan ke koordinat baru (0,2)

Hasil perhitungan permutasi *Arnold Cat Map* sebagai berikut:

Tabel 4.3 Hasil Permutasi *Arnold Cat Map*

Koordinat	X awal	Y awal	X akhir	Y akhir	Hasil Permutasi
0,0	0	0	0	0	0,0
0,1	0	1	2	0	2,0
0,2	0	2	1	0	1,0
1,0	1	0	1	1	1,1
1,1	1	1	0	1	0,1
1,2	1	2	2	1	2,1
2,0	2	0	2	2	2,2
2,1	2	1	1	2	1,2
2,2	2	2	0	2	0,2

Pada tabel 4.3 menjelaskan bahwa terjadi pengacakan *pixel* berdasarkan metode *Arnold Cat Map*. Dimana nilai *pixel* pada koordinat berganti nilai, seperti nilai *pixel* pada koordinat (0,1) digantikan dengan nilai *pixel* pada koordinat (2,0),

nilai *pixel* pada koordinat (1,2) digantikan dengan nilai *pixel* pada koordinat (2,1), dan sebagainya. Dari hasil permutasi diatas maka mendapatkan citra teracak sebagai berikut:

Koordinat	0	1	2
0	50	87	54
1	83	35	92
2	58	75	65

Gambar 4.5 Ilustrasi Citra Simulasi Hasil Permutasi Arnold Cat Map

4.5.3.2 Ekstraksi 4-bit MSB

Simulasi selanjutnya merupakan ekstraksi 4-bit MSB dari citra hasil pengacakan hasil langkah sebelumnya. Nilai dari setiap piksel dirubah dahulu ke biner. Selanjutnya diambil 4-bit MSB. 4-bit MSB merupakan 4 bit diambil mulai dari paling kiri pada biner 8 bit. Berikut ekstraksi 4-bit MSB berdasarkan gambar 4.6:

Tabel 4.4 Hasil Ekstraksi 4-bit MSB Pada Simulasi Enkripsi

Koordinat	Nilai	Biner	4-bit MSB (p_i)
0,0	50	00110010	0011
0,1	87	01010111	0101
0,2	54	00110110	0011
1,0	83	01010011	0101
1,1	35	00100011	0010
1,2	92	01011100	0101
2,0	58	00111010	0011
2,1	75	01001011	0100
2,2	65	01000001	0100

Pada tabel 4.4 menunjukkan hasil ekstraksi 4-bit MSB dari setiap nilai *pixel* pada gambar 4.5 atau bisa diwakil sebagai (p_i) . Dimana pada gambar 4.5 merupakan citra semulaisi yang setiap nilai pikselnya sudah ditentukan.

4.5.3.3 Pembangkitan *keystream*

Pembangkitan *keystream* dengan cara menggunakan metode *Logistic Map* dengan persamaan:

$$x_{i+1} = r x_i (1 - x_i) \quad (4.2)$$

4-bit *keystream* (k_i) diperoleh dengan teknik sebagai berikut: nilai *chaos* x_i diambil bagian desimalnya (setelah tanda koma) seukuran panjang angka (*size*) yang diinginkan dalam penelitian ini diambil 2 angka dibelakang koma, kemudian diubah menjadi *integer*. Empat bit terakhir dari representasi biner *integer* itulah yang dijadikan sebagai k_i . Dengan menggunakan nilai $x_0 = 0.7$ dan $r = 4$ dan dengan ukuran citra 3x3 maka didapat 9 bilangan acak, berikut hasil pembangkitan *keystream*:

$$\begin{aligned}x_1 &= 4 \cdot x_0(1 - x_0) = 0.84 \\x_2 &= 4 \cdot x_1(1 - x_1) = 0.5376 \\x_3 &= 4 \cdot x_2(1 - x_2) = 0.99434496 \\x_4 &= 4 \cdot x_3(1 - x_3) = 0.022492242 \\x_5 &= 4 \cdot x_4(1 - x_4) = 0.087945365 \\x_6 &= 4 \cdot x_5(1 - x_5) = 0.32084391 \\x_7 &= 4 \cdot x_6(1 - x_6) = 0.871612381 \\x_8 &= 4 \cdot x_7(1 - x_7) = 0.447616953 \\x_9 &= 4 \cdot x_8(1 - x_8) = 0.989024066\end{aligned}$$

Berikut hasil dari iterasi Logistic Map:

Tabel 4.5 Hasil Iterasi Logistic Map

Koordinat	X ke-	Nilai
0,0	1	0.84
0,1	2	0.5376
0,2	3	0.99434496
1,0	4	0.022492242
1,1	5	0.087945365
1,2	6	0.32084391
2,0	7	0.871612381
2,1	8	0.447616953
2,2	9	0.989024066

Berdasarkan hasil tabel tersebut, selanjutnya diambil 2 angka *integer* dibelakang koma, dari 2 angka *integer* tersebut dikonversi ke biner 8 bit dan selanjutnya diambil 4-bit LSB. 4-bit LSB diambil dari paling kanan pada biner 8 bit, kemudian dijadikan sebagai *keystream* (k_i).

Tabel 4.6 Hasil Pembangkitan *Keystream*

X ke-	Integer	Biner	4-bit LSB (<i>ki</i>)
0	84	01010100	0100
1	53	00110101	0101
2	99	01100011	0011
3	2	00000010	0010
4	8	00001000	1000
5	32	00100000	0000
6	87	01010111	0111
7	44	00101100	1100
8	98	01100010	0010

Pada tabel 4.6 menunjukan bahwa *Keystream* diambil 4-bit LSB dari biner 8 bit *integer* yang telah ditentukan. 4-bit LSB diambil mulai dari paling kanan pada biner 8 bit.

4.5.3.4 Operasi XOR antara *pi* dengan *ki*

Proses XOR dilakukan untuk merubah atau menyamarkan nilai pada setiap *pixel* citra. Sehingga akan mempersulit kriptanalisis untuk mendapatkan informasi citra tersebut. Proses XOR dilakukan antara *pi* yang merupakan hasil dari ekstraksi 4-bit MSB dengan *ki* yang merupakan *keystream* yang dibangkitkan dengan metode *Logistic Map*. Hasil dari proses tersebut adalah *ci*. Berikut hasil operasi XOR antara *pi* dengan *ki*:

Tabel 4.7 Hasil Operasi Pi XOR Ki

Koordinat	Pi	Ki	Ci (Pi XOR Ki)
0,0	0011	0100	0111
0,1	0101	0101	0000
0,2	0011	0011	0000
1,0	0101	0010	0111
1,1	0010	1000	1010
1,2	0101	0000	0101
2,0	0011	0111	0100
2,1	0100	1100	1000
2,2	0100	0010	0110

4.5.3.5 Proses *replace*

Selanjutnya c_1, c_2, \dots, c_n menggantikan 4-bit MSB dari setiap piksel yang

dienkripsi. Hasil enkripsi terhadap seluruh piksel adalah citra terenkripsi. Berikut simulasi prosesnya:

$$\begin{array}{l}
 \text{nilai pixel} \quad \boxed{0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0} = 50 \\
 \text{replace} \\
 \text{ci} \quad \boxed{0 \ 1 \ 1 \ 1} \\
 = \\
 \boxed{0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0} = 114
 \end{array}$$

Proses tersebut dilakukan pada setiap *pixel* pada citra. Hasil secara keseluruhan ditunjukkan pada tabel dibawah ini:

Tabel 4.8 Hasil Penggantian Ci

Koordinate	Nilai	Biner	Ci	Hasil	Nilai Baru
0,0	50	00110010	0111	01110010	114
0,1	87	01010111	0000	00000111	7
0,2	54	00110110	0000	00000110	6
1,0	83	01010011	0111	01110011	115
1,1	35	00100011	1010	10100011	163
1,2	92	01011100	0101	01011100	92
2,0	58	00111010	0100	01001010	74
2,1	75	01001011	1000	10001011	139
2,2	65	01000001	0110	01100001	97

Pada hasil yang ditunjukkan pada tabel 4.8 maka setiap *pixel* dari citra teracak memiliki nilai baru, berikut hasil citra hasil proses enkripsi:

Koordinat	0	1	2
0	114	7	6
1	115	163	92
2	74	139	97

Gambar 4.6 Simulasi Hasil Citra Terenkripsi

4.5.4 Simulasi Proses Dekripsi

Pada simulasi proses dekripsi menggunakan citra berukuran 3 x 3. Citra yang digunakan meruapkan citra hasil enkripsi pada proses sebelumnya yaitu pada gambar 4.6. Dalam proses dekripsi tata acara hampir sama dengan proses enkripsi yang membedakan adalah urutan prosesnya. Pada proses dekripsi menggunakan kunci yang sama dengan proses enkripsi menggunakan parameter $p = 5$, $q = 4$, iterasi = 1, $x = 0.7$, $r = 4$.

4.5.4.1 Ekstraksi 4-bit MSB

Proses ekstraksi 4-bit MSB dilakukan pada citra hasil enkripsi. 4-bit MSB merupakan 4 bit diambil mulai dari paling kiri pada biner 8 bit. Berikut ekstraksi 4-bit MSB berdasarkan gambar 4.6:

Tabel 4.9 Hasil Ekstraksi 4-bit MSB Pada Simulasi Dekripsi

Koordinat	Nilai	Biner	4-bit MSB (c_i)
0,0	114	01110010	0111
0,1	7	00000111	0000
0,2	6	00000110	0000
1,0	115	01110011	0111
1,1	163	10100011	1010
1,2	92	01011100	0101
2,0	74	01001010	0100
2,1	139	10001011	1000
2,2	97	01100001	0110

Pada tabel 4.9 menunjukkan hasil ekstraksi 4-bit MSB dari setiap nilai *pixel* pada gambar 4.6 atau bisa diwakil sebagai (c_i). Hasil ekstraksi 4-bit MSB akan digunakan pada proses selanjutnya.

4.5.4.2 Pembangkitan *keystream*

Pembangkitan *keystream* sama dengan saat psimulasi enkripsi yaitu dengan cara menggunakan metode *Logistic Map* dengan persamaan:

$$x_{i+1} = r \cdot x_i(1 - x_i) \quad (4.3)$$

Empat-bit *keystream* (k_i) diperoleh dengan teknik sebagai berikut: nilai *chaos* x_i diambil bagian desimalnya (setelah tanda koma) seukuran panjang angka (*size*) yang diinginkan dalam penelitian ini diambil 2 angka dibelakang koma, kemudian diubah menjadi *integer*. Empat bit terakhir dari representasi biner *integer* itulah yang dijadikan sebagai k_i . Dengan menggunakan nilai $x = 0.7$ dan $r = 4$, berikut hasil pembangkitan *keystream*:

$$x_1 = 4 \cdot x_0(1 - x_0) = 0.84$$

$$x_2 = 4 \cdot x_1(1 - x_1) = 0.5376$$

$$x_3 = 4 \cdot x_2(1 - x_2) = 0.99434496$$

$$x_4 = 4 \cdot x_3(1 - x_3) = 0.022492242$$

$$x_5 = 4 \cdot x_4(1 - x_4) = 0.087945365$$

$$x_6 = 4 \cdot x_5(1 - x_5) = 0.32084391$$

$$x_7 = 4 \cdot x_6(1 - x_6) = 0.871612381$$

$$x_8 = 4 \cdot x_7(1 - x_7) = 0.447616953$$

$$x_9 = 4 \cdot x_8(1 - x_8) = 0.989024066$$

Tabel 4.10 Hasil Iterasi Logistic Map Pada Simulasi Dekripsi

Koordinat	X ke-	Nilai
0,0	1	0.84
0,1	2	0.5376
0,2	3	0.99434496
1,0	4	0.022492242
1,1	5	0.087945365
1,2	6	0.32084391
2,0	7	0.871612381
2,1	8	0.447616953
2,2	9	0.989024066

Berdasarkan hasil tabel tersebut, selanjutnya diambil 2 angka *integer* dibelakang koma, selanjutnya dirubah ke biner, kemudian 4-bit terakhir dijadikan sebagai *keystream* (k_i).

Tabel 4.11 Hasil Pembangkitan *Keystream* Pada Simulasi Dekripsi

X ke-	Integer	Biner	4-bit LSB (k_i)
0	84	01010100	0100
1	53	00110101	0101
2	99	01100011	0011
3	2	00000010	0010
4	8	00001000	1000
5	32	00100000	0000
6	87	01010111	0111
7	44	00101100	1100
8	98	01100010	0010

Pada tabel 4.11 menunjukan bahwa *Keystream* diambil 4-bit LSB dari biner 8 bit *integer* yang telah ditentukan. 4-bit LSB diambil mulai dari paling kanan pada biner 8 bit.

4.5.4.3 Operasi XOR antara ci dengan ki

Proses XOR antara ci dan ki dilakukan untuk merubah nilai pada setiap *pixel* citra enkripsi kembali ke nilai semula. Proses XOR dilakukan antara ci yang

merupakan hasil dari ekstraksi 4-bit MSB dengan ki yang merupakan *keystream* yang dibangkitkan dengan metode *Logistic Map*. Hasil tersebut adalah pi . Berikut hasil operasi XOR antara ci dengan ki :

Tabel 4.12 Hasil Operasi Ci XOR Ki

Koordinate	Ci	Ki	Pi (Ci XOR Ki)
0,0	0111	0100	0011
0,1	0000	0101	0101
0,2	0000	0011	0011
1,0	0111	0010	0101
1,1	1010	1000	0010
1,2	0101	0000	0101
2,0	0100	0111	0011
2,1	1000	1100	0100
2,2	0110	0010	0100

4.5.4.4 Proses *replace*

Selanjutnya p_1, p_2, \dots, p_n menggantikan 4-bit MSB dari setiap *pixel* yang didekripsi. Berikut simulasi prosesnya:

$$\begin{array}{l}
 \text{nilai pixel} \quad \boxed{0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0} = 114 \\
 \text{replace} \\
 \text{ci} \quad \boxed{0 \ 0 \ 1 \ 1} \\
 = \\
 \boxed{0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0} = 50
 \end{array}$$

Proses tersebut dilakukan pada setiap *pixel* pada citra. Hasil secara keseluruhan ditunjukkan pada tabel dibawah ini:

Tabel 4.13 Hasil Penggantian Pi

Koordinat	Nilai	Biner	Pi	Hasil	Nilai Baru
0,0	114	01110010	0011	00110010	50
0,1	7	00000111	0101	01010111	87
0,2	6	00000110	0011	00110110	54
1,0	115	01110011	0101	01010011	83
1,1	163	10100011	0010	00100011	35
1,2	92	01011100	0101	01011100	92
2,0	74	01001010	0011	00111010	58
2,1	139	10001011	0100	01001011	75
2,2	97	01100001	0100	01000001	65

Pada tabel 4.12 menunjukan bahwa warna citra sudah kembali seperti semula, tetapi posisinya masih acak seperti gambar berikut:

Koordinat	0	1	2
0	50	87	54
1	83	35	92
2	58	75	65

Gambar 4.7 Hasil Citra Teracak

4.5.4.5 Proses *Invers* Permutasi *Arnold Cat Map*

Pada hasil proses sebelumnya masih menghasilkan citra teracak. Untuk mengembalikan posisi *pixel* seperti citra awal maka diakukan perhitungan *invers* permutasi *Arnold Cat Map* dengan persamaan seperti berikut:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \text{mod}(N) \quad (2.7)$$

Dari persamaan di atas maka dapat diturunkan rumus untuk mengetahui posisi x awal (x) dan y awal (y), sebagai berikut:

$$\begin{aligned} \begin{bmatrix} x_i \\ y_i \end{bmatrix} &= \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \text{mod}(N) \\ &= \frac{1}{1.(pq+1)-p.q} \begin{bmatrix} pq + 1 & -q \\ -p & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \text{mod}(N) \\ &= \begin{bmatrix} pq + 1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \text{mod}(N) \\ &= \begin{bmatrix} (pq + 1)x' + (-py') \\ -qx' + 1y' \end{bmatrix} \text{mod}(N) \end{aligned}$$

$$\text{Jadi, } x = ((pq + 1)x' + (-py')) \text{mod}(N)$$

$$y = (-qx' + y') \text{mod}(N)$$

Berikut perhitungan pada setiap koordinat untuk mengetahui lokasi awal dasil hasil acak sebelumnya, dengan nilai parameter $p = 5$, $q = 4$, dan iterasi = 1 (1 kali pengacakan), $N = 3$ (pada citra 3x3):

➤ Koordinat (0,0)

$$x' = 0 \text{ dan } y' = 0, \text{ maka}$$

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \text{mod}(N) & y &= (-qx' + y') \text{mod}(N) \\ &= ((5.4 + 1).0 + (-5.0)) \text{mod}(3) & &= (-4.0 + 0) \text{mod}(3) \\ &= 0 \text{ mod}(3) & &= 0 \text{ mod}(3) \end{aligned}$$

$$x = 0$$

$$y = 0$$

Jadi, koordinat (0,0) di kembalikan ke koordinat (0,0)

- Koordinat (0,1)

$x' = 0$ dan $y' = 1$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).0 + (-5.1)) \bmod (3) & &= (-4.0 + 1) \bmod (3) \\ &= -5 \bmod (3) & &= 1 \bmod (3) \end{aligned}$$

$$x = 1$$

$$y = 1$$

Jadi, koordinat (0,1) di kembalikan ke koordinat (1,1)

- Koordinat (0,2)

$x' = 0$ dan $y' = 2$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).0 + (-5.2)) \bmod (3) & &= (-4.0 + 2) \bmod (3) \\ &= -10 \bmod (3) & &= 2 \bmod (3) \end{aligned}$$

$$x = 2$$

$$y = 2$$

Jadi, koordinat (0,2) di kembalikan ke koordinat (2,2)

- Koordinat (1,0)

$x' = 1$ dan $y' = 0$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).1 + (-5.0)) \bmod (3) & &= (-4.0 + 2) \bmod (3) \\ &= 21 \bmod (3) & &= 2 \bmod (3) \end{aligned}$$

$$x = 0$$

$$y = 2$$

Jadi, koordinat (0,2) di kembalikan ke koordinat (2,2)

- Koordinat (1,1)

$x' = 1$ dan $y' = 1$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).1 + (-5.1)) \bmod (3) & &= (-4.1 + 1) \bmod (3) \\ &= 16 \bmod (3) & &= -3 \bmod (3) \end{aligned}$$

$$x = 1$$

$$y = 0$$

Jadi, koordinat (1,1) di kembalikan ke koordinat (1,0)

➤ Koordinat (1,2)

$x' = 1$ dan $y' = 2$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).1 + (-5.2)) \bmod (3) & &= (-4.1 + 2) \bmod (3) \\ &= 11 \bmod (3) & &= -2 \bmod (3) \\ x &= 2 & y &= 1 \end{aligned}$$

Jadi, koordinat (1,2) di kembalikan ke koordinat (2,1)

➤ Koordinat (2,0)

$x' = 2$ dan $y' = 0$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).2 + (-5.0)) \bmod (3) & &= (-4.2 + 0) \bmod (3) \\ &= 42 \bmod (3) & &= -8 \bmod (3) \\ x &= 0 & y &= 1 \end{aligned}$$

Jadi, koordinat (2,0) di kembalikan ke koordinat (0,1)

➤ Koordinat (2,1)

$x' = 2$ dan $y' = 1$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).2 + (-5.1)) \bmod (3) & &= (-4.2 + 1) \bmod (3) \\ &= 37 \bmod (3) & &= -7 \bmod (3) \\ x &= 1 & y &= 2 \end{aligned}$$

Jadi, koordinat (2,1) di kembalikan ke koordinat (1,2)

➤ Koordinat (2,2)

$x' = 2$ dan $y' = 2$, maka

$$\begin{aligned} x &= ((pq + 1)x' + (-py')) \bmod (N) & y &= (-qx' + y') \bmod (N) \\ &= ((5.4 + 1).2 + (-5.2)) \bmod (3) & &= (-4.2 + 2) \bmod (3) \\ &= 32 \bmod (3) & &= -6 \bmod (3) \\ x &= 2 & y &= 0 \end{aligned}$$

Jadi, koordinat (2,2) di kembalikan ke koordinat (2,0)

Hasil perhitungan *invers* permutasi *Arnold Cat Map* sebagai berikut:

Tabel 4.13 Hasil *Invers* Permutasi Arnold Cat Map

Koordinat	X' awal	Y' awal	X' akhir	Y' akhir	Hasil (x,y)
0,0	0	0	0	0	0,0
0,1	0	1	1	1	1,1
0,2	0	2	2	2	2,2
1,0	1	0	0	2	0,2
1,1	1	1	1	0	1,0
1,2	1	2	2	1	2,1
2,0	2	0	0	1	0,1
2,1	2	1	1	2	1,2
2,2	2	2	2	0	2,0

Pada tabel 4.3 menunjukkan bahwa posisi *pixel* kembali ke posisi semula berikut hasil citra:

Koordinat	0	1	2
0	50	35	65
1	54	83	75
2	87	92	58

Gambar 4.8 Ilustrasi Hasil Citra Invers Permutasi Arnold Cat Map

4.6 Racangan *User Interface*

Rancangan *user interface* merupakan rancangan tampilan sebagai media untuk berinteraksi antara pengguna dengan sistem. Berikut merupakan rancang *user interface* pada gambar 4.9:

Pada gambar 4.9 menampilkan rancang *user interface* yang hendak diterapkan. Pada rancang *user interface* tersebut memiliki menu bar yang terdiri dari *File* dan *Run*. Menu *File* terdiri dari menu *open image*, *save image*, *clear*. Menu *Open image* berfungsi untuk membuka atau memasukan citra. Menu *save image* berfungsi untuk menyimpan citra. Menu *clear* berfungsi untuk mengkosongkan *picture box* dan *textbox secret key*. Menu *Run* terdiri dari menu *Enkripsi* dan *Dekripsi*. Menu *Enkripsi* berfungsi untuk menjalankan proses enkripsi. Menu *Dekripsi* berfungsi untuk menjalankan proses dekripsi. Tombol “*generate key*”

berfungsi untuk memasukan kunci rahasia secara otomatis yang bersifat *random*. Tombol “Save Key” untuk menyimpan kunci rahasia yang sudah ditentukan.



Gambar 4.9 Rancang *User Interface*

BAB V. IMPLEMENTASI

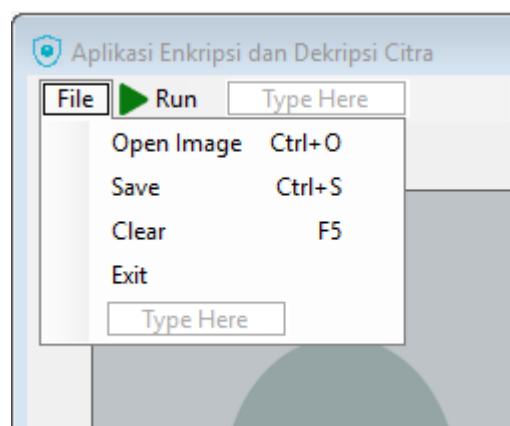
Bab ini menjelaskan tentang pembuatan aplikasi yang sesuai dengan teori yang digunakan dalam pembuatan sistem. Penjelasan berisi langkah-langkah dalam pembangunan aplikasi.

5.1 Pembuatan Aplikasi

Pembuatan Aplikasi berdasarkan pada desain yang dijabarkan pada bab sebelumnya. Bab implementasi adalah melakukan penulisan kode sesuai dengan apa yang sudah dirancang. Aplikasi memiliki dua fungsi utama yaitu melakukan proses enkripsi dan proses dekripsi. Selain itu aplikasi juga harus bisa menyediakan kebutuhan pengguna seperti membuka file gambar, menyimpan file gambar, dan *generate key* secara otomatis.

5.2 Pembuatan Menu Utama

Tampilan awal memiliki fungsi membuka gambar, simpan, hapus, dan tutup. Fungsi tersebut merupakan fungsi dasar untuk memenuhi kebutuhan dari *user*. Dengan fungsi tersebut, *user* dapat membuka gambar yang akan dipilih untuk proses enkripsi atau dekripsi, dan kemudian *user* bisa menyimpannya dengan menu *save*.



Gambar 5.1 Menu Utama

Pada gambar 5.1 menampilkan menu yang dapat memenuhi kebutuhan *user* untuk penggunaan aplikasi Enkripsi Citra. Pada menu tersebut *user* juga bisa menggunakan *shortcut* untuk menjalankan menu tersebut. Pada menu bar "File" terdiri beberapa menu yaitu:

a. *Button Open Image*

Button Open Image digunakan untuk membuka dialog untuk memilih file citra. File citra yang dipilih akan ditampilkan ke *picture box*. *Shortcut* untuk menjalankan menu *open image* adalah Ctrl + O.

b. *Button Save*

Button Save berfungsi untuk melakukan penyimpanan citra yang dibuka pada aplikasi. *User* bisa melakukan penyimpanan untuk citra pada *image output* sesuai dengan kebutuhan. *Shortcut* untuk menjalankan menu *save* adalah Ctrl + S.

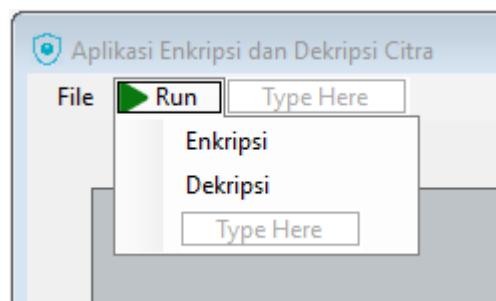
c. *Button Clear*

Button clear digunakan untuk menghilangkan citra yang ada pada *picture box* pada *image input* dan *image output*, mengkosongkan *textbox secret key*, dan *progressbar*. *Shortcut* untuk menjalankan menu *clear* adalah F5.

d. *Button Exit*

Button exit digunakan untuk menutup form yang ada.

Selain menu utama, aplikasi juga memiliki menu untuk menjalankan proses yaitu pada menu bar “Run”. Pada menu bar “Run” memiliki beberapa menu yang ditunjukkan pada gambar 5.2:



Gambar 5.2 Menu Proses

a. *Button Enkripsi*

Button enkripsi berfungsi untuk menjalankan proses enkripsi pada citra digital.

b. *Button Dekripsi*

Button dekripsi berfungsi untuk menjalankan proses dekripsi pada citra digital.

5.2.1 Proses Pengambilan Citra

Pada proses pengambilan citra *user* disediakan fitur *open image*. Fitur tersebut digunakan untuk membuka citra dan menampilkan pada *picturebox imgae input*. Pada proses enkripsi dan dekripsi, sistem membutuhkan penyimpanan bertipe *bitmap* pada *memory*. Untuk memenuhi kebutuhan sistem tersebut maka sebelum melakukan proses enkripsi dan dekripsi maka citra masukan di konversi terlebih dahulu dalam bentuk *bitmap*. Dibawah ini menunjukkan contoh kode atau *script* untuk konversi ke *bitmap* dengan Bahasa VB.NET

```
'inialisasi variabel
Dim image1 As New Bitmap(PB_input.Image)
Dim image_input As New Bitmap(PB_input.Image)
```

Dengan menggunakan perintah tersebut, maka sistem akan mendapatkan citra pada *picturebox input image* yang memiliki tipe *bitmap*.

5.3 Pembuatan Pembangkit Kunci

Proses enkripsi dan dekripsi bisa berjalan jika kunci rahasia sudah diinputkan. Kunci rahasia tersebut terdiri dari 5 buah yaitu *p* dan *q* sebagai parameter *Arnold Cat Map*, *r* dan *x* sebagai parameter *Logistic Map*, serta *m* sebagai banyaknya iterasi. Dalam memasukan kunci rahasia *user* bisa memasukan secara manual dengan cara menginputkan pada *textbox* yang sudah disediakan atau dapat langsung membangkitkan kunci secara otomatis dengan cara menekan *button generate key*. Sehingga memberika kemudahan pada *user* untuk menentukan kunci rahasia.

Dalam proses pembuatan *button* untuk pembangkitan kunci tetap mengacu pada kebutuhan dari setiap parameter dimana untuk parameter *p* dan *q* yang merupakan parameter *Arnold Cat Map* dapat disi dengan sembarang *integer*, sedangkan untuk parameter *Logistic Map* *x* dan *r* masing-masing memiliki *requirement* yang berbeda, dengan $0 \leq x \leq 1$, dan $0 \leq r \leq 4$. Berikut merupakan kode untuk pembangkitan kunci menggunakan Bahasa VB.NET:

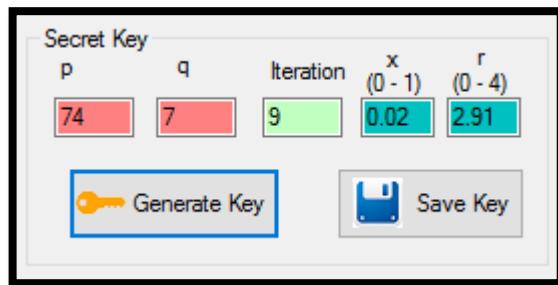
```
'inialisasi variabel
Dim random As New Random()
'Generate P
TBp.Text = random.Next(1, 99)
'Generate Q
TBq.Text = random.Next(1, 99)
'Generete X (0 - 1)
Dim nmbr As String = random.NextDouble().ToString()
Dim gnmb As String = Strings.Left(nmbr, 4)
```

```

TBx.Text = gnmbr
'Generate r (0-4)
TBr.Text = random.Next(100, 400) / 100
'Generate Iteration
TBIteration.Text = random.Next(1, 10)

```

Hasil *generate key* ditunjukan pada gambar 5.3 dibawah ini:



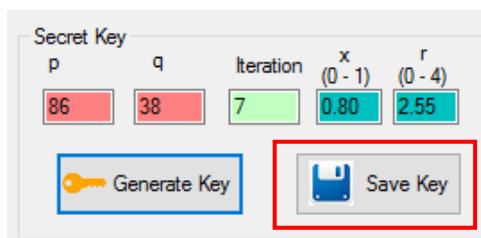
Gambar 5.3 Tampilan Hasil *Generate Key*

Pada gambar 5.3 menunjukan bahawa p, q, dan iterasi berisikan nilai yang bertipe *integer*, sedangkan x dan r berisikan nilai yang bertipe *double*. Dengan adanya fitur tersebut *user* akan mudah menentukan kunci rahasia yang akan digunakan untuk proses enkripsi dan dekripsi. Selain itu *user* juga disediakan *button* untuk menyimpan kunci rahasia tersebut dengan *button Save Key*.

5.3.1 Proses Penyimpanan Kunci Rahasia

Pada Aplikasi Enkripsi dan Dekripsi Citra Digital menggunakan metode Arnold Cat Map dan Logistic Map memberikan fasilitas untuk dapat menyimpan kunci rahasia agar mempermudah pengguna (*user*) untuk menyimpan dan menghindari pengguna lupa dengan kunci rahasia yang digunakan untuk proses enkripsi maupun proses dekripsi. Proses dari menyimpan kunci rahasia sebagai berikut:

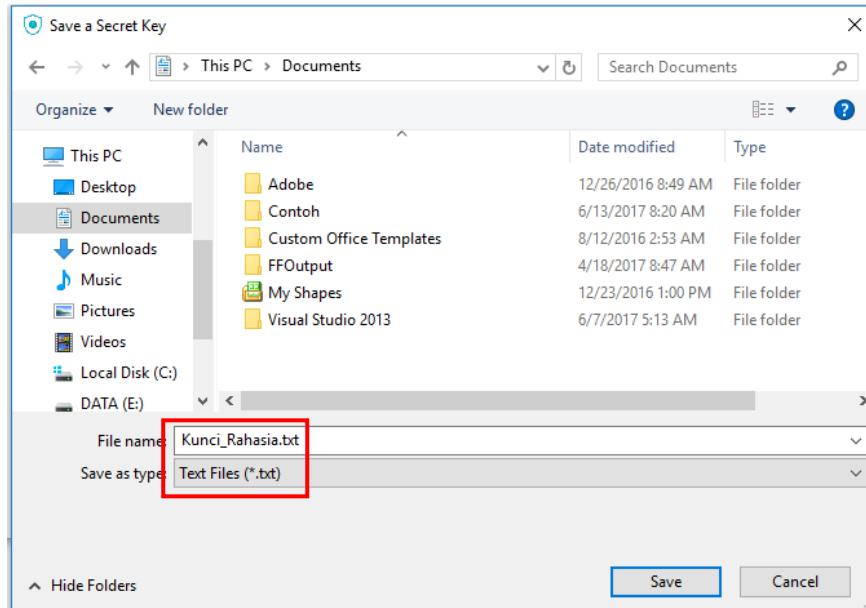
- Klik button Save Key pada groupbox Secret Key



Gambar 5.4 Tampilan GroupBox Secret Key

Button *save key* akan berjalan jika setiap Textbox dari parameter sudah terisi. Jika tidak akan menampilkan pemberitahuan secret Key Kosong

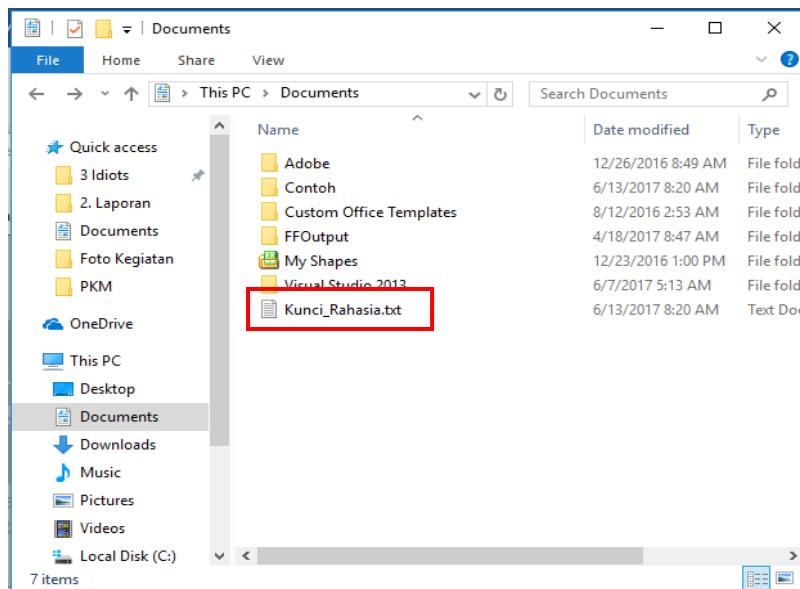
b. Selanjutnya akan muncul Kotak Dialog



Gambar 5.5 Tampilan Kotak Dialog *Save a Secret Key*

Pada kotak Dialog Save, pengguna dapat memilih tempat untuk menyimpan kunci rahasia. Setelah itu, pengguna dapat langsung memberi nama filenya. Klik *button save* maka kunci rahasia akan tersimpan. Kunci rahasia akan di simpan dalam bentuk file .txt.

c. Kunci Rahsia berhasil di simpan



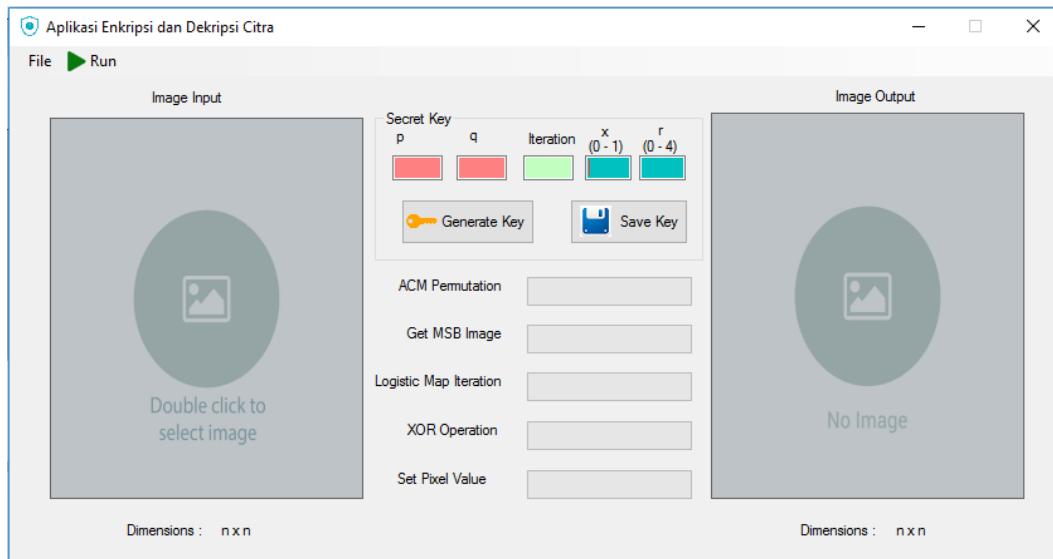
Gambar 5.6 Tampilan Tempat File *Secret Key* Tersimpan

Kunci Rahsia berhasil di simpan. Pada contoh di atas kunci rahsia di simpan pada directory C:\Users\ANGGI\Documents.

5.4 Hasil Aplikasi

5.4.1 Tampilan Program

Aplikasi yang dibuat berdasarkan yang sudah dirancang dan menggunakan modul dasar *prototype* yang sudah diuji coba sebelumnya.



Gambar 5.7 Tampilan Aplikasi Enkripsi dan Dekripsi Citra

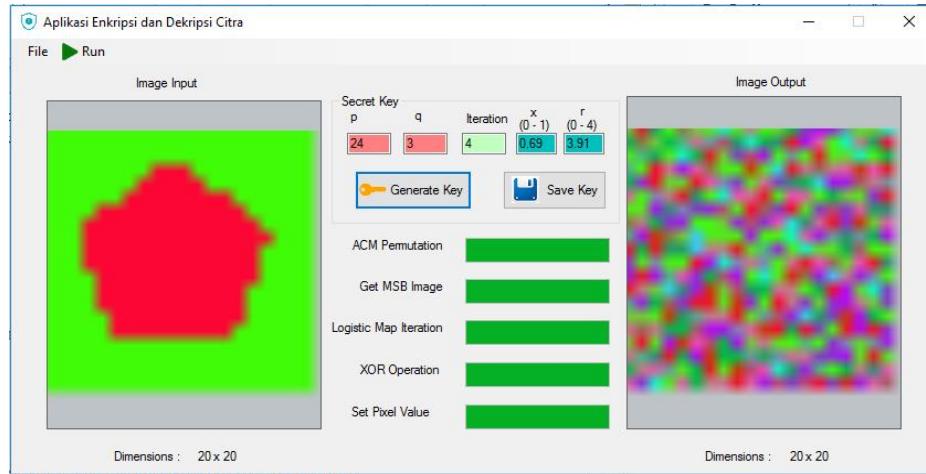
Pada gambar 5.4 menunjukkan tampilan aplikasi enkripsi dan dekripsi citra digital dokumen hasil *scan*. Terdapat dua *picturebox* yaitu *picturebox image input* dan *image output*. Pada *picturebox image input* pengguna (*user*) dapat memilih citra yang akan diproses, baik untuk proses enkripsi atau proses dekripsi. *Picturebox image output* merupakan tempat hasil proses enkripsi atau proses dekripsi. Citra yang berada di *picturebox image output* dapat disimpan oleh *user* dengan memilih menu *save* yang berada di menu bar *File*.

5.4.2 Hasil Program

Proses enkripsi menggunakan citra berukuran 20×20 pixel. Warna dasar yang digunakan adalah hijau dan merah. Proses enkripsi menggunakan kunci dengan parameter:

- p = 24
- q = 3
- iterasi = 4
- x = 0.69
- r = 3.91.

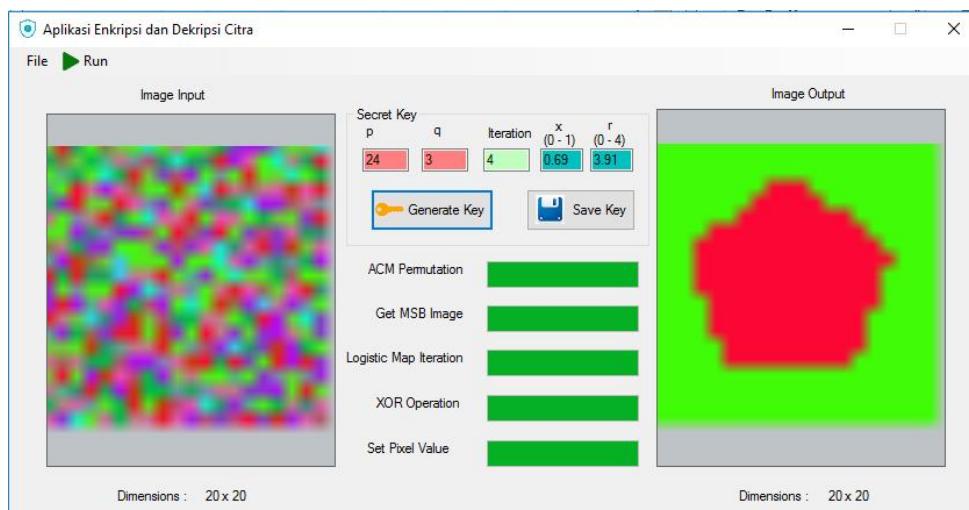
Hasil program saat melakukan proses enkripsi citra sebagai berikut:



Gambar 5.8 Tampilan Hasil Enkripsi

Proses enkripsi dijalankan ketika *secrete key* dan citra sudah terpenuhi. Hasil dari proses enkripsi ditampilkan pada *picturebox image output*. Yang kemudian hasil citra terenkripsi tersebut dapat disimpan.

Selanjutnya proses yang dilakukan adalah proses dekripsi. Proses dekripsi menggunakan kunci yang sama dengan kunci untuk proses enkripsi yaitu dengan parameter $p = 24$, $q = 3$, iterasi = 4, $x = 0.69$, $r = 3.91$. Jika tidak sama maka proses dekripsi tidak menghasilkan citra semula. Berikut tampilan program saat melakukan proses dekripsi citra:



Gambar 5.9 Tampilan Hasil Dekripsi

Pada gambar 5.6 menunjukan bahwa program berhasil melakukan dekripsi citra. Hal ini membuktikan bahwa aplikasi yang dibuat dapat menjalankan proses enkripsi dan dekripsi.

BAB VI. PENGUJIAN DAN PEMBAHASAN

Pada bab ini dilakukan pengujian setelah dilakukan implementasi sistem, metode, dan konten. Pengujian bermaksud untuk mengetahui perangkat lunak yang dibuat sudah memenuhi kriteria yang sesuai dengan tujuan perancangan yang sudah dirancang. Pengujian dibagi menjadi pengujian sistem dan pengujian hasil. Pengujian sistem berfungsi untuk melihat fitur yang ada pada aplikasi. Pengujian hasil sebagai analisa yang dilakukan untuk melihat kesesuaian dengan metode yang digunakan serta kelayakan metode pada aplikasi yang serupa.

6.1 Pengujian Sistem

Pada proses pengujian sistem menggunakan metode *black box*. Pengujian *black box* digunakan untuk menguji fungsi-fungsi khusus dari perangkat lunak yang dirancang. Dengan menggunakan metode *black box* dapat dinilai apakah *input* yang diterima dan *output* sudah tepat atau belum. Berikut merupakan hasil pengujian sistem menggunakan metode *black box* pada aplikasi enkripsi dan dekripsi dokumen hasil *scan* menggunakan metode *Arnold Cat Map* dan *Logistic Map*:

Tabel 6.1 Pengujian Sistem

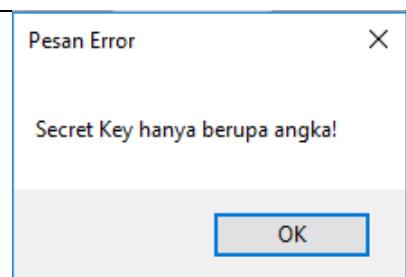
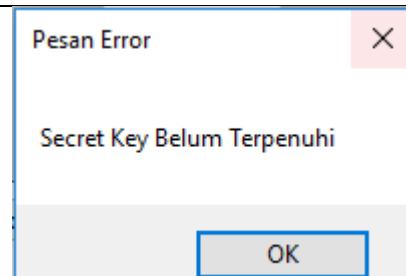
No	Skenario	Hasil yang diharapkan	Hasil yang terjadi	Keterangan
1.	Mebuka citra asli	Citra terbuka di <i>picturebox</i> citra awal pada form	Citra terbuka pada <i>picturebox</i> citra awal	[<input checked="" type="checkbox"/>] Berhasil [<input type="checkbox"/>] Tidak Berhasil
2.	Membuka citra terenkripsi	Citra terbuka di <i>picturebox</i> citra enkripsi pada form	Citra terbuka pada <i>picturebox</i> citra enkripsi	[<input checked="" type="checkbox"/>] Berhasil [<input type="checkbox"/>] Tidak Berhasil

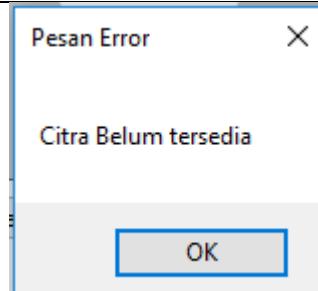
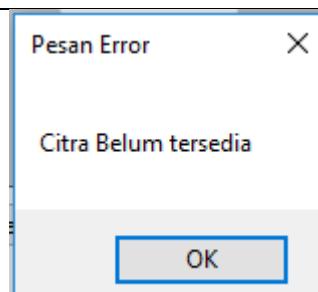
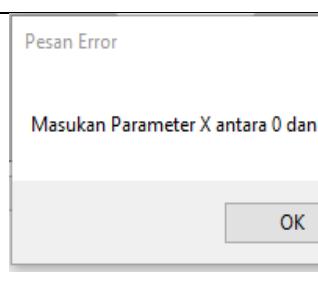
No	Skenario	Hasil yang diharapkan	Hasil yang terjadi	Keterangan
3.	Proses <i>generate key</i>	Proses <i>generate key</i> berjalan secara normal, dan menampilkan <i>secret key</i> secara otomatis	Proses berjalan dengan normal	[√] Berhasil [] Tidak Berhasil
4.	Proses enkripsi	Proses enkripsi berjalan secara normal, saat menu dipilih, dan citra terenkripsi muncul di <i>picturebox</i> citra enkripsi	Proses berjalan normal	[√] Berhasil [] Tidak Berhasil
5.	Proses dekripsi	Proses dekripsi berjalan dengan normal, saat menu dipilih dan citra tersekripsi muncul di <i>picturebox</i> citra dekripsi	Proses berjalan normal	[√] Berhasil [] Tidak Berhasil
6.	Menyimpan citra	Citra pada <i>picturebox image input</i> dan <i>picturebox image output</i> dapat disimpan ke dalam peyimpanan.	Peyimpanan berhasil	[√] Berhasil [] Tidak Berhasil

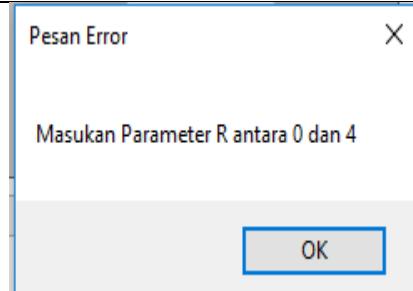
No	Skenario	Hasil yang diharapkan	Hasil yang terjadi	Keterangan
7.	Clear <i>picturebox</i> dan <i>textbox secretkey</i>	Menghilangkan citra pada <i>picturebox</i> dan nilai <i>secretkey</i> pada <i>textbox</i>	Menghilangkan citra dan <i>secret key</i> berhasil	[√] Berhasil [] Tidak Berhasil
8.	Keluar pada program	Aplikasi akan tertutup jika memilih menu <i>exit</i>	Aplikasi berhasil tertutup	[√] Berhasil [] Tidak Berhasil

Dari tabel tersebut dapat disimpulkan bahwa aplikasi berjalan dengan baik dan benar. Pengujian tersebut menjalankan aplikasi dengan menggunakan parameter yang sesuai. Pengujian selanjutnya untuk melihat pesan *error* saat aplikasi menerima *inputan* yang tidak sesuai parameter yang dibutuhkan.

Tabel 6.2 Pengujian Pesan Error

No	Skenario	Proses sebenarnya	Tampilan <i>Error</i>	Keterangan
1.	Nilai <i>secret key</i> bukan berupa angka	Nilai <i>secret key</i> berupa angka		Pesan <i>error</i> muncul saat masukan selain angka pada <i>textbox secret key</i>
2.	Nilai <i>secret key</i> masih kosong	Nilai <i>secret key</i> harus sudah tersedia saat proses enkripsi		Pesan <i>error</i> muncul ketika tombol enkripsi atau dekripsi ditekan sedangkan

No	Skenario	Proses sebenarnya	Tampilan <i>Error</i>	Keterangan
		atau dekripsi		<i>secret key</i> masih kosong
3.	Citra <i>input</i> kosong	Citra <i>input</i> harus sudah tersedia saat proses enkripsi		Pesan <i>error</i> muncul saat tombol enkripsi dan <i>picturebox input</i> masih kosong
4.	Citra Enkripsi kosong	Citra terenkripsi harus sudah tersedia saat proses dekripsi		Pesan <i>error</i> muncul saat tombol dekripsi ditekan sedangkan <i>picturebox</i> ekripsi masih kosong
5.	Nilai Parameter x bukan kurang dari 0 dan lebih dari 1	Nilai parameter bernilai antara 0 dan 1		Pesan <i>error</i> muncul ketika tombol enkripsi atau dekripsi ditekan sedangkan parameter "x" pada <i>secret key</i> bernilai kurang dari 0

No	Skenario	Proses sebenarnya	Tampilan <i>Error</i>	Keterangan
				dan lebih dari 1
6.	Nilai Parameter R bukan kurang dari 0 dan lebih dari 4	Nilai parameter bernilai antara 0 dan 4		Pesan <i>error</i> muncul ketika tombol enkripsi atau dekripsi ditekan sedangkan parameter “r” pada <i>secret key</i> bernilai kurang dari 0 dan lebih dari 4

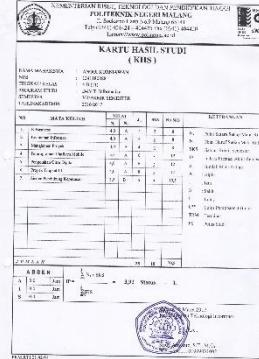
Dari tabel tersebut dapat diketahui ada beberapa kesalahan dari pengguna dalam menggunakan aplikasi tersebut. Aplikasi yang dibangun telah dapat membuat validasi kesalahan penggunaan yang mungkin terjadi. Aplikasi akan memberikan pesan eror sesuai dengan kesalahan yang dilakukan oleh pengguna (*user*). Aplikasi tidak akan berjalan sampai pengguna (*user*) menginputkan parameter sesuai dengan *requirement* (kebutuhan) dari aplikasi tersebut. Dengan demikian tidak terjadi kesalahan dalam *input* yang disebabkan oleh pengguna.

6.2 Pengujian Hasil

Pengujian hasil dilakukan untuk melihat kesesuaian dan kelayakan metode untuk digunakan pada aplikasi enkripsi dan dekripsi citra dokumen hasil *scan*. Hasil yang diharapkan adalah hasil sebaik-baiknya untuk membuktikan bahwa metode ini memberikan keamanan pada citra dokumen hasil *scan*. Pengujian menggunakan citra RGB dalam prosesnya. Citra yang digunakan sebagai pengujian adalah sebagai berikut:

Tabel 6.3 Citra Uji Coba

No	Nama Citra	Tampilan Citra	Keterangan Citra
1.	Logo Polinema		Lebar : 327 Tinggi : 304 Ukuran : 71.8 KB
2.	Sampul Skripsi		Lebar : 1246 Tinggi : 1754 Ukuran : 244 KB
3.	Sertifikat Microsoft Office		Lebar : 1447 Tinggi : 2048 Ukuran : 988 KB
4.	Sertifikat LDK		Lebar : 1435 Tinggi : 2048 Ukuran : 904 KB

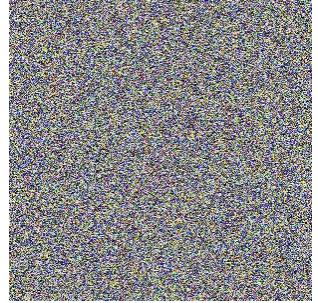
No	Nama Citra	Tampilan Citra	Keterangan Citra
5.	Sertifikat Pra Study		Lebar : 1473 Tinggi : 2048 Ukuran : 824 KB
6.	Sertifikat TF 2016		Lebar : 1455 Tinggi : 2048 Ukuran : 560 KB
7.	KHS		Lebar : 1544 Tinggi : 2048 Ukuran : 380 KB
8.	Sertifikat Seminar		Lebar : 1438 Tinggi : 2048 Ukuran : 837 KB

No	Nama Citra	Tampilan Citra	Keterangan Citra
9.	Sertifikat Microkontroler		Lebar : 1468 Tinggi : 2048 Ukuran : 731 KB
10.	Sertifikat SIAP		Lebar : 1435 Tinggi : 2048 Ukuran : 921 KB

6.2.1 Pengujian Visual

Pengujian visual digunakan untuk melihat kecocokan citra antara citra asli, citra terenkripsi (*cipher-image*), dan citra terdekripsi. Citra asli dan citra terenkripsi (*cipher-image*) harus memiliki perbedaan yang besar, sedangkan citra asli dan citra terdekripsi diharuskan mememiliki persamaan yang besar. Pada pengujian citra menggunakan parameter $p = 19$, $q = 38$, iterasi = 5, $x = 0.67$, dan $r = 3.98$. Berikut adalah hasil pengujian visual:

Tabel 6.4 Uji Coba Enkripsi Citra

No	Citra Input	Citra Terenkripsi	Citra terdekripsi
1.			

No	Citra Input	Citra Terenkripsi	Citra terdekripsi
2.			
3.			
4.			
5.			
6.			

No	Citra Input	Citra Terenkripsi	Citra terdekripsi
7.			
8.			
9.			
10.			

Uji coba menggunakan 10 citra digital hasil *scan* yang berbeda. Hasil yang didapat pada pengujian kasat mata sesuai dengan yang diharapkan. Informasi pada citra digital dokumen hasil *scan* terlindungi, sehingga tidak terjadi kebocoran informasi pada citra yang sudah dienkripsi.

Uji coba proses dekripsi juga dilakukan dengan menggunakan kunci atau parameter yang sama pada proses enkripsi yaitu menggunakan parameter $p = 19$, $q = 38$, $\text{iterasi} = 5$, $x = 0.67$, dan $r = 3.98$. Hasil yang diharapkan adalah citra digital

kembali ke bentuk semula. Pada pengujian visual didapatkan hasil yang sama antara citra asli dan citra hasil dekripsi.

Pada pengujian visual dilakukan analisa nilai NPCR, UACI, MSE, dan PSNR. Nilai tersebut diambil dari rata-rata nilai *Red*, *Green*, *Blue* pada setiap citra digital. Perbandingan yang digunakan yaitu citra asli dengan citra hasil dekripsi. Hasil yang diharapkan untuk nilai NPCR, UACI, dan MSE adalah 0 dan nilai PSNR adalah tak terhingga sehingga dapat disimpulkan bahwa citra asli dengan citra hasil dekripsi memiliki kesamaan.

Tabel 6.5 Analisa Dekripsi Citra berdasarkan tabel 6.4

No	NPCR	UACI	MSE	PSNR
1	0 %	0 %	0	∞ db
2	0 %	0 %	0	∞ db
3	0 %	0 %	0	∞ db
4	0 %	0 %	0	∞ db
5	0 %	0 %	0	∞ db
6	0 %	0 %	0	∞ db
7	0 %	0 %	0	∞ db
8	0 %	0 %	0	∞ db
9	0 %	0 %	0	∞ db
10	0 %	0 %	0	∞ db

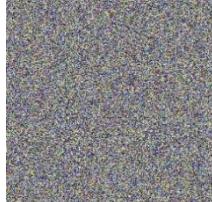
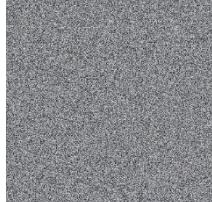
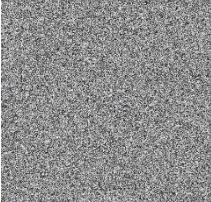
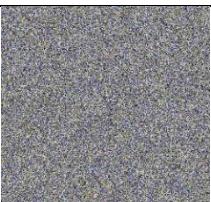
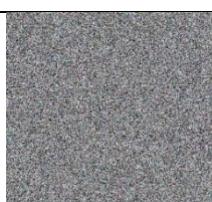
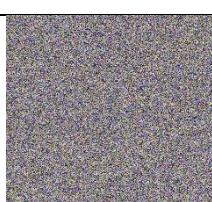
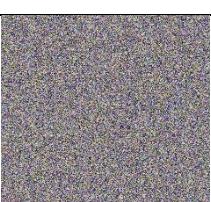
Pada hasil pengujian diatas mendapatkan nilai NPCR, dan UACI sama dengan 0 %. Sedangkan nilai MSE sama dengan 0 dan nilai PSNR mendapatkan nilai tak terhingga (∞). Dengan demikian dapat disimpulkan bahwa citra asli dan citra yang telah mengalami proses enkripsi dan dekripsi dinyatakan sama 100%.

6.2.2 Pengujian Sensifitas Kunci

Suatu sistem enkripsi yang baik adalah sistem yang sensitif terhadap perubahan kunci. Sehingga perubahan sedikit kunci saja akan mengakibatkan dampak yang sangat besar dalam proses enkripsi dan dekripsi. Pengujian dilakukan dengan menggunakan citra yang sama tetapi menggunakan kunci yang berbeda pada saat proses dekripsi. Pada pengujian ini menggunakan *key* 1 dengan parameter $p = 19$, $q = 38$, $\text{iterasi} = 5$, $x = 0.67$, dan $r = 3.98$. Sedangkan *Key* 2 dengan parameter

$p = 43$, $q = 96$, iterasi = 2, $x = 0.56$, dan $r = 1.98$. Berikut hasil dari pengujian sensivitas kunci:

Tabel 6.6 Hasil Uji coba Sensifitas Kunci

No	Citra Asli	Citra enkripsi dengan Key 1	Citra dekripsi dengan Key 1	Citra dekripsi dengan Key2
1.				
2.				
3.				
4.				
5.				
6.				

No	Citra Asli	Citra enkripsi dengan Key 1	Citra dekripsi dengan Key 1	Citra dekripsi dengan Key2
7.				
8.				
9.				
10.				

Pada pengujian sensifitas kunci, diketahui jika penggunaan kunci yang berbeda pada saat proses enkripsi dan dekripsi citra tidak bisa kembali ke citra semula. Pada percobaan 10 citra didapatkan 100% citra tidak kembali ke kondisi awal. Sehingga dapat dinyatakan sistem enkripsi sangat sensitive terhadap perubahan kunci.

6.2.3 Pengujian Kecepatan Proses

Pengujian kecepatan dilakukan untuk mengetahui keberhasilan metode dalam melakukan proses. Dengan algoritma yang sama sedangkan penulisan kode yang berbeda dapat mempengaruhi waktu proses secara signifikan. Pengujian dilakukan dengan cara menggunakan citra dengan ukuran yang berbeda dan jumlah iterasi yang berbeda.

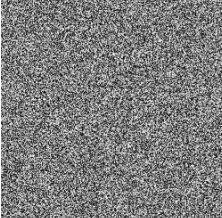
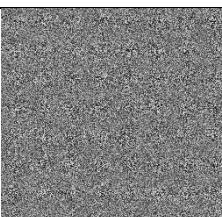
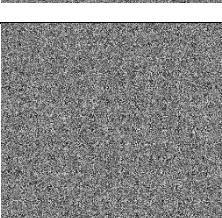
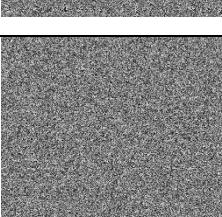
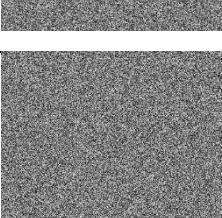
Pengujian kecepatan dilakukan dengan laptop peneliti dengan spesifikasi:

- Processor : Intel® Core™ i3 CPU 2.53GHz
- RAM : 6 GB
- VGA : Intel® HD Graphics (Core i3)

Uji coba dengan spesifikasi lain juga bisa mempengaruhi kecepatan proses. Berikut hasil pengujian kecepatan proses:

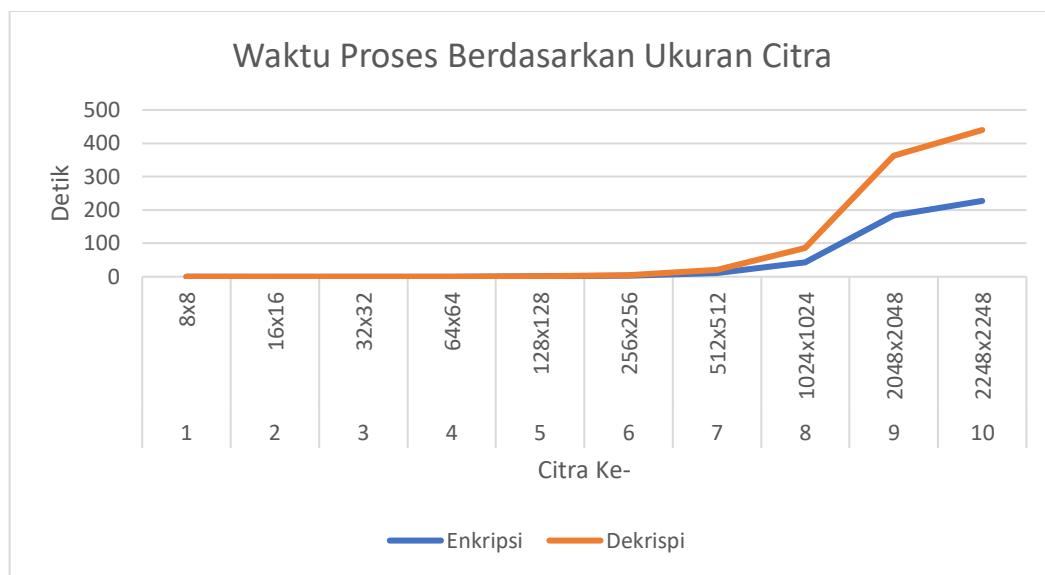
Tabel 6.7 Hasil Pengujian Kecepatan Proses

No	Ukuran Citra	Keterangan Citra	Waktu Enkripsi	Waktu Dekripsi
1.	8 x 8		0.000000 detik	0.00000 detik
2	16 x 16		0.015625 detik	0.015625 detik
3	32 x 32		0.046875 detik	0.046875 detik
4	64 x 64		0.187500 detik	0.171875 detik
5	128 x 128		0.656250 detik	0.640625 detik

No	Ukuran Citra	Keterangan Citra	Waktu Enkripsi	Waktu Dekripsi
6	256 x 256		2.640625 detik	2.734375 detik
7	512 x 512		10.578125 detik	10.671875 detik
8	1024x1024		42.593750 detik	42.843750 detik
9	2048x2048		182.953125 detik	179.250000 detik
10	2248x2248		227.296875 detik	212.484375 detik

Berikut hasil pengujian kecepatan proses dalam bentuk diagram:

Pada gamabr 6.1 menunjukkan bahwa ukuran citra berpengaruh terhadap kecepatan proses. Semakin besar ukuran citra maka proses akan membutuhkan waktu yang lama. Hal ini terlihat pada grafik kecepatan proses berdasarkan ukuran citra. Pada Grafik kecepatan proses berdasarkan ukuran citra lamanya waktu proses berbanding lurus dengan besar ukuran citra. Sehingga ukuran citra berpengaruh dalam kecepatan proses aplikasi dalam melakukan enkripsi dan dekripsi.



Gambar 6.1 Grafik Kecepatan Proses Berdasarkan Ukuran Citra

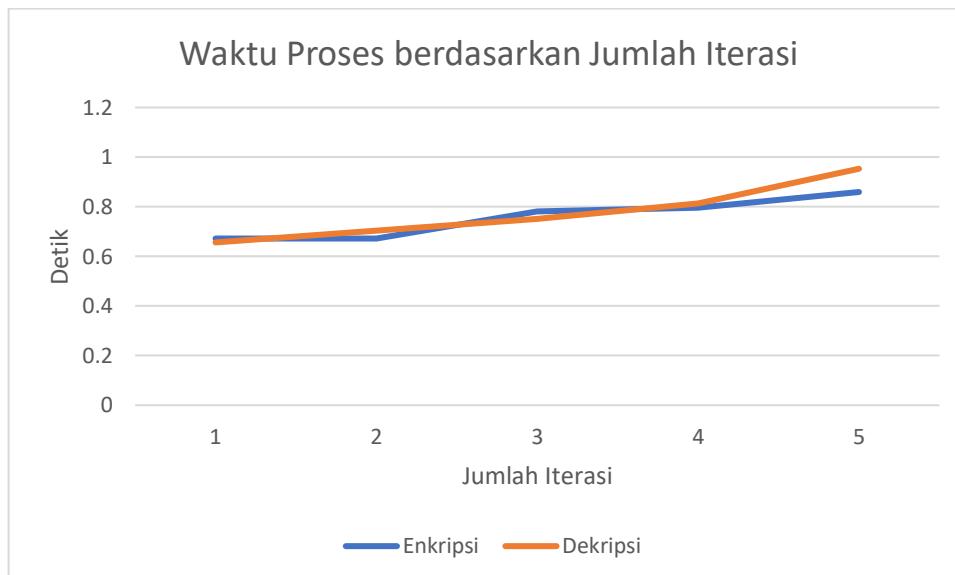
Pengujian kecepatan proses selanjutnya yaitu pengujian berdasarkan banyaknya iterasi yang dilakukan pada proses enkripsi atau proses dekripsi dengan menggunakan ukuran citra yang sama yaitu 128 x 128. Berikut hasil pengujian kecepatan proses berdasarkan jumlah iterasi:

Tabel 6.8 Uji Coba Kecepatan Proses berdasarkan Jumlah Iterasi

No	Jumlah Iterasi	Keterangan Citra	Waktu Enkripsi	Waktu Dekripsi
1.	1		0.671875 detik	0.65625 detik
2.	2		0.671880 detik	0.70313 detik
3.	3		0.781250 detik	0.750000 detik

No	Jumlah Iterasi	Keterangan Citra	Waktu Enkripsi	Waktu Dekripsi
4.	4		0.79688 detik	0.81250 detik
5.	5		0.85938 detik	0.95313 detik

Berikut merupakan penyajian kecepatan dalam bentuk grafik:



Gambar 6.2 Grafik Kecepatan Proses Berdasarkan Jumlah Iterasi

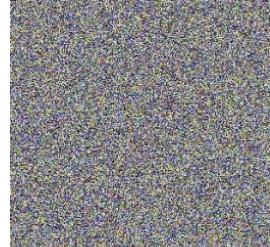
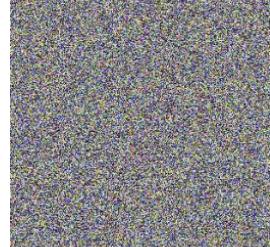
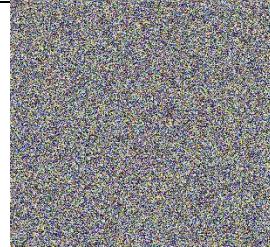
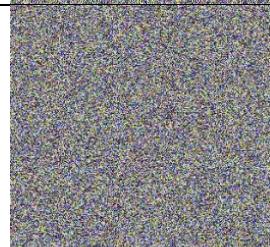
Pada gambar 6.2 menunjukkan bahwa grafik kecapatan proses yang semakin meningkat. Semakin banyak iterasi yang dilakukan maka semakin banyak waktu yang dibutuhkan. Namun, semakin banyak iterasi yang dilakukan maka citra akan lebih teracak.

6.2.4 Pengujian Tipe Data Penyimpanan

Pengujian selanjutnya yaitu pengujian penyimpanan dalam berbagai format penyimpanan yang berbeda. Pengujian dilakukan dengan citra dan kunci yang sama. Untuk citra menggunakan citra RGB dengan ukuran 304 x 304 yang memiliki

format .bmp dan memiliki *size* 361 Kb. Untuk kunci atau *secret key* menggunakan parameter $p = 19$, $q = 38$, $\text{iterasi} = 5$, $x = 0.67$, dan $r = 3.98$. Berikut citra uji coba Tipe Data penyimpanan:

Tabel 6.9 Hasil Pengujian Tipe Data Penyimpanan

No	Tipe Data	Ukuran File	Hasil Penyimpanan	Hasil Dekripsi
1.	Bitmap	361 KB		
2.	Png	272 KB		
3.	Jpeg	55.3 KB		
4.	Tiff	371 KB		
5.	Gif	93.1 KB		

Pada tabel 6.9 menunjukkan bahwa setiap tipe data penyimpanan memiliki ukuran file yang berbeda. Hal ini tergantung pada kompresi yang dimiliki oleh

setiap tipe data penyimpanan. Pada hasil uji coba di atas dapat dilihat dengan visual ada beberapa hasil dekripsi yang berbeda dari tipe data yang diuji cobakan. Dari hasil tersebut dapat dianalisa dengan perhitungan pengujian visual yaitu NPCR, UACI, MSE, dan PSNR. Berikut hasil analisa yang ditujukan pada tabel 6.10:

Tabel 6.10 Analisa Penyimpanan Citra

No	Tipe Data	Hasil Dekripsi	NPCR	UACI	MSE	PSNR
1.	Bitmap		0 %	0 %	0 %	∞ db
2.	Png		0 %	0 %	0 %	∞ db
3.	Jpeg		97.814%	14.430%	3420.5%	13.070db
4.	Tiff		0 %	0 %	0 %	∞ db
5.	Gif		97.627%	10.569%	2189.9%	44.202db

Pada tabel 6.10 menunjukkan bahwa hasil dekripsi dari tipe data *bitmap*, *png*, dan *tiff* menghasilkan nilai NPCR, UACI, MSE yaitu 0 dan PSNR dengan nilai tak hingga. Dengan hasil tersebut maka proses dekripsi menghasilkan citra yang

sama dengan citra asli. Sedangkan hasil dekripsi dari tipe data jpeg dan gif tidak menghasilkan citra yang sama dengan citra asli.

Pada hasil proses dekripsi haruslah bersifat *lossless* dimana citra hasil dekripsi sama dengan citra asli. Sedangkan untuk penyimpanan yang bersifat *lossy*, tidak dapat menghasilkan citra yang sama dengan citra asli. Uji coba diatas menunjukan bahwa tipe data penyimpanan *bitmap*, png, dan jpeg menghasilkan citra yang bersifat *lossless*. Dilihat dari ukuran penyimpanan tipe data png lebih kecil dari pada *bitmap* dan tif. Dapat ditarik kesimpulan bahawa penyimpanan terbaik yaitu dengan tipe data png.

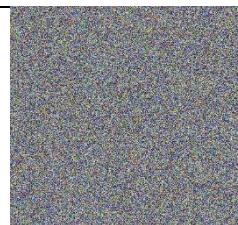
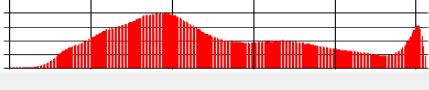
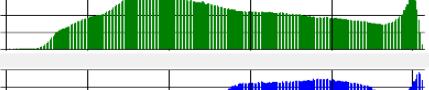
6.2.5 Pengujian dan Analisa Histogram

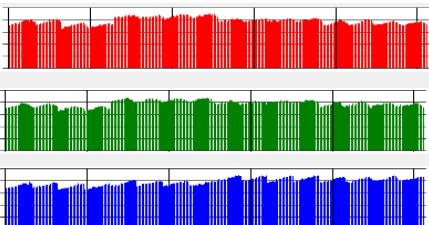
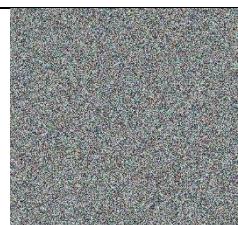
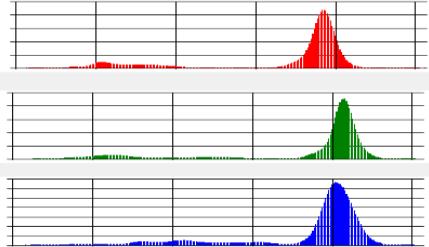
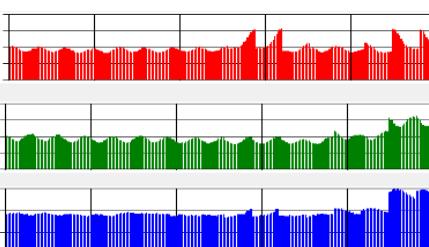
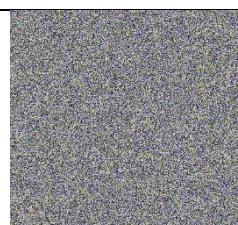
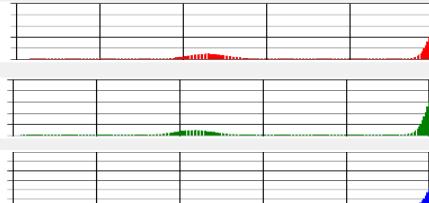
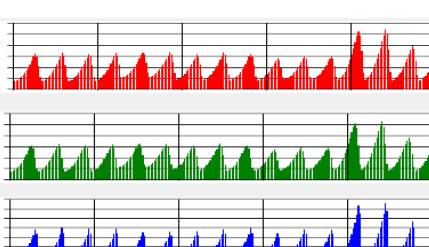
Di dalam bidang pengolahan citra histogram memperlihatkan distribusi nilai *pixel* di dalam sebuah citra. Histogram digunakan penyerang (*attacker*) untuk melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan *pixel* di dalam histogram.

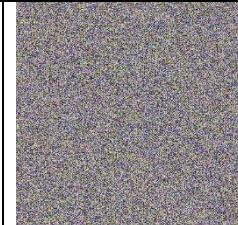
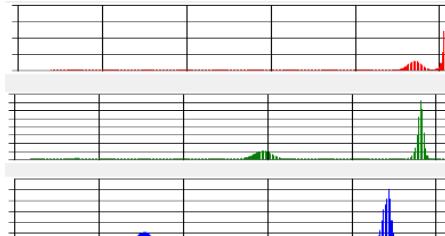
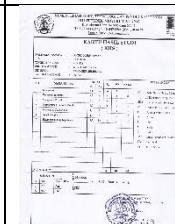
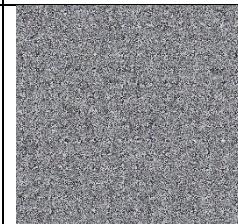
Dalam pengujian histogram diharapkan histogram dari citra terenkripsi memiliki histogram yang berbeda secara signifikan atau secara statistic tidak memiliki kemiripan. Oleh Karena itu, histogram citra terenkripsi seharusnya datar (*flat*) atau secara statistic memiliki distribusi (relative) *uniform*. Distribusi yang (relatif) *uniform* pada *cipher-image* adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki tingkat keamanan yang bagus [12].

Pengujian histogram dilakukan pada lima citra dokumen hasil *scan* yang berbeda dengan menggunakan kunci yang sama menggunakan parameter $p = 19$, $q = 38$, iterasi = 5, $x = 0.67$, dan $r = 3.98$. Berikut hasil pengujian histogram:

Tabel 6.11 Pengujian Histogram

No	Citra Asli	Citra Terenkripsi	Histogram
1.			<p>Citra Asli:</p>   

			<i>Cipher-image:</i> 
2.			<i>Citra Asli:</i>  <i>Cipher-image:</i> 
3.			<i>Citra Asli:</i>  <i>Cipher-image:</i> 

4.			<p>Citra Asli:</p> 
5.			<p>Citra Asli:</p> 

Pada tabel 6.11 menunjukkan hasil dari pengujian histogram dari lima citra dokumen hasil *scan* yang berbeda. Dapat dilihat histogram citra terenkripsi (*cipher-image*) dengan histogram citra asli memiliki berbedaan yang signifikan. Ada beberapa histogram dari citra terenkripsi yang mendekati datar yaitu citra nomer 1 dan 2. Dari uji coba tersebut datarnya suatu histogram selain dipengaruhi oleh algoritma enkripsi pada citra juga dipengaruhi oleh banyaknya warna yang

menyusun pada citra tersebut. Dapat disimpulkan bahwa sistem enkripsi pada citra digital dokumen hasil *scan* dapat membuat histogram citra terenkripsi berbeda secara signifikan dengan citra asli sehingga akan mempersulit kriptanalisis untuk menentukan gambar aslinya.

6.2.6 Pengujian dan Analisa Entropi

Di dalam teori informasi, entropi menyatakan derajat ketidakpastian. Persamaan Entropi sudah dijelaskan pada bab sebelumnya pada persamaan 2.14. Pada kasus enkripsi citra, citra terenkripsi (*cipher-image*) yang dihasilkan adalah citra acak, maka entropinya seharusnya ideal 8.

Pada pengujian Entropi ada 2 parameter yang akan dianalisa yaitu:

1. Penggunaan Kunci yang berbeda pada citra yang sama.
2. Penggunaan Kunci yang sama pada citra yang berbeda.

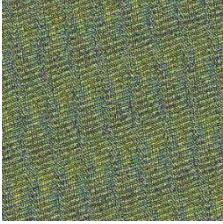
6.2.6.1 Penggunaan Kunci yang berbeda pada citra yang sama

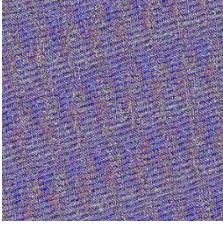
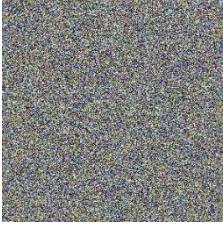
Analisa dilakukan untuk melihat penggunaan kunci yang dapat memberikan tingkat keamanan pada saat proses enkripsi. Pada Analisa ini berfokus pada penggunaan nilai x dan r karena merupakan paremeter dari *Logistic Map* yang berfungsi untuk membangkitkan *keystream*. *Keystream* berfungsi untuk melakukan proses XOR dengan 4-bit MSB dari citra. Dikatakan aman jika nilai entropi mendekati 8. Berikut hasil pengujinya:



Gambar 6.3 Citra Uji Entropi

Tabel 6.12 Hasil Uji Entropi Berdasarkan *Secret Key*

No	Kunci	Citra Terenkripsi	Entropi		
			Red	Green	Blue
1.	$p = 86, q = 46,$ $\text{iterasi} = 5,$ $x = 0.15, r = 1.37$		NaN	NaN	NaN

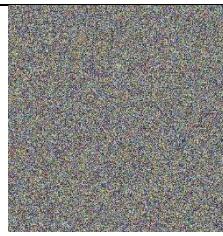
No	Kunci	Citra Terenkripsi	Entropi		
			Red	Green	Blue
2.	$p = 86, q = 46,$ $\text{iterasi} = 5,$ $x = 0.53, r = 2.27$		NaN	NaN	NaN
3.	$p = 86, q = 46,$ $\text{iterasi} = 5,$ $x = 0.87, r = 3.89$		7.96426	7.96760	7.92952

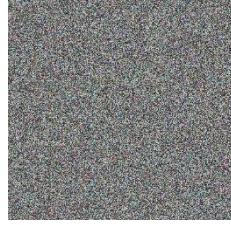
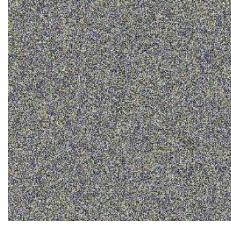
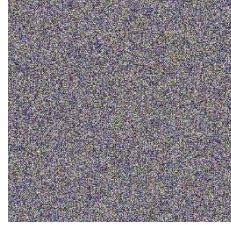
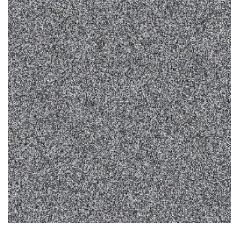
Dari hasil pengujian diatas menunjukan bahwa untuk penggunaan parameter $x = 0.87$ dan $r = 3.89$ memiliki nilai entropi mendekati 8. Dimana hal ini menunjukan tingkat keamanan pada citra terenkripsi. Dapat ditarik kesimpulan bahwa untuk memberikan tingkat keamanan pada citra terenkripsi dapat menggunakan nilai x mendekati 1 dan nilai r mendekati 4.

6.2.6.2 Penggunaan Kunci yang sama pada citra yang berbeda

Dari hasil pengujian sebelumnya didapatkan kombinasi kunci yang memberikan nilai tingkat keamanan pada citra dengan nilai entropi mendekati 8. Selanjutnya dengan menggunakan kunci yang sama diuji cobakan ke beberapa citra yang berbeda. Kunci yang digunakan yaitu dengan parameter $p = 86, q = 46, \text{iterasi} = 5, x = 0.87, \text{dan } r = 3.89$. Di bawah ini merupakan hasil pengujian:

Tabel 6.13 Hasil Uji Entropi berdasarkan Warna pada Citra

No	Citra Asli	Citra Terenkripsi	Entropi		
			Red	Green	Blue
1.			7.99835	7.99877	7.99659

2.			7.98407	7.97615	7.98099
3.			7.84164	7.85031	7.75785
4.			7.39140	7.62342	7.77100
5.			6.8298	6.8408	6.5433

Pada tabel 6.13 menyajikan bahwa nilai entropi dari citra terenkripsi (*cipher-image*) 1, 2, dan 3 memiliki nilai mendekati 8. Sedangkan citra terenkripsi no 4 dan 5 memiliki nilai kurang dari 8. Hal ini menunjukan bahwa nilai entropi juga dipengaruhi oleh banyaknya warna yang menyusun pada citra tersebut. Dapat disimpulkan bahwa metode atau algoritma enkripsi yang diterapkan pada citra digital dokumen hasil *scan* aman dari serangan entropi (*entropy attack*) sebesar 99%.

BAB VII. KESIMPULAN

Pada bab ini menjelaskan tentang kesimpulan yang didapat pada saat proses pengeraanskripsi melalui uji coba yang dilakukan dan Analisa yang digunakan dalam penelitian. Bab ini juga berisi saran yang bisa dilakukan untuk penelitian di masa yang akan datang.

7.1 Kesimpulan

Kesimpulan dari skripsi yang berjudul “Implementasi Enkripsi Dan Dekripsi Pada Citra Digital Dokumen Hasil Scan Menggunakan Metode *Arnold Cat Map* Dan *Logistic Map*” sebagai berikut:

1. Dalam pengujian visual, proses enkripsi dan dekripsi dinyatakan berhasil. Dengan dibuktikan kesamaan citra asli dan citra hasil proses dekripsi sebesar 100% pada analisa yang dilakukan.
2. Metode yang diterapkan aman terhadap serangan kunci. Dibuktikan dengan sensifitas terhadap kunci yang diberikan. Kunci pada proses enkripsi harus sama dengan proses dekripsi, jika tidak maka citra tidak bisa kembali seperti citra asli.
3. Dalam kecepatan proses, dipengaruhi oleh beberapa faktor diantara ukuran citra dan iterasi pengacakan yang dilakukan. Semakin besar ukuran citra, maka waktu yang dibutuhkan akan lama. Semakin banyak iterasi yang dilakukan membuat proses semakin lama, namun banyaknya iterasi berpengaruh pada pengacakan yang lebih baik.
4. Penyimpanan dengan format .png merupakan format penyimpanan yang terbaik. Dengan memiliki ukuran yang paling kecil dan dapat memberikan hasil dekripsi dengan kecocokan 100% pada analisa yang dilakukan.
5. Pada pengujian histogram, metode yang diterapkan pada enkripsi citra digital dokumen hasil *scan* memberikan histogram citra terenkripsi (*cipher-image*) berbeda secara signifikan dengan histogram citra asli. sehingga akan mempersulit kriptanalisis untuk menentukan gambar aslinya Namun masih belum sepenuhnya membuat histogram datar pada beberapa citra yang diuji cobakan.

6. Pengujian entropi memberikan nilai mendekati 8, sehingga metode yang diterapkan aman dari kebocoran informasi.

7.2 Saran

Dalam pembuatan skripsi ini masih banyak hal yang dapat dilakukan untuk penelitian selanjutnya, diantaranya:

1. Untuk penelitian lebih lanjut dapat dikembangkan metode yang dapat memberikan histogram pada berbagai citra hasil dekripsi mendekati datar.
2. Untuk penelitian lebih lanjut dapat menambahkan algoritma keamanan enkripsi pada citra selain proses pengacakan *pixel* dan proses XOR untuk peningkatan kemanan yang lebih baik.
3. Penggunaan kunci yang berbeda pada saat proses enkripsi dan dekripsi. Misalkan menggunakan kunci *private* untuk proses enkripsi dan kunci *public* untuk proses dekripsi. Sehingga mempersulit kriptanalisis untuk membongkar informasi pada citra.
4. Pengembangan aplikasi untuk media *mobile* dan web.

DAFTAR PUSTAKA

- [1] Pengertian Scanner Dan Fungsinya Dilengkapi Cara Kerjanya. 2015 [Online]
Tersedia:
<http://www.pengertianku.net/2015/02/pengertian-scanner-dan-fungsinyadilengkapi-cara-kerjanya.html> [26 Januari 2017]
- [2] Pengertian dan Fungsi Scanner. 2014 [Online]
Tersedia:
<http://www.solusikompi.com/2014/08/pengertian-dan-fungsi-scanner.html>
[26 Januari 2017]
- [3] Dhian Sweetania, ST., MMSI. 2015. "Metode Endkripsi Dekripsi". [Online]
Tersedia:
http://dhian_sweetania.staff.gunadarma.ac.id/Downloads/files/35348/Enkripsi-I.pdf [17 Desember 2016]
- [4] Ariyus Dony, "Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi".
Yogyakarta: Penerbit ANDI, 2008
- [5] Pengertian citra digital. 2013 [Online]
Teredia:
<http://www.temukanpengertian.com/2013/08/pengertian-citra-digital.html>
[17 Desember 2016]
- [6] Pengertian citra digital. 2012 [Online]
Tersedia:
<http://repository.usu.ac.id/bitstream/123456789/31325/4/Chapter%20II.pdf>
[18 Desember 2016]
- [7] Munir Rinaldi. "Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi Dan Teknik Substitusi Menggunakan Arnold Cat Map Dan Logistic Map" in Prosiding Seminar Nasional Pendidikan Teknik Informatika (SENAPATI 2012), Singaraja, 2012, ISSN 2087-2658
- [8] Irfan Pahrul dan Prayudi Yudi. 2015. "Penggabungan Algoritma Chaos dan Rivers Shamir Adleman (RSA) Untuk Peningkatan Keamanan Citra".
[Online]

Tersedia:

<http://journal.uii.ac.id/index.php/Snati/article/view/3535>

[18 Desember 2016]

[9] Pengenalan Visual Basic.NET 2015[Online] Tersedia:

<http://www.pendidikanmu.com/2015/02/pengenalan-visual-basic-net-2005.html> [24 Mei 2017]

[10] Zolyviade Zarcelonia, "Perancangan Aplikasi Perbesaran Citra dengan Metode Proyeksi Cahaya," 2014.

[11] Prabowo Yudhi, Hidayatno Achmad, dan Aj Julian Ajub. "Kompresi Citra Digital Aras-Keabuan Menggunakan Metode Hadamard". Jurusan Teknik Elektro, Fakultas Teknik, Universitas Diponegoro, 2012

[12] Munir Rinaldi. "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map Dan Penerapan Teknik Selektif", JUTI. Volume 10, Nomor 2, Juli 2012: 89 – 95

[13] Perbedaan Format Gambar JPG, GIF, PNG, dan TIFF. 2010 [Online]

Tersedia:

<http://www.idseducation.com/articles/perbedaan-format-gambar-jpg-gif-png-dan-tiff/> [24 Mei 2017]

[14] Andri Yoga, Andrie Rosa, dan Retno Ariadi. "Implementasi Enkripsi Digital Pada Citra Dokumen Menggunakan Algoritma Kubus Rubik Dengan Pembangkit Kunci Md5". Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang, 2016

LAMPIRAN

Lampiran 1. Source Code Aplikasi

1. Fungsi Permutasi Arnod Cat Map

```
Function PermutationACM(img As Image, p As Integer, q As Integer, m As Integer) As Image
    'Membuat variabel sejumlah M
    Dim arrImage(m) As Bitmap
    For k As Integer = 0 To arrImage.Length - 1
        arrImage(k) = New Bitmap(img)
    Next

    Dim i As Integer
    Dim xnn, ynn, x, y, iteration As Integer

    iteration = m
    For i = 0 To iteration - 1
        For x = 0 To img.Width - 1
            For y = 0 To img.Height - 1
                '-----Arnold Cat Map-----
                xnn = (x + (p * y))
                ynn = ((q * x) + (((p * q) + 1) * y))

                xnn = ModOperation(xnn, img.Width)
                ynn = ModOperation(ynn, img.Height)

                Dim clr As Color = arrImage(i).GetPixel(x, y)
                arrImage(i + 1).SetPixel(xnn, ynn, clr)
            Next
        Next
        ProgBarPermutation.Value = Int(100 * i / iteration + 1)
    Next
    ProgBarPermutation.Value = 100

    Return arrImage(m)

End Function
```

2. Fungsi Invers Permutasi Arnod Cat Map

```
Function InversePermutationACM(img As Image, p As Integer, q As Integer, m As Integer) As Image
    Dim arrImage(m) As Bitmap
    For k As Integer = 0 To arrImage.Length - 1
        arrImage(k) = New Bitmap(img)
    Next

    Dim i As Integer
    Dim xn, yn, x, y, iteration As Integer

    Dim Adterminan As Double = 1 / ((p * q + 1) - (p * q))

    iteration = m
    For i = 0 To iteration - 1
        For xn = 0 To img.Width - 1
            For yn = 0 To img.Height - 1
```

```

'-----Inverse Arnold Cat Map-----
x = (((p * q) + 1) * xn) + (-p * yn))
y = ((-q * xn) + yn)

x = ModOperation(x, img.Width)
y = ModOperation(y, img.Height)

Dim clr As Color = arrImage(i).GetPixel(xn,
yn)
arrImage(i + 1).SetPixel(x, y, clr)
Next
Next
ProgBarPermutation.Value = Int(100 * i / iteration)
Next
ProgBarPermutation.Value = 100

Return arrImage(m)
End Function

```

3. Ekstraksi 4-bit MSB setiap pixel

```

Public Sub getMSBimageRandom(img As Image)
    Dim image1 As New Bitmap(img)
    Dim merah, hijau, biru As Integer
    arrPixelRandomRed = New String(image1.Width, image1.Height)
    {}
    arrPixelRandomGreen = New String(image1.Width, image1.Height)
    {}
    arrPixelRandomBlue = New String(image1.Width, image1.Height)
    {}

    Dim count As Integer = 0
    For baris = 0 To image1.Width - 1
        For kolom = 0 To image1.Height - 1
            merah = image1.GetPixel(baris, kolom).R
            hijau = image1.GetPixel(baris, kolom).G
            biru = image1.GetPixel(baris, kolom).B

            arrPixelRandomRed(baris, kolom) = "" & GetMSB(merah)
            arrPixelRandomGreen(baris, kolom)= "" & GetMSB(hijau)
            arrPixelRandomBlue(baris, kolom) = "" & GetMSB(biru)

            count += 1
        Next
        ProgBarMsb.Value = Int(100 * baris / image1.Width + 1)
    Next
    ProgBarMsb.Value = 100
End Sub

```

4. Iterasi *Logistic Map*

```

Public Sub LogisticMapIteration(x0 As Double, r As Double,
sizeOfInteger As Integer, image As Image)
    Dim numberInteger As String
    Dim image1 As New Bitmap(image)
    Dim listX0 As New List(Of Double)
    listLogisticMap = New String(image1.Width, image1.Height) {}
    For baris = 0 To image1.Width - 1

```

```

For kolom = 0 To image1.Height - 1
    x0 = ((r * x0 * (1 - x0)))
    numberInteger = Strings.Mid(x0.ToString(), 3,
sizeOfInteger)
    listLogisticMap(baris, kolom) = "" &
GetLSB(CInt(numberInteger))
    Next
    ProgBarLogisticMap.Value = Int(100 * baris /
image1.Width)
    Next
    ProgBarLogisticMap.Value = 100
End Sub

```

5. Proses Enkripsi *Pi XOR Ki*

```

Public Sub EnkripsiPiKi(piRed(),) As String, piGreen(),) As String,
piBlue(),) As String, ki(),) As String)
    arrEnkripPiKiRed = New String(piRed.GetLength(0),
piRed.GetLength(1)) {}
    arrEnkripPiKiGreen = New String(piRed.GetLength(0),
piRed.GetLength(1)) {}
    arrEnkripPiKiBlue = New String(piRed.GetLength(0),
piRed.GetLength(1)) {}

    For baris = 0 To piRed.GetLength(0) - 1
        For kolom = 0 To piRed.GetLength(1) - 1
            arrEnkripPiKiRed(baris, kolom) = "" &
XOROperation(piRed(baris, kolom), ki(baris, kolom))
            arrEnkripPiKiGreen(baris, kolom) = "" &
XOROperation(piGreen(baris, kolom), ki(baris, kolom))
            arrEnkripPiKiBlue(baris, kolom) = "" &
XOROperation(piBlue(baris, kolom), ki(baris, kolom))
        Next
        ProgBarEnkripsi.Value = Int(100 * baris /
piRed.GetLength(0) + 1)
    Next

    ProgBarEnkripsi.Value = 100
End Sub

```

6. Proses Dekripsi *Ci XOR Ki*

```

Public Sub DekripsiCiKi(ciRed(),) As String, ciGreen(),) As String,
ciBlue(),) As String, ki(),) As String)
    arrDekripCiKiRed = New String(ciRed.GetLength(0),
ciRed.GetLength(1)) {}
    arrDekripCiKiGreen = New String(ciRed.GetLength(0),
ciRed.GetLength(1)) {}
    arrDekripCiKiBlue = New String(ciRed.GetLength(0),
ciRed.GetLength(1)) {}

    For baris = 0 To ciRed.GetLength(0) - 1
        For kolom = 0 To ciRed.GetLength(1) - 1
            arrDekripCiKiRed(baris, kolom) =
XOROperation(ciRed(baris, kolom), ki(baris, kolom))
            arrDekripCiKiGreen(baris, kolom) =
XOROperation(ciGreen(baris, kolom), ki(baris, kolom))
            arrDekripCiKiBlue(baris, kolom) =
XOROperation(ciBlue(baris, kolom), ki(baris, kolom))
        Next
    Next

```

```

        Next
ProgBarEnkripsi.Value = Int(100 * baris / ciRed.GetLength(0) + 1)
        Next
ProgBarEnkripsi.Value = 100
End Sub

```

7. Proses menggantikan 4-bit MSB dari setiap *pixel*

```

Public Function SetPixcel(image1 As Bitmap, listRed(,) As String,
listGreen(,) As String, listBlue(,) As String) As Image
    Dim image2 As New Bitmap(image1)
    Dim merah, hijau, biru As Integer
    Dim LSBRed As String
    Dim newBinerRed As String
    Dim Rnew As Integer

    Dim LSBGreen As String
    Dim newBinerGreen As String
    Dim Gnew As Integer

    Dim LSBBBlue As String
    Dim newBinerBlue As String
    Dim Bnew As Integer

    Dim i As Integer = 0
    For baris = 0 To image1.Width - 1
        For kolom = 0 To image1.Height - 1
            merah = image1.GetPixel(baris, kolom).R
            hijau = image1.GetPixel(baris, kolom).G
            biru = image1.GetPixel(baris, kolom).B

            'Mencari nilai merah baru
            LSBRed = GetLSB(merah)
            newBinerRed = listRed(baris, kolom) & "" & LSBRed
            Rnew = ConvertBinerToDecimal(newBinerRed)

            'Mencari nilai hijau baru
            LSBGreen = GetLSB(hijau)
            newBinerGreen = listGreen(baris, kolom) & "" & LSBGreen
            Gnew = ConvertBinerToDecimal(newBinerGreen)

            'Mencari nilai biru baru
            LSBBBlue = GetLSB(biru)
            newBinerBlue = listBlue(baris, kolom) & "" & LSBBBlue
            Bnew = ConvertBinerToDecimal(newBinerBlue)

            image2.SetPixel(baris, kolom, Color.FromArgb(Rnew,
Gnew, Bnew))

            i = i + 1
        Next
        ProgBarSet.Value = Int(100 * baris / image1.Width + 1)
    Next
    ProgBarSet.Value = 100
    Return image2
End Function

```

8. Proses Membuka Citra

```
OpenFileDialog1.Title = "Open Image"
    OpenFileDialog1.Filter = "Image
File|*.bmp;*.jpg;*.png;*.jpeg;*.gif;*.tiff"
    If OpenFileDialog1.ShowDialog() = Windows.Forms.DialogResult.OK
Then
    If PB_input.Width <> PB_input.Height Then
        PB_input.Image =
ResizeImage(Image.FromFile(OpenFileDialog1.FileName))
    Else
        PB_input.Image =
Image.FromFile(OpenFileDialog1.FileName)
    End If
    lblSize1.Text = PB_input.Image.Width & " x " &
PB_input.Image.Height
End If
```

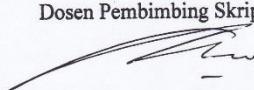
9. Fungsi Menyimpan Citra

```
Private Sub save(output As PictureBox)
    Dim saveFileDialog1 As New SaveFileDialog()
    saveFileDialog1.Filter = "Bitmap Image|*.bmp|Jpeg
Image|*.jpeg|PNG Image|*.png|Tiff Image|*.tiff|Gif Image|*.gif"
    saveFileDialog1.Title = "Save an Image File"

    If saveFileDialog1.ShowDialog() = Windows.Forms.DialogResult.OK
Then
    Select Case saveFileDialog1.FilterIndex
        Case 1
            output.Image.Save(saveFileDialog1.FileName,
ImageFormat.Bmp)
        Case 2
            output.Image.Save(saveFileDialog1.FileName,
ImageFormat.Jpeg)
        Case 3
            output.Image.Save(saveFileDialog1.FileName,
ImageFormat.Png)
        Case 4
            output.Image.Save(saveFileDialog1.FileName,
ImageFormat.Tiff)
        Case 5
            output.Image.Save(saveFileDialog1.FileName,
ImageFormat.Gif)
    End Select
End If
End Sub
```

Lampiran 2. Lembar Bimbingan Pembimbing

	KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI POLITEKNIK NEGERI MALANG JURUSAN TEKNOLOGI INFORMASI PROGRAM STUDI TEKNIK INFORMATIKA JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122			
NO SKRIPSI: 05				
LEMBAR BIMBINGAN SKRIPSI 2016/2017				
JUDUL : IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP DAN LOGISTIC MAP				
Nama : Anggi Kurniawan		NIM : 1341180028		
No.	Tanggal	Materi Bimbingan	Tanda Tangan	
			Mahasiswa	Dosen
1.	22 - 2 - 2017	Konsultasi Aplikasi'	<i>Am</i>	<i>Am</i>
2.	1 - 3 - 2017	Konsultasi Aplikasi'	<i>Am</i>	<i>Am</i>
3.	8 - 3 - 2017	TF SCALE	<i>Am</i>	<i>Am</i>
4.	15 - 3 - 2017	TF SCALE	<i>Am</i>	<i>Am</i>
5.	22 - 3 - 2017	Implementasi'	<i>Am</i>	<i>Am</i>
6.	29 - 3 - 2017	Progres	<i>Am</i>	<i>Am</i>
7.	05 - 4 - 2017	Progres	<i>Am</i>	<i>Am</i>
8.	12 - 4 - 2017	Progres	<i>Am</i>	<i>Am</i>
9.	19 - 4 - 2017	Penyajian dan analisa	<i>Am</i>	<i>Am</i>
10.	26 - 4 - 2017	Revisi: penyajian dan analisa	<i>Am</i>	<i>Am</i>
11.	3 - 5 - 2017	Bab I , II - VI	<i>Am</i>	<i>Am</i>
12.	17 - 5 - 2017	Bab IV, V, VI, VII	<i>Am</i>	<i>Am</i>
13.	31 - 5 - 2017	Makalah	<i>Am</i>	<i>Am</i>
14.				
15.				
16.				
17.				
18.				
19.				

Malang, 31 Mei 2017...
 Dosen Pembimbing Skripsi,

DR. Eng. Rosa Andrie Asmara ST., MT.
 NIP. 198010102005011001



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI MALANG
JURUSAN TEKNOLOGI INFORMASI
PROGRAM STUDI TEKNIK INFORMATIKA
JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122



NO SKRIPSI: 05

LEMBAR BIMBINGAN SKRIPSI 2016/2017

JUDUL : IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL
DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP
DAN LOGISTIC MAP

Nama : Anggi Kurniawan

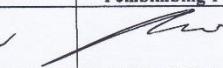
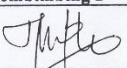
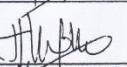
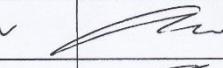
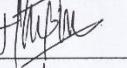
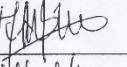
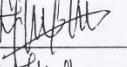
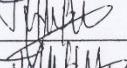
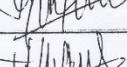
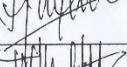
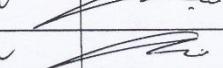
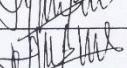
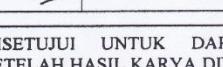
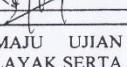
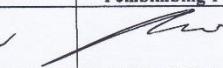
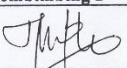
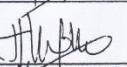
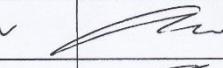
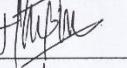
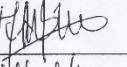
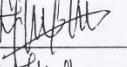
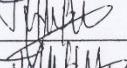
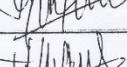
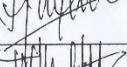
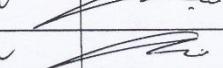
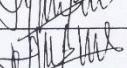
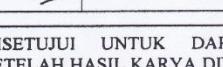
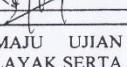
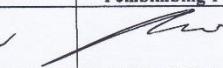
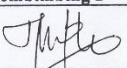
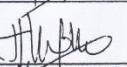
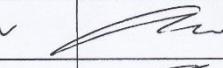
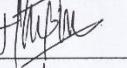
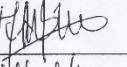
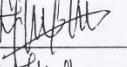
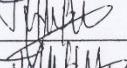
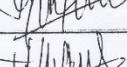
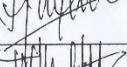
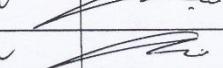
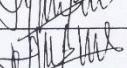
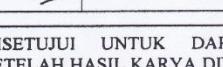
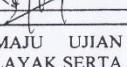
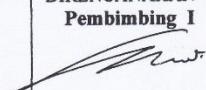
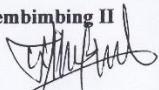
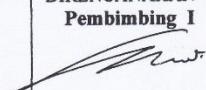
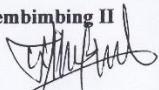
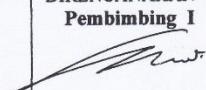
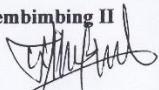
NIM : 1341180028

No.	Tanggal	Materi Bimbingan	Tanda Tangan	
			Mahasiswa	Dosen
1.	10 - 3 - 2017	Flowchart Sistem	Ag	W
2.	13 - 3 - 2017	Resize Image	An	W
3.	24 - 3 - 2017	Bilinier Interpolation	An	W
4.	6 - 4 - 2017	Resize Image Bilinier Interpolation	An	W
5.	13 - 4 - 2017	Implementasi	An	W
6.	4 - 5 - 2017	Pengujian dan Analisa	An	W
7.	15 - 5 - 2017	Bab I, II dan III	An	W
8.	26 - 5 - 2017	Bab IV, V, VI, VII	An	W
9.	12 - 6 - 2017	Pencarian Masalah	An	W
10.	14 - 6 - 2017	Review Laporan Bab IV	An	W
11.	16 - 6 - 2017	Review Laporan Bab .	An	W
12.	21 - 6 - 2017	Review Program (Aplikasi)	An	W
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Malang, 22 Juni 2017.....
Dosen Pembimbing Skripsi,

Irawati Nurmala Sari, S.Kom., M.Sc
NIP.

Lampiran 3. Lembar Persetujuan Maju Ujian

	KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI POLITEKNIK NEGERI MALANG JURUSAN TEKNOLOGI INFORMASI PROGRAM STUDI TEKNIK INFORMATIKA JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122																																																											
		NO SKRIPSI: 05																																																										
LEMBAR PERSETUJUAN MENGIKUTI UJIAN SKRIPSI 2016/2017 PROGRAM STUDI TEKNIK INFORMATIKA																																																												
N A M A	: ANGGI KURNIAWAN N I M / K E L A S : 1341180028 / TI-4D																																																											
JUDUL SKRIPSI	: IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP DAN LOGISTIC MAP																																																											
PEMBIMBING	: 1. DR.Eng. Rosa Andrie Asmara ST., MT. 2. Irawati Nurmala Sari, S.Kom., M.Sc	NIP : 198010102005011001 NIP :																																																										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">No.</th> <th style="width: 50%;">Uraian / Bab</th> <th style="width: 15%;">Diselesaikan</th> <th style="width: 15%;">Tanda Tangan</th> </tr> <tr> <th></th> <th></th> <th style="text-align: center;">Pembimbing 1</th> <th style="text-align: center;">Pembimbing 2</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td>PENDAHULUAN</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>2.</td> <td>LANDASAN TEORI</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>3.</td> <td>METODOLOGI PENELITIAN</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>4.</td> <td>ANALISIS DAN PERANCANGAN</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>5.</td> <td>IMPLEMENTASI</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>6.</td> <td>PENGUJIAN DAN PEMBAHASAN</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>7.</td> <td>KESIMPULAN DAN SARAN</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>8.</td> <td>BAGIAN AKHIR - Daftar Pustaka - Lampiran (Isi lampiran disesuaikan dengan judul laporan akhir) - Profile Penulis (Riwayat Penulis)</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>9.</td> <td>Hardware/Software - Didemokan di depan pembimbing</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> <tr> <td>10</td> <td>Draft Makalah</td> <td style="text-align: center;">✓</td> <td style="text-align: center;"></td> <td style="text-align: center;"></td> </tr> </tbody> </table>			No.	Uraian / Bab	Diselesaikan	Tanda Tangan			Pembimbing 1	Pembimbing 2	1.	PENDAHULUAN	✓			2.	LANDASAN TEORI	✓			3.	METODOLOGI PENELITIAN	✓			4.	ANALISIS DAN PERANCANGAN	✓			5.	IMPLEMENTASI	✓			6.	PENGUJIAN DAN PEMBAHASAN	✓			7.	KESIMPULAN DAN SARAN	✓			8.	BAGIAN AKHIR - Daftar Pustaka - Lampiran (Isi lampiran disesuaikan dengan judul laporan akhir) - Profile Penulis (Riwayat Penulis)	✓			9.	Hardware/Software - Didemokan di depan pembimbing	✓			10	Draft Makalah	✓		
No.	Uraian / Bab	Diselesaikan	Tanda Tangan																																																									
		Pembimbing 1	Pembimbing 2																																																									
1.	PENDAHULUAN	✓																																																										
2.	LANDASAN TEORI	✓																																																										
3.	METODOLOGI PENELITIAN	✓																																																										
4.	ANALISIS DAN PERANCANGAN	✓																																																										
5.	IMPLEMENTASI	✓																																																										
6.	PENGUJIAN DAN PEMBAHASAN	✓																																																										
7.	KESIMPULAN DAN SARAN	✓																																																										
8.	BAGIAN AKHIR - Daftar Pustaka - Lampiran (Isi lampiran disesuaikan dengan judul laporan akhir) - Profile Penulis (Riwayat Penulis)	✓																																																										
9.	Hardware/Software - Didemokan di depan pembimbing	✓																																																										
10	Draft Makalah	✓																																																										
Malang, Ketua Pelaksana LA & SKRIPSI 2016/2017 Program Studi Teknik Informatika																																																												
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: auto;"> <p style="text-align: center; margin: 0;">DISETUJUI UNTUK DAPAT MAJU UJIAN SETELAH HASIL KARYA DINILAI LAYAK SERTA HASIL UJI SESUAI DENGAN SPESIFIKASI YANG DIRENCANAKAN</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center; padding: 5px;"> Pembimbing I  </td> <td style="width: 50%; text-align: center; padding: 5px;"> Pembimbing II  </td> </tr> <tr> <td colspan="2" style="text-align: center; padding: 5px;"> DR.Eng. Rosa Andrie Asmara ST.,MT. NIP. 198010102005011001 Irawati Nurmala Sari, S.Kom., NIP. </td> </tr> </table> </div>			Pembimbing I 	Pembimbing II 	DR.Eng. Rosa Andrie Asmara ST.,MT. NIP. 198010102005011001 Irawati Nurmala Sari, S.Kom., NIP.																																																							
Pembimbing I 	Pembimbing II 																																																											
DR.Eng. Rosa Andrie Asmara ST.,MT. NIP. 198010102005011001 Irawati Nurmala Sari, S.Kom., NIP.																																																												
Arief Prasetyo, S.Kom., M.Kom. NIP. 19790313 200812 1 002																																																												
FRM.RTI.01,49.04																																																												

Lampiran 4. Lembar Revisi



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI MALANG
JURUSAN TEKNOLOGI INFORMASI
PROGRAM STUDI TEKNIK INFORMATIKA
JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122



FORM REVISI SKRIPSI

No. Skripsi: 05

Nama Mahasiswa : Anggi Kurniawan NIM : 1341180028
 Tanggal Ujian : ...
 Judul : Implementasi Enkripsi Dan Dekripsi Pada Citra Digital
 Dokumen Hasil Scan Menggunakan Metode Arnold Cat Map
 Dan Logistic Map

NO	SARAN PERBAIKAN	PARAF
1	flowchart dibuat standar bahasanya.	RPM
2	beratkan contoh enkripsi dan deskripsi seterbaik pada citra ukuran 3x3	PL

Malang, 16 Juni 2017

Dosen Pengaji

(Cahya R....)

FORM VERIFIKASI:

Laporan Akhir telah diperbaiki sesuai dengan saran perbaikan dari dosen pengaji.

PENGUJI/PEMBIMBING	NAMA	TTD	TANGGAL
Pengaji	Cahya R	RPM	16/6/2017
Pembimbing 1	Dr. Eng. Rosa Andrie A., S.T., M.T.	RA	17/6/2017
Pembimbing 2	Irawati Nurmala Sari, S.Kom., M.Sc	IRAWATI	17/6/2017

FRM.RTI.01.35.03



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
 POLITEKNIK NEGERI MALANG
 JURUSAN TEKNOLOGI INFORMASI
 PROGRAM STUDI TEKNIK INFORMATIKA

JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122



FORM REVISI SKRIPSI

No. Skripsi: 05

Nama Mahasiswa : Anggi Kurniawan NIM : 1341180028
 Tanggal Ujian : 02/07/2017
 Judul : Implementasi Enkripsi Dan Dekripsi Pada Citra Digital
 Dokumen Hasil Scan Menggunakan Metode Arnold Cat Map
 Dan Logistic Map

NO	SARAN PERBAIKAN	PARAF
1.	Alen penyimpanan berlaku dan informasi.	<i>[Signature]</i>
2.	Proses Entropi yg dilakukan klo yg - send htr key? - pixel?	<i>[Signature]</i>
3.	Uj. coba generate key dgn berlaku bilat jta memungkinkan?	<i>[Signature]</i>

Malang, 02/07/2017
 Dosen Pengaji

[Signature] Irawati Nurmala Sari, M.Sc

FORM VERIFIKASI:

Laporan Akhir telah diperbaiki sesuai dengan saran perbaikan dari dosen pengaji.

PENGUJI/PEMBIMBING	NAMA	TTD	TANGGAL
Pengaji	Irawati Nurmala Sari, M.Sc	<i>[Signature]</i>	21-6-2017
Pembimbing 1	Dr. Eng. Rosa Andrie A., S.T., M.T.	<i>[Signature]</i>	21-6-2017
Pembimbing 2	Irawati Nurmala Sari, S.Kom., M.Sc	<i>[Signature]</i>	21-6-2017

FRM.RTI.01.35.03



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI MALANG
JURUSAN TEKNOLOGI INFORMASI
PROGRAM STUDI TEKNIK INFORMATIKA

JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122



No. Skripsi: 05

FORM REVISI SKRIPSI

Nama Mahasiswa : Anggi Kurniawan NIM : 1341180028
Tanggal Ujian : 8 Juni 2017
Judul : Implementasi Enkripsi Dan Dekripsi Pada Citra Digital
Dokumen Hasil Scan Menggunakan Metode Arnold Cat Map
Dan Logistic Map

NO	SARAN PERBAIKAN	PARAF
1.	Cek laporan halaman pengaturan margin). Hal 16, 23, 25	<i>[Signature]</i>
2.	Beri penjelasan di setiap tabel. Hal 26 - 29 dan cek tabel yang terpotong lainnya	<i>[Signature]</i>
3.	Typo hal 31 (33, 38)	<i>[Signature]</i>
4.	Beri penjelasan range setiap parameter lebih pada program agar user mengetahui key (P, q, Iteration)	<i>[Signature]</i>

Malang, 8 Juni 2017
Dosen Pengaji,
[Signature] NS. S. Kurni, M.Sc

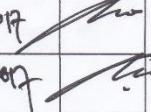
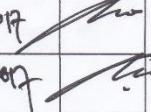
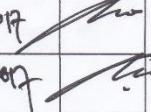
FORM VERIFIKASI:

Laporan Akhir telah diperbaiki sesuai dengan saran perbaikan dari dosen pengaji.

PENGUJI/PEMBIMBING	NAMA	TTD	TANGGAL
Pengaji			
Pembimbing 1	Dr. Eng. Rosa Andrie A., S.T., M.T.	<i>[Signature]</i>	21/6/2017
Pembimbing 2	Irawati Nurmala Sari, S.Kom., M.Sc	<i>[Signature]</i>	21/6/2017

FRM.RTI.01.35.03

Lampiran 5. Lembar Verifikasi

	KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI POLITEKNIK NEGERI MALANG JURUSAN TEKNOLOGI INFORMASI PROGRAM STUDI TEKNIK INFORMATIKA JL. Soekarno Hatta PO Box 04 Malang Telp. (0341) 404424 pes. 1122																		
No. Skripsi : 05																			
<u>FORM VERIFIKASI</u>																			
<u>ABSTRAK BAHASA INGGRIS DAN TATA TULIS BUKU SKRIPSI</u>																			
<p>Nama Mahasiswa : Anggi Kurniawan NIM :1341180028 Tanggal Ujian : 8 Juni 217 Judul : IMPLEMENTASI ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL DOKUMEN HASIL SCAN MENGGUNAKAN METODE ARNOLD CAT MAP DAN LOGISTIC MAP</p>																			
<table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th style="text-align: center;">NO</th><th style="text-align: center;">BAGIAN YANG DIVERIFIKASI</th><th style="text-align: center;">NAMA VERIFIKATOR</th><th style="text-align: center;">TANGGAL VERIFIKASI</th><th style="text-align: center;">TTD</th></tr></thead><tbody><tr><td style="text-align: center;">1</td><td>Abstrak Berbahasa Inggris</td><td>Dr.Eng. Rosa Andrie A.,ST.,M.T</td><td style="text-align: center;">2-8-2017</td><td style="text-align: center;"></td></tr><tr><td style="text-align: center;">2</td><td>Tata Tulis Buku Skripsi</td><td>Dr.Eng. Rosa Andrie A.,ST.,M.T</td><td style="text-align: center;">2-8-2017</td><td style="text-align: center;"></td></tr></tbody></table>					NO	BAGIAN YANG DIVERIFIKASI	NAMA VERIFIKATOR	TANGGAL VERIFIKASI	TTD	1	Abstrak Berbahasa Inggris	Dr.Eng. Rosa Andrie A.,ST.,M.T	2-8-2017		2	Tata Tulis Buku Skripsi	Dr.Eng. Rosa Andrie A.,ST.,M.T	2-8-2017	
NO	BAGIAN YANG DIVERIFIKASI	NAMA VERIFIKATOR	TANGGAL VERIFIKASI	TTD															
1	Abstrak Berbahasa Inggris	Dr.Eng. Rosa Andrie A.,ST.,M.T	2-8-2017																
2	Tata Tulis Buku Skripsi	Dr.Eng. Rosa Andrie A.,ST.,M.T	2-8-2017																
FRM.RTI.01.46.01																			

Lampiran 6. Biodata Mahasiswa

BIODATA MAHASISA



Nama Lengkap : Anggi Kurniawan
Nomor Induk Mahasiswa : 1341180028
Jurusan : Teknologi Informasi
Program Studi : Teknik Informatika
Jenis Kelamin : Laki – Laki
Tempat, tanggal lahir : Tulungagung, 02 Agustus 1994
Alamat Asal : RT/RW 02/01, Desa TalunKulon,
Kec. Bandung, Kab. Tulungagung
No. Telepon : 085791341410
Agama : Islam
Nama Ayah : Suyatno
Nama Ibu : Eni Endrawati

Riwayat Pendidikan

2001 – 2007 : SDN Tulungrejo II Tulungagung
2007 – 2010 : SMPN 1 Bandung Tulungagung
2010 – 2013 : SMAN 1 Boyolangu Tulungagung
2013 - Sekarang : D4 Teknik Informatika Politeknik Negeri Malang