

**YAYASAN LEMBAGA PENDIDIKAN ISLAM DAERAH RIAU  
UNIVERSITAS ISLAM RIAU  
FAKULTAS TEKNIK**

---

**ANALISIS KEAMANAN ALGORITMA ENKRIPSI CITRA  
MENGUNAKAN BAKER'S MAP DAN  
LOGISTIC MAP**

**SKRIPSI**

*Diajukan Untuk Memenuhi Salah Satu Syarat Penyusunan  
Laporan Skripsi Pada Fakultas Teknik  
Universitas Islam Riau Pekanbaru*

**Oleh:**

**NOVIA RISKA ARSELA  
143510222**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS ISLAM RIAU  
PEKANBARU  
2019**

## LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : Novia Riska Arsela  
NPM : 143510222  
Jurusan : Teknik  
Program Studi : Teknik Informatika  
Jenjang Pendidikan : Strata Satu (S1)  
Judul Skripsi : Analisis Keamanan Algoritma Enkripsi Citra Menggunakan  
Baker's Cipher

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria-kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 4 Oktober 2019

Disetujui Oleh  
**PEKANBARU**

Dosen Pembimbing

  
APRI SISWANTO, S.Kom., M.Kom

Disahkan Oleh :



Ketua Prodi Teknik Informatika  
  
AUSE LABEL LAPANSA, ST., M.Cs., M.Kom

**LEMBAR PENGESAHAN  
TIM PENGUJI UJIAN SKRIPSI**

Nama : Novia Riska Arsela  
NPM : 143510222  
Jurusan : Teknik  
Program Studi : Teknik Informatika  
Jenjang Pendidikan : Strata Satu (S1)  
Judul Skripsi : Analisis Keamanan Algoritma Enkripsi Citra Menggunakan Baker's Map dan Logistic Map

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah. Telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 4 Oktober 2019** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika**.

Pekanbaru, 4 Oktober 2019

Tim Penguji

1. Ana Yulianti, ST., M.Kom
2. Yudhi Arta, ST., M.Kom

Sebagai Tim Penguji I

Sebagai Tim Penguji II

Disetujui Oleh

Dosen Pembimbing

APRI SISWANTO, S.Kom., M.Kom

Disahkan Oleh :



Dekan Fakultas Teknik

Dr. H. ABD. KADIS ZAINI, MT., MS., TR  
88 03 02 098

Ketua Prodi Teknik Informatika

An Gek Prodi

AUSE LABELAPANSA, ST., M.Cs., M.Kom

## LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama : Novia Riska Arselia  
Tempat/Tgl Lahir : Tembilahan, 04 Januari 1997  
Alamat : Jl.Tg. Harapan Lr.Tg Sari, RT/RW 006/002,  
Kecamatan Tembilahan

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada :

Fakultas : Teknik  
Jurusan : Teknik Informatika  
Program Studi : Teknik Informatika  
Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul "Analisis Keamanan Algoritma Enkripsi Citra menggunakan Baker's Map dan Logistic Map". Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini bukan karya saya sendiri atau plagiat hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 16 November 2019  
Yang membuat pernyataan,



(Novia Riska Arselia)

## LEMBAR IDENTITAS PENULIS

Nama : Novia Riska Arsela

NPM : 143510222

Tempat/TglLahir : Tembilahan, 04 Januari 1997

Alamat Orang Tua : Jl. Tg. Harapan Lr.Tg. Sari, RT/RW 006/002, Kecamatan Tembilahan

Nama Orang Tua

Ayah : Marjani

Ibu : Megawati

No Hp/Telp : 085263039648

Jurusan : Teknik Informatika

Fakultas : Teknik

Masuk Th. Ajaran : 2014

Wisuda Th. Ajaran : 2020

Judul Penelitian : Analisis Keamanan Algoritma Enkripsi Citra menggunakan Baker's Map dan Logistic Map



Pekanbaru, 16 November 2019

Novia Riska Arsela

## HALAMAN PERSEMBAHAN

Assalamu'alaikum Wr, Wb.

Alhamdulillah, puji dan rasa syukur yang tak terhingga penulis ucapkan tiada henti kepada Allah SWT atas segala rahmat dan karunia-Nya yang telah diberikan kepada penulis sehingga dapat menyelesaikan tugas akhir skripsi dengan judul **“Analisis Keamanan Algoritma Enkripsi Citra menggunakan Baker’s Map dan Logistic Map ”**.

Tugas akhir skripsi ini disusun untuk memenuhi persyaratan mencapai derajat strata satu (S1) di jurusan Teknik Informatika Fakultas Teknik Universitas Islam Riau. Penulis menyadari tanpa adanya bantuan dari berbagai pihak, usaha yang penulis lakukan dalam menyelesaikan skripsi ini tidak akan membuahkan hasil. Oleh karena itu, dalam kesempatan kali ini penulis menyampaikan ucapan terima kasih kepada :

1. Terkhususnya orang tua tercinta yakni Ayahanda Marjani dan Ibunda Megawati, S.pd. Kemudian kakak Tercinta Nova Sinta Marwanti, S.pd dan abang ipar Dery dan ponakan Tersayang M.octa Pratama, beserta keluarga besar yang tak henti-hentinya selalu mensupport penulis dan membantu dalam segi materi maupun doa-doanya sehingga penulis dapat menyelesaikan penulisan skripsi ini.
2. Seluruh teman-teman seperjuangan angkatan 2014 yang tidak bisa disebutkan satu persatu, terima kasih atas kebersamaan yang membangun semangat dan motivasi dalam menyelesaikan skripsi ini.

Akhir kata penulis mohon maaf atas kekeliruan dan kesalahan yang terdapat dalam skripsi ini dan berharap semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Pekanbaru, 16 November 2019

Novia Riska Arsela



Dokumen ini adalah Arsip Miik :

Perpustakaan Universitas Islam Riau

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalaamu'alaikum Wr.Wb.

Segala puji bagi Allah SWT yang selalu memberikan rahmat dan hidayah-Nya serta nikmat yang tak terhingga, sehingga penulis dapat menyelesaikan proposal skripsi ini dengan judul “Analisis Keamanan Enkripsi Citra Menggunakan Algoritma Baker’s Map dan Logistic Map” sebagai salah satu syarat untuk penyusunan laporan skripsi pada Fakultas Teknik Prodi Teknik Informatika Universitas Islam Riau.

Dalam penyusunan proposal ini, penulis sadar bahwa tanpa bantuan dan bimbingan berbagai pihak lain maka proposal ini sulit untuk terwujud. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua dan keluarga, yang selalu mendo’akan, serta memberikan dukungan yang sangat baik.
2. Seluruh Dosen Prodi Teknik Informatika yang mendidik serta memberi arahan.

Penulis menyadari sepenuhnya bahwa dalam penyusunan proposal ini masih banyak kekurangan, untuk itu dengan segala kerendahan hati penulis mengharapkan saran dan kritik yang sifatnya membangun guna memperbaiki proposal ini.



Akhir kata semoga proposal ini dapat menambah ilmu pengetahuan dan bermanfaat bagi semua pihak yang membacanya.

Wassalamu'alaikum Wr. Wb.

Pekanbaru, 21 Maret 2019

Novia Riska Arsela



Dokumen ini adalah Arsip Milik :  
**Perpustakaan Universitas Islam Riau**

## DAFTAR ISI

	<b>Halaman</b>
<b>HALAMAN JUDUL</b>	
<b>LEMBAR PERNYATAAN BEBAS PLAGIARISME</b>	
<b>LEMBAR IDENTITAS PENULIS</b>	
<b>HALAMAN PERSEMBAHAN</b>	
<b>KATA PENGANTAR</b> .....	i
<b>ABSTRAK</b> .....	iii
<b>ABSTRACT</b> .....	iv
<b>DAFTAR ISI</b> .....	v
<b>DAFTAR GAMBAR</b> .....	viii
<b>DAFTAR TABEL</b> .....	ix
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang Masalah.....	1
1.2 Identifikasi Masalah.....	1
1.3 Rumusan Masalah.....	2
1.4 Batasan Masalah.....	2
1.5 Tujuan Penelitian.....	2
1.6 Manfaat Penelitian.....	3
<b>BAB II LANDASAN TEORI</b>	
2.1 Studi Kepustakaan.....	4
2.2 Dasar Teori.....	6
2.2.1 Kriptografi.....	6
2.2.2 Baker's Map.....	8
2.2.3 Logistic Map.....	9
2.2.4 Hitung Manual <i>Baker's Map</i> dan <i>Logistic Map</i> .....	11
2.2.5 Citra Digital.....	13

2.2.6 PHP.....	13
2.2.7 Unified Modeling Language (UML).....	14
2.2.8 Use Case Diagram.....	14
2.2.9 Class Diagram.....	15
2.2.10 Activity Diagram.....	16
2.2.11 Sequence Diagram.....	17
2.2.12 Diagram Alir( <i>Flowchart</i> ).....	18
2.2.13 Basis Data( <i>Database</i> ).....	19

**BAB III METODOLOGI PENELITIAN**

3.1 Metodologi Penelitian.....	21
3.2 Alat dan Bahan Penelitian yang digunakan.....	21
3.2.1 Spesifikasi Perangkat Keras ( <i>Hardware</i> ).....	21
3.2.2 Spesifikasi Perangkat Lunak ( <i>Software</i> ).....	21
3.3 Usulan Skema Enkripsi.....	22
3.4 Pengembangan dan Perancangan Sistem.....	23
3.4.1 <i>Hirarchy Chart</i> .....	23
3.4.2 <i>Activity Diagram</i> .....	25
3.4.3 <i>Use Case Diagram</i> .....	29
3.4.4 Class Diagram.....	29
3.5 Perancangan Input.....	30
3.5.1 Desain Input.....	30
3.6 Perancangan Output.....	32
3.6.1 Desain Output.....	32
3.7 Desain Interface.....	33
3.7.1 Halaman Utama.....	33
3.8 Perancangan Logika Program.....	34
3.8.1 <i>Flowchart</i> Login.....	38
3.8.2 <i>Flowchart</i> Menu Utama.....	39
3.8.3 <i>Flowchart Embedding</i> .....	40
3.8.4 <i>Flowchart Extraction</i> .....	41

## **BAB IV HASIL DAN PEMBAHASAN**

4.1 Pengujian Black Box .....	42
4.2 Penjelasan Sistem .....	42
4.2.1 Form Login.....	42
4.2.2 Form Menu Embedding.....	44
4.2.3 Form Menu Extraction .....	47
4.2.4 Form Menu Data.....	49
4.2.5 Form Menu Profile .....	48
4.3 Kesimpulan Hasil Pengujian Blackbox.....	50
4.4 Kesimpulan Hasil Implementasi .....	51

## **BAB V KESIMPULAN DAN SARAN**

5.1 Kesimpulan.....	52
---------------------	----

<b>DAFTAR PUSTAKA .....</b>	<b>57</b>
-----------------------------	-----------



## DAFTAR TABEL

Tabel 2.1.Simbol Pada Use Case .....	15
Tabel 2.2.Simbol Pada Class Diagram.....	16
Tabel 2.3.Simbol Pada Activity Diagram .....	17
Tabel 2.4.Simbol <i>Sequence Diagram</i> .....	18
Tabel 2.5.Simbol <i>flowchart</i> .....	19
Tabel 3.1 Citra Dalam Bentuk Matriks .....	35
Tabel 3.2 Matriks Citra Hasil Enkripsi .....	37
Tabel 4.1.Pengujian Form Login .....	44
Tabel 4.2.Pengujian Form Embedding .....	46
Tabel 4.4.Pengujian Form Extraction .....	48
Tabel 4.5.Pengujian Form Menu Data .....	50
Tabel 4.6.Hasil Nilai Presentase Tiap Pertanyaan Kuisisioner .....	53

## DAFTAR GAMBAR

Gambar 3.1.Skema yang akan dibangun.....	23
Gambar 3.2.Hierarchy Chart.....	24
Gambar 3.3. <i>Activity Diagram Embedding</i> .....	26
Gambar 3.4. <i>Activity Diagram Extraction</i> .....	28
Gambar 3.5. <i>Use Case Sistem Yang Dibangun</i> .....	29
Gambar 3.6. <i>Class Diagram</i> .....	30
Gambar 3.7.Desain Input Embedding.....	31
Gambar 3.8.Desain Input Extraction.....	31
Gambar 3.9.Desain Output Embedding.....	32
Gambar 3.10.Desain Output Extraction.....	33
Gambar 3.11.Desain Output Data.....	33
Gambar 3.12.Halaman Utama.....	34
Gambar 3.13.Citra Original.....	35
Gambar 3.14.Citra Original (crop).....	35
Gambar 3.15.Flowchart Login.....	38
Gambar 3.16.Flowchart Menu Utama.....	39
Gambar 3.17.Flowchart Menu Embedding.....	40
Gambar 3.18.Flowchart Menu Extraction.....	41
Gambar 4.1 Form Login.....	43
Gambar 4.2 Peringatan Gagal Login.....	43
Gambar 4.3 Form Menu Embedding (Input Gambar).....	45
Gambar 4.4 Form Menu Embedding (Hasil Enkripsi).....	45
Gambar 4.5 Form Menu Extraction (pilih gambar).....	47
Gambar 4.6 Form Menu Extraction (Proses Dekripsi).....	48
Gambar 4.7 Form Menu Data.....	49
Gambar 4.8 Form Menu Profile.....	50
Gambar 4.9 Grafik Hasil Kuisisioner.....	52

## Analisis Keamanan Enkripsi Citra Menggunakan Algoritma Baker's Map dan Logistic Map

Novia Riska Arsela<sup>1</sup>, Apri Siswanto<sup>2</sup>

Program Studi Teknik Informatika

Universitas Islam Riau, Pekanbaru

E-mail: [noviariskaarsela@student.uir.ac.id](mailto:noviariskaarsela@student.uir.ac.id) , [aprisiswanto@eng.uir.ac.id](mailto:aprisiswanto@eng.uir.ac.id)

### ABSTRAK

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas.

Berdasarkan hasil analisa dan pengujian, Dengan adanya sistem Keamanan Enkripsi Citra Menggunakan Baker's Map dan Logistic Map dapat membantu user menjaga kerahasiaan sebuah citra, Hasil simulasi program kriptografi dengan menggunakan algoritma *baker's map* dan *logistic map* memiliki hasil citra yang lebih terjaga kerahasiaannya dibandingkan citra asli, Berdasarkan hasil analisa yang diperoleh, sistem kriptografi ini memiliki batasan citra yang dapat dienkripsi atau diproses yaitu hanya citra yang memiliki ukuran dimensi yang kecil dari 3000x4000 pixel.

**Kata Kunci:** Kriptografi, Metode Baker's Map, Metode Logistic Map.

# Image Encryption Security Analysis Using the Baker's Map and Logistic Map Algorithm

Novia Riska Arselal, Apri Siswanto2

Informatics Engineering Study Program

Riau Islamic University, Pekanbaru

E-mail: [noviariskaarsela@student.uir.ac.id](mailto:noviariskaarsela@student.uir.ac.id) [aprisiswanto@eng.uir.ac.id](mailto:aprisiswanto@eng.uir.ac.id)

## ABSTRACT

Cryptography was originally described as the study of how to hide messages. But in the modern sense of cryptography is a science that relies on mathematical techniques to deal with information security such as confidentiality, data integrity and entity authentication

Based on the analysis and testing results, the Image Encryption Security System Using Baker's Map and Logistic Map can help users maintain the confidentiality of an image. The results of the cryptographic program simulation using the baker's map and logistic map algorithm have a more secure image confidentiality than the original image. The analysis results obtained, this cryptographic system has a limited image that can be encrypted or processed, that is, only images that have dimensions smaller than 3000x4000 pixels.

**Keywords:** Cryptography, Baker's Map Method, Logistic Map Method.



# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Citra digital merupakan salah satu data atau informasi yang sering disalahgunakan, oleh karena itu untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi salah satunya dapat dengan tehnik enkripsi dan dekripsi. Teknik ini berguna untuk membuat data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak dan mengetahui teknik dekripsinya. Melihat penting dan bermanfaatnya teknik enkripsi dan dekripsi, maka akan sangat baik jika metode dalam pemrosesnya menggunakan algoritma dengan tingkat keamanan yang tinggi, salah satunya dengan algoritma Baker's Map dan Logistic Map. Sehingga mampu mengenkripsi dan dekripsi file citra tanpa mengubah integritas data dari file citra tersebut.

Maka dari itu agar file citra tetap aman dan terjaga kerahasiaannya akan dibuat sebuah sistem analisis keamanan dengan menggunakan algoritma enkripsi baker's map dan logistic map. Kombinasi dari 2 algoritma tersebut akan memudahkan untuk melakukan pengamanan file citra. Sehingga penulis menarik sebuah judul yaitu "Analisis Keamanan Algoritma Enkripsi Citra Menggunakan Baker's Map dan Logistic Map".

### 1.2 Identifikasi Masalah

Adapun identifikasi masalah yang dapat diambil dari latar belakang tersebut adalah sebagai berikut :

1. Kurangnya keamanan pada file citra sehingga pihak lain dapat melihat isi informasi data dan dapat disalahgunakan.
2. Belum adanya proses enkripsi dengan menggunakan sebuah algoritma Baker's Map dan Logistic Map untuk keamanan data/file.
3. Pihak lain dapat mengambil atau mencuri data/file citra karena tidak adanya keamanan pada data/file tersebut.

### 1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka yang menjadi rumusan masalah dalam penelitian ini adalah bagaimana membuat suatu sistem untuk keamanan file citra dengan mengkombinasikan Baker's Map dan Logistic Map untuk keamanan data/file citra.

### 1.4 Batasan Masalah

Mengingat keterbatasan waktu, biaya, dan kemampuan penelitian maka penelitian ini dibatasi dalam hal :

1. Jenis file citra yang dapat di enkripsikan hanya file yang berformat JPG atau PNG.
2. Hasil file output akan tersimpan dengan format yang sama yaitu JPG atau PNG.
3. Sistem ini berbasis web.

### 1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Mengamankan file citra dengan metode Baker's Map dan Logistic Map.

2. Membantu pengguna untuk mengamankan file citra agar data dan informasi tidak dapat disalah gunakan.

### 1.6 Manfaat penelitian

Adapun manfaat dari penelitian ini yaitu diharapkan dapat membantu pengguna untuk mengamankan file citra yang bersifat rahasia atau privasi agar file atau informasi tidak dapat diketahui orang lain.



## BAB II

### LANDASAN TEORI

#### 2.1 Studi Kepustakaan

Dalam penyusunan proposal skripsi ini, penulis mengambil atau melakukan literatur review terhadap penelitian-penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada proposal skripsi ini. Adapun penelitian yang berhubungan dengan proposal skripsi ini adalah sebagai berikut :

Studi kepustakaan pertama adalah berdasarkan penelitian yang dilakukan oleh Pahrul Irfan (2016), Yang bertujuan menerapkan algoritma Chaos menggunakan sistem Logistic Map untuk melakukan enkripsi pada pixel RGB citra, dan ditambahkan dengan algoritma Arnold Cat Map yang digunakan untuk melakukan pengacakan pada posisi pixel citra.

Studi kepustakaan kedua adalah berdasarkan penelitian yang dilakukan oleh Aida, Dkk (2017), Secara default, Gallery akan menampilkan semua file citra yang ada pada smartphone android baik itu citra yang berasal dari hasil pengambilan gambar dengan kamera maupun citra lain yang sengaja disimpan pada perangkat smartphone tersebut. Hal ini memungkinkan semua orang dapat mengetahui semua informasi citra yang bersifat umum maupun yang penting dan atau rahasia dalam smartphone android hanya dengan membuka gallery. Oleh karena itu, penulis membuat aplikasi enkripsi yang disusun dalam laporan penelitian ini dengan judul “Implementasi Algoritma Baker Map Untuk Enkripsi Citra Pada Perangkat Android”. Untuk melindungi konten di dalam citra dari pengaksesan illegal dan

mentransformasikan citra ke dalam bentuk lain yang tidak bermakna sehingga konten di dalam citra tidak dapat dipahami lagi secara visual.

Studi kepustakaan ketiga adalah berdasarkan penelitian yang dilakukan oleh Ronsen Purba, Dkk (2014), Dalam penelitian diusulkan algoritma enkripsi citra digital menggunakan dua buah fungsi chaos, yakni Arnold's Cat Map (ACM) dan Nonlinear Chaotic Algorithm (NCA). Hal ini dilakukan untuk mendapatkan enkripsi citra yang lebih robust. Proses enkripsi yang dilakukan meliputi pengacakan susunan pixel menggunakan Arnold's Cat Map, pengacakan nilai RGB dan perubahan nilai dalam citra memanfaatkan bilangan acak yang dibangkitkan menggunakan Nonlinear Chaotic Algorithm (NCA). Hasil pengujian menunjukkan cipher image memiliki distribusi intensitas pixel yang uniform. Selain itu pixel-pixel yang bertetangga memiliki koefisien korelasi yang rendah, koefisien korelasi yang rendah mengindikasikan pixel yang bertetangga tidak memiliki hubungan.

Studi kepustakaan keempat adalah berdasarkan penelitian yang dilakukan oleh Rinaldi Munir (2012), Solusi terhadap keamanan citra digital dari pengaksesan yang ilegal adalah dengan mengenkripsinya. Tujuan enkripsi citra adalah menyandikan citra (plain-image) sehingga tidak dapat dikenali lagi (cipher-image). Saat ini enkripsi citra sudah telah digunakan secara luas sebagai salah satu teknik menjaga keamanan informasi. Enkripsi merupakan salah satu teknik keamanan pesan di dalam kriptografi, termasuk pesan dalam bentuk citra. Salah satu layanan yang diberikan oleh kriptografi adalah kerahasiaan pesan (confidentiality), dan confidentiality diimplementasikan dengan enkripsi dan dekripsi pesan.

Studi kepustakaan kelima adalah berdasarkan penelitian yang dilakukan oleh Halim, Dkk (2015), Pengamanan data citra menjadi sangatlah penting untuk misi penginderaan jarak jauh. Saat ini banyak algoritma-algoritma yang sangat baik dari sisi keamanan, permasalahannya tidak semua algoritma sesuai diimplementasikan untuk mengenkripsi data citra. Data citra memiliki kapasitas volume yang lebih besar dari pada text, jika diterapkan algoritma-algoritma konvensional seperti DES, dan RSA maka akan membutuhkan waktu komputasi yang lama saat enkripsi.

## 2.2 Dasar Teori

### 2.2.1 Kriptografi

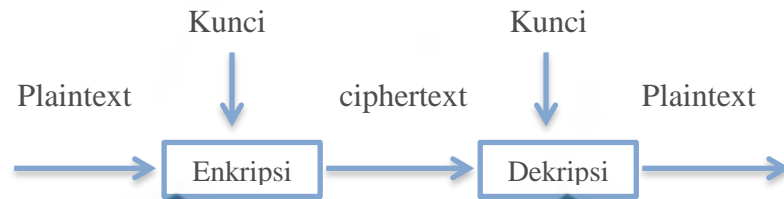
Kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing*(tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi, (Dony Ariyus, 2008).

Berikut ini adalah beberapa sistem kriptografi yaitu :

1. **Plainteks** : Pesan atau data dalam bentuk aslinya yang dapat terbaca. *Plainteks* adalah masukan bagi algoritma enkripsi. Untuk selanjutnya digunakan istilah teks asli sebagai padanan kata *plaintexts*.
2. **Secret Key** : *secret key* yang juga masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi. Untuk selanjutnya digunakan istilah kunci rahasia sebagai padanan kata *secret key*.
3. **Chiper Teks** : *chiper teks* adalah keluaran algoritma enkripsi. *Chiper text* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *chipertext* yang terlihat acak. Untuk selanjutnya digunakan istilah teks sandi sebagai padanan kata *chipertext*.
4. **Algoritma Enkripsi:** Algoritma enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. **Algoritma Dekripsi:** Algoritma dekripsi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma enkripsi.

Berikut ini adalah gambaran mekanisme atau cara kerja dalam kriptografi.

Perhatikan pada Gambar 2.1



**Gambar 2.1** Mekanisme Kriptografi

### 2.2.2 Baker's Map

Baker Map merupakan salah satu metoda *chaotic map* yang menciptakan suatu *permuted version* pada matriks segi empat ( $M \times M$ ). Bentuk dari diskrit Baker Map merupakan alat yang efisien untuk mengacak data pada matriks segi empat Suci Auli, Dkk (2014). *Diskrit Baker Map* dapat direpresentasikan dengan persamaan di bawah :

$$B_{(r,s)} = \left[ \frac{M}{n_i} (r - P_i) + s \bmod \left( \frac{M}{n_i} \right), \frac{n_i}{M} \left( s - s \bmod \left( \frac{M}{n_i} \right) + P_i \right) \right]$$

Dimana :

$B_{(r,s)}$  merupakan indikasi baru dari data  $(r,s)$ .

$$P_i \leq r \leq P_i + n_i, 0 \leq s \leq M \text{ dan } P_i = n_0 + \dots + n_i \quad (n_0 = 0)$$

	0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7	8
1	9	10	11	12	13	14	15	16
2	17	18	19	20	21	22	23	24
3	25	26	27	28	29	30	31	32
4	33	34	35	36	37	38	39	40
5	41	42	43	44	45	46	47	48
6	49	50	51	52	53	54	55	56
7	57	58	59	60	61	62	63	64

**Gambar 2.2** Ilustrasi Citra Asli (8x8) piksel.

Keterangan :



$m$  = matrix

$n$  = *key* (kunci)

$R$  = Row (baris)

$P$  = Piksel

$S$  = Sel

Hitung Manual Enkripsi Baker's Map :

Diketahui  $n = 3$

$$\begin{aligned} \text{EBM} &= \frac{m}{n} (R + P) + S \bmod \left(\frac{m}{n}\right) \\ &= \frac{8}{3} (0 + 1) + 0 \bmod \left(\frac{8}{3}\right) \\ &= 2,66 \end{aligned}$$

Lakukan langkah diatas sampai  $P_i \dots n$

### 2.2.3 Logistic Map

Menurut Mohammad Hamdani (2019). Untuk melakukan enkripsi maupun dekripsi menggunakan logistic map, terdapat beberapa proses antara lain adalah :

1. Fungsi Pemotongan Enkripsi dan dekripsi beroperasi dalam himpunan bilangan bulat yang nilainya dari 0 - 255, sedangkan barisan nilai *chaos* yang digunakan sebagai *keystream* adalah bilangan real yaitu 0 dan 1. Agar barisan nilai *chaos* dapat dipakai untuk enkripsi dan deskripsi, maka nilai *chaos* harus dikonversi ke nilai integer menggunakan rumus sebagai berikut :

$$T(x, size) = \lfloor x * 10^{count} \rfloor \quad \text{|| } x \neq 0$$

yang dalam hal ini count dimulai dari 1 dan bertambah 1  $10^{count} * \text{hingga } x > 10^{size-1}$ . Hasilnya kemudian diambil bagian integer saja dilambangkan

dengan pasangan garis ganda. Sebagai contoh, misalkan  $x = 0.003176501$  dan  $size = 4$ , maka dimulai dari  $count = 1$  sampai  $count = 6$  diperoleh.

$$10^6 * 0.003176501 = 3176.501 > 10^3$$

kemudian ambil bagian integer-nya dengan

$$\|3176.501\| = 3176$$

Bit LSB (*Least Significant Bit*) dari representasi bit 3176 adalah 0 (perhatikanlah bahwa 3176 bilangan genap, maka bit LSB-nya pasti 0). Jadi, kita memperoleh sebuah bit kunci dari nilai chaotik 0.003176501 yaitu 0.

Prosedur yang sama dilakukan untuk nilai-nilai chaotik lainnya.

2. Membangkitkan *keystream* menggunakan *Chaos* Pada proses membangkitkan kunci ini menggunakan rumus sebagai berikut :

$$X_{i+1} = r x_i (1 - x_i)$$

Sebagai contoh, jika kita menggunakan  $r = 4.0$  dan nilai awal  $x_0 = 0.456$ , maka kita memperoleh 100 bilangan acak:  $X_1 = 4.0x_0(1 - x_0) = 0.992256$ ,

$$X_2 = 4.0x_1(1 - x_1) = 0.030736, X_3 = 4.0x_2(1 - x_2) = 0.119166, \dots, X_{99} = 4.0x_{98}(1 - x_{98}) = 0.914379, X_{100} = 4.0x_{99}(1 - x_{99}) = 0.313162$$

Nilai-nilai acak yang dihasilkan di dalam barisan chaotik tersebut nilainya berada di antara 0 dan 1.

3. Enkripsi Plaintext dengan Kunci. Enkripsi dikerjakan dengan menjumlahkan plaintext  $p_i$  dan *keystream*  $k_i$  dalam modulus 256, seperti yang dituliskan dalam persamaan berikut :

$$C_i = (p_i + k_i) \bmod 256$$

Alasan pemilihan modulus 256 karena *stream cipher* mengenkripsi plainteks menjadi cipertext satu karakter (1 *byte*) setiap kali.

4. Dekripsi Cipertext menggunakan kunci. Dekripsi dikerjakan dengan mengurangi cipertext  $c_i$  dengan *keystream*  $k_i$  dalam modulus 256, seperti yang dituliskan dalam persamaan berikut :

$$\text{Dekripsi} = (C_i - K_i) \bmod 256$$

#### 2.2.4 Hitung Manual Baker's Map dan Logistic Map

Pada tahap ini akan dilakukan perhitungan manual untuk melakukan enkripsi dan dekripsi menggunakan algoritma *baker's map* dan *logistic map*.

	0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7	8
1	9	10	11	12	13	14	15	16
2	17	18	19	20	21	22	23	24
3	25	26	27	28	29	30	31	32
4	33	34	35	36	37	38	39	40
5	41	42	43	44	45	46	47	48
6	49	50	51	52	53	54	55	56
7	57	58	59	60	61	62	63	64

**Gambar 2.2** Ilustrasi Citra Asli (8x8) piksel.

Keterangan :

m = matrix

n = *key* (kunci)

R = Row (baris)

P = Piksel

S = Sel

Diketahui n = 3

#### 1. Enkripsi Baker's Map dan Logistic Map

$$\begin{aligned} EBM &= \frac{m}{n} (R + P) + S \bmod \left(\frac{m}{n}\right) \\ &= \frac{8}{3} (0 + 1) + 0 \bmod \left(\frac{8}{3}\right) \end{aligned}$$

$$EBM = 2,66$$

Lakukan langkah diatas sampai  $P_i \dots n$

$$\begin{aligned} ELM &= (EBM + n) \bmod (256) \\ &= (2,66 + 3) \bmod (256) \\ &= 5,66 \bmod (256) \end{aligned}$$

$$ELM = 5,66$$

Lakukan langkah diatas sampai  $P_i \dots n$

## 2. Dekripsi *Logistic Map* dan *Baker's Map*

$$\begin{aligned} DLM &= (P - n) \bmod (256) \\ &= (5,66 - 3) \bmod (256) \end{aligned}$$

$$DLM = 2,66$$

Lakukan langkah diatas sampai  $P_i \dots n$

$$\begin{aligned} DBM &= \frac{DLM - \left(\frac{m}{n} (R) + S \bmod \left(\frac{m}{n}\right)\right)}{\left(\frac{m}{n}\right)} \\ &= \frac{2,66 - \left(\frac{8}{3} (0) + 0 \bmod \left(\frac{8}{3}\right)\right)}{\left(\frac{8}{3}\right)} \\ &= \frac{2,66 - (0 + 0)}{2,66} \end{aligned}$$

$$DBM = 1$$

### 2.2.5 Citra Digital

Citra (*Image*) adalah sebuah istilah lain untuk gambar, sebagai salah satu komponen multimedia yang memegang peranan penting sebagai bentuk informasi visual. Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi. Secara harfiah citra (*Image*) adalah gambar pada bidang dwimatra (*Dua dimensi*) ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*Continue*) dari intensitas cahaya pada dwimatra. Sumber cahaya menerangi objek dan objek memantulkan kembali sebagian dari berkas cahaya. pantulan cahaya tersebut ditangkap oleh alat - alat optik, misalnya mata pada manusia, kamera, pemindai (*Scanner*) sehingga objek yang disebut citra tersebut terekam (Munir, 2004).

#### 2.2.6 PHP

Pengertian PHP menurut (Anhar, 2010), PHP merupakan singkatan dari *Hypertext Preprocessor* yaitu bahasa pemrograman *webserver-side* yang bersifat *open source*. PHP merupakan *script* yang terintegrasi dengan HTML dan berada pada *server* (*server side HTML embedded scripting*). PHP adalah *script* yang digunakan untuk membuat halaman *website* yang dinamis. Dinamis berarti halaman yang akan ditampilkan dibuat saat halaman itu diminta oleh *client*. Mekanisme ini menyebabkan informasi yang diterima *client* selalu yang terbaru/*up to date*. Semua *script* PHP dieksekusi pada *server* di mana *script* tersebut dijalankan.

#### 2.2.7 Unified Modelling Language (UML)


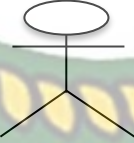

*Unified Modeling Language*(UML) adalah sebuah bahasa pemrograman yang telah menjadi standard untuk merancang dan mendokumentasikan sistem perangkat lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem dan sudah digunakan secara luas dan menggunakan notasi yang sudah dikenal untuk analisa dan desain berorientasi objek. Sesuai dengan pengertian dan konsep UML, maka ada beberapa diagram yang dapat digunakan untuk memperjelas penggunaan UML dalam pemrograman berorientasi objek, diantaranya: *Use Case Diagram*, *Class Diagram*, *Component Diagram* dan *Physical Diagram*.

#### 2.2.8 *Use Case Diagram*

*Use Case Diagram* menggambarkan sebuah fungsi yang dibutuhkan oleh sebuah sistem. Dalam hal ini ada kondisi yang agak beda, yaitu disini sistem dituntut untuk berbuat. Sebuah *use case* mempresentasikan sebuah interaksi antara pengguna dengan sebuah sistem. *Use Case* merupakan sebuah pekerjaan tertentu, misalnya login ke sistem, membuat sebuah daftar aktivitas dan sebagainya.

*Use Case diagram* sangat membantu apabila kita sedang menyusun *requirement* sebuah sistem, mengkomunikasikan rancangan dengan pengguna, dan merancang *test case* untuk semua ciri yang ada pada sistem. *Use Case* terdiri dari beberapa *symbol*, yaitu bisa dilihat pada tabel 2.1 dibawah ini :

**Tabel 2.1** Simbol pada *Use Case*

No	Nama	Symbols	Keterangan
1	<i>Use Case</i>		Abstraksi dari interaksi antara <i>system</i> dan <i>actor</i>
2	<i>Actor</i>		Mewakili peran orang, system yang lain atau alat ketika berkomunikasi dengan <i>use case</i>
3	<i>Relationship</i>		Penghubung antara objek satu dengan yang lain.

### 2.2.9 Class Diagram

*Class* adalah sebuah spesifikasi yang jika diinstansiasi akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek. *Class* menggambarkan keadaan (atribut/properti) suatu sistem, sekaligus menawarkan layanan untuk memanipulasi keadaan tersebut (metode/fungsi). Class diagram memberikan pandangan secara luas dari sebuah sistem dengan menunjukkan kelas-kelasnya dan hubungan mereka. Diagram Class bersifat statis, menggambarkan hubungan apa yang terjadi bukan apa yang terjadi jika mereka berhubungan. Dalam *class diagram* terdapat beberapa simbol, beberapa simbol tersebut dapat dilihat pada tabel 2.2 dibawah ini:

Tabel 2.2 Simbol pada *Class Diagram*

No	SIMBOL	PENJELASAN
1		<i>Class</i> , digambarkan sebagai sebuah kotak yang terbagi atas 3 bagian. Bagian atas adalah bagian nama dari <i>class</i> . Bagian tengah mendefinisikan <i>property/atribut class</i> . Bagian akhir mendefinisikan <i>method-method</i> dari sebuah <i>class</i> .
2		<i>Assosiation</i> , digunakan sebagai relasi antar dua kelas atau lebih.
3		<i>Composition</i> , jika sebuah <i>class</i> tidak bisa berdiri sendiri dan harus merupakan bagian dari <i>class</i> yang lain, maka <i>class</i> tersebut memiliki relasi <i>composition</i> terhadap <i>class</i> tempat dia bergantung tersebut. Sebuah <i>Relationship composition</i> digambarkan sebagai garis dengan ujung berbentuk jajaran genjang berisi/solid.
4		<i>Dependency</i> , digunakan untuk menunjukkan operasi pada suatu <i>class</i> yang menggunakan <i>class</i> yang lain. Sebuah <i>dependency</i> dilambangkan sebagai sebuah panah bertitik-titik.

### 2.2.10 Activity Diagram

*Activity Diagram* menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi. *Activity diagram* merupakan *state diagram* khusus, dimana sebagian besar *sate* adalah *action* dan sebagian besar transisi di-*trigger* oleh selesainya *state* sebelumnya (*internal processing*). *Activity diagram* dapat digunakan untuk



menjelaskan bisnis dan alur kerja operasional secara tahap demi tahap dari komponen suatu sistem. *Activity diagram* menunjukkan keseluruhan dari aliran *control*. Berikut ini ada beberapa simbol yang terdapat pada *activity diagram*, perhatikan pada Tabel 2.3 dibawah ini:

**Tabel 2.3 Simbol pada Activity Diagram**

No	SIMBOL	PENJELASAN
1		<i>Activity</i> , memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain.
2		<i>Action, state</i> dari sistem yang mencerninkan eksekusi dari suatu aksi.
3		<i>Initial State</i> , bagaimana objek dibentuk atau diawali.
4		<i>Final State</i> , bagaimana objek dibentuk dan diakhiri.
5		<i>Decision</i> , digunakan untuk menggambarkan suatu keputusan atau tindakan yang harus diambil pada kondisi tertentu.
6		<i>Control Flow</i> , menunjukkan bagaimana kendali suatu aktivitas terjadi pada aliran kerja dalam tindakan tertentu.

### 2.2.11 Sequence Diagram

*Sequence diagram* menjelaskan interaksi objek yang disusun berdasarkan urutan waktu. Secara mudahnya *sequence diagram* adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *use case diagram*. Dalam *sequence diagram* terdapat beberapa simbol yang dapat dilihat pada tabel 2.4 dibawah ini :

Tabel 2.4 Simbol *Sequence Diagram*

No	SIMBOL	PENJELASAN
1		<i>Lifeline</i> mengindikasikan keberadaan sebuah <i>object</i> dalam basis waktu. Notasi untuk <i>Lifeline</i> adalah garis putus-putus <i>vertikal</i> yang ditarik dari sebuah <i>object</i> .
2		<i>Object</i> merupakan <i>instance</i> dari sebuah <i>class</i> dan dituliskan tersusun secara <i>horizontal</i> . Digambarkan sebagai sebuah <i>class</i> (kotak) dengan nama <i>object</i> didalamnya yang diawali dengan sebuah titik koma.
3		<i>Actor</i> juga dapat berkomunikasi dengan <i>object</i> , maka <i>actor</i> juga dapat diurutkan sebagai kolom. Simbol <i>actor</i> sama dengan simbol pada <i>Actor Case Diagram</i> .
4		<i>Activation</i> dinotasikan sebagai sebuah kotak segi empat yang digambar pada sebuah <i>lifeline</i> . Mengindikasikan sebuah objek yang akan melakukan sebuah aksi.
5		<i>Message</i> , digambarkan dengan anak panah horizontal antara <i>Activation Message</i> mengindikasikan komunikasi antara objek-objek.

### 2.2.12 Diagram Alir (Flowchart)

Penggunaan diagram alir ini adalah untuk menggambarkan alur logika dari sebuah program. Penggambaran alur logika digambarkan secara grafis menggunakan *flowchart*. Urutan-urutan proses yang sangat rumit yang tidak bias dibuat dengan pseudocode akan mampu digambarkan oleh diagram alir ini. Simbol-simbol yang digunakan dalam diagram alir dapat dilihat pada tabel 2.5.

Tabel 2.5 Simbol *Flowchart*

Simbol	Nama	Fungsi
	Memulai/Selesai	Memulai proses
	Proses	Menyatakan operasi yang dilakukan oleh sebuah sistem
	Input / Output	Menunjukkan data masukan atau keluaran
	Kondisi	Menentukan kondisi yang diambil oleh sistem
	Dokumen	Menyatakan cetak
	Penghubung	Menyatakan titik temu aliran diagram alur
	Tanda Prosedur	Menyatakan prosedur algoritma

### 2.2.13 Database(Basis Data)

Definisi *database* (basis data) menurut Fathansyah (2007) adalah basis data terdiri dari dua kata yaitu basis dan data. Basis dapat diartikan sebagai markas atau gudang, sedangkan data adalah representasi fakta dunia nyata yang mewakili suatu objek. Dalam berbagai sudut pandang, basis data dapat didefinisikan sebagai berikut :

1. Himpunan kelompok data (arsip) yang saling berhubungan yang dapat dimanfaatkan kembali dengan cepat dan mudah.
2. Kumpulan data yang saling berhubungan yang disimpan sedemikian rupa tanpa adanya redundansi data.

3. Kumpulan file/tabel/arsip yang saling berhubungan dan disimpan dalam media penyimpanan elektronik.

Prinsip utama basis data adalah pengaturan data/arsip. Dan tujuan utamanya adalah kemudahan dan kecepatan dalam pengambilan kembali data/arsip. Yang sangat ditonjolkan dalam basis data adalah pengelompokan/pengorganisasian data yang akan disimpan sesuai fungsi dan jenisnya. Pengelompokan ini dapat berbentuk sejumlah file/tabel terpisah atau dalam bentuk pendefinisian kolom-kolom data dalam setiap tabel.



## BAB III

### METODOLOGI PENELITIAN

#### 3.1 Metodologi Penelitian

Metodologi Penelitian adalah proses atau cara ilmiah untuk mendapatkan data yang akan digunakan untuk keperluan penelitian. Metodologi juga merupakan analisis teoretis mengenai suatu cara atau metode.

#### 3.2 Alat dan Bahan Penelitian Yang Digunakan

Adapun alat dan bahan penelitian ini adalah sebuah pendukung baik perangkat keras maupun perangkat lunak sehingga penelitian ini sesuai dengan tujuan dan manfaatnya. Berikut adalah alat dan bahan penelitian yang digunakan penulis untuk menganalisa dan merancang sistem.

##### 3.2.1 Spesifikasi Perangkat Keras ( *Hardware* )

Spesifikasi Perangkat Keras (*hardware*) pada laptop yang digunakan dalam melakukan penelitian ini adalah sebagai berikut :

1. *Processor* : *Intel Core i3-4030U*
2. *Ram* : *8,00 GB*
3. *Hardisk* : *500 GB*
4. *Sysitem Type* : *64-bit Operating System*

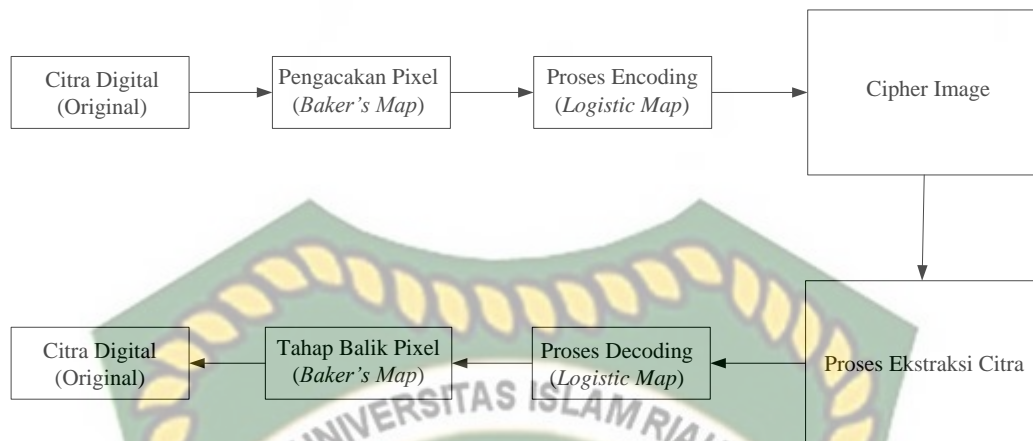
##### 3.2.2 Spesifikasi Perangkat Lunak ( *Software* )

1. *Microsoft Windows 7 Ultimate* adalah sistem operasi dari laptop yang digunakan penulis dalam melakukan penelitian ini.

2. PHP adalah bahasa pemrograman web yang digunakan dalam melakukan pembuatan sistem kriptografi login web ini.
3. CSS, digunakan untuk menghias dan mengatur gaya tampilan atau *layout* halaman web supaya terlihat lebih elegan dan menarik.
4. *Java Script*, digunakan untuk membuat sebuah halaman *website* lebih interaktif dan dinamis, dan perannya sebagai pembantu kode CSS agar pengaturan dan hiasannya lebih bagus.
5. *Microsoft Visio 2007*, digunakan untuk membuat diagram, diagram alir(*flowchart*) dll.
6. *Sublime Text 3*, digunakan sebagai text editor.
7. *XAMPPV3.2.4*, digunakan sebagai server yang berdiri sendiri (*localhost*), yang terdiri atas program *Apache HTTP Server, MySQL database*, dan penerjemah bahasa yang ditulis dengan bahasa.
8. *Web browser : Mozilla Firefox dan Google Chrome.*

### 3.3 Usulan Skema Enkripsi

Pada perancangan skema kombinasi kriptografi *Baker's Map* dan *Logistic Map* ini terdiri dari dua proses utama yang dilakukan oleh pengguna yaitu, proses Pengacakan koordinasi piksel atau Enkripsi file citra menggunakan *Baker's Map* dan *Logistic Map* sebagai algoritma yang digunakan untuk mendekripsikan file citra. Usulan skema yang akan dibangun dapat dilihat pada gambar 3.1.



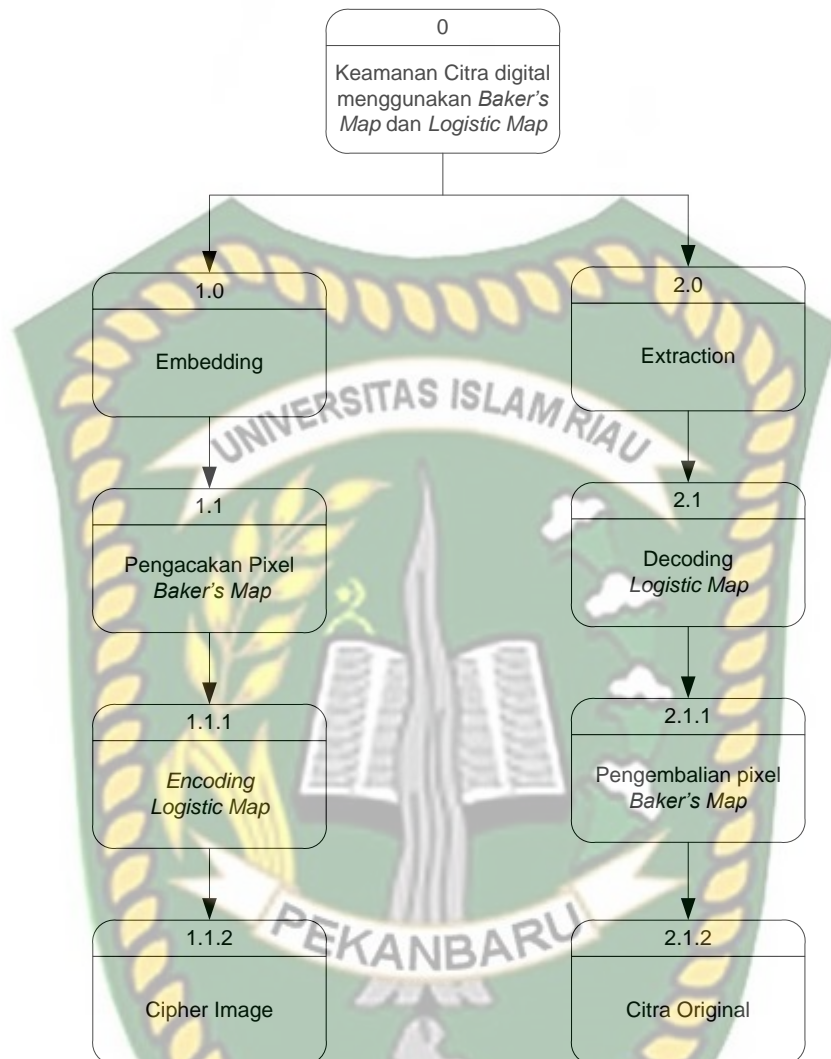
**Gambar 3.1** Skema yang akan dibangun

### 3.4 Pengembangan dan Perancangan Sistem

Pada perancangan kombinasi kriptografi *Baker's Map* dan *Logistic Map* ini terdiri dari 2 proses utama. Pertama proses enkripsi file citra. Kedua ekstraksi atau pengembalian seperti semula atau mendekripsikan file citra yang telah dienkripsikan sebelumnya.

#### 3.4.1 Hierarchy Chart

*Hierarchy chart* adalah diagram yang menggambarkan permasalahan kompleks yang kemudian diuraikan dalam beberapa elemen, berikut gambaran *hirarchy chart* pada sistem keamanan citra digital menggunakan algoritma *Baker's Map* dan *Logistic Map*. dapat dilihat pada gambar 3.2.



**Gambar 3.2** Hierarchy Chart

Berdasarkan *Hierarchy Chart* pada gambar 3.2, terdapat 2 proses utama yang terdiri dari proses *Embedding* dan proses *Extraction*. Pada proses *Embedding* akan dilakukan enkripsi file citra dengan menggunakan algoritma kriptografi yaitu *Baker's Map* dan *Logistic Map*. Selanjutnya pada proses *Extraction*, akan dilakukan deskripsi pada file citra dengan menggunakan algoritma kriptografi yaitu *Baker's Map* dan *Logistic Map*.



### 3.4.2 *Activity Diagram*

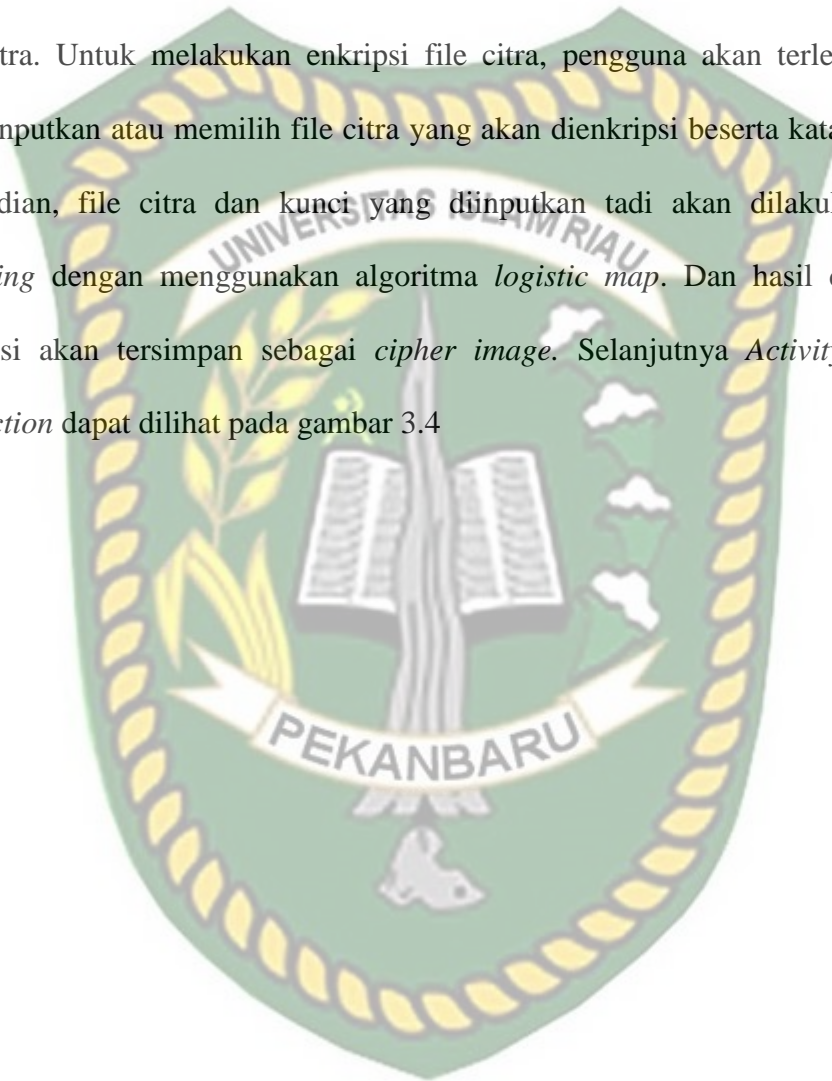
*Activity Diagram* menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity Diagram* pada sistem ini terdiri atas 2 bagian, yaitu *Activity Diagram Embedding* dan *Activity Diagram Extraction*. *Activity Diagram Embedding* dapat dilihat pada gambar 3.3.





Gambar 3.3 Activity Diagram Embedding

Pada gambar 3.3 dapat dijelaskan bahwa proses *Embedding* terdiri dari beberapa tahap. Tahap pertama dimulai dari implementasi algoritma kriptografi *Baker's Map*. Dimana pada tahap ini akan dilakukan pengacakan pixel terhadap file citra. Untuk melakukan enkripsi file citra, pengguna akan terlebih dahulu menginputkan atau memilih file citra yang akan dienkripsi beserta kata kuncinya. Kemudian, file citra dan kunci yang diinputkan tadi akan dilakukan proses *encoding* dengan menggunakan algoritma *logistic map*. Dan hasil dari proses enkripsi akan tersimpan sebagai *cipher image*. Selanjutnya *Activity Diagram Extraction* dapat dilihat pada gambar 3.4



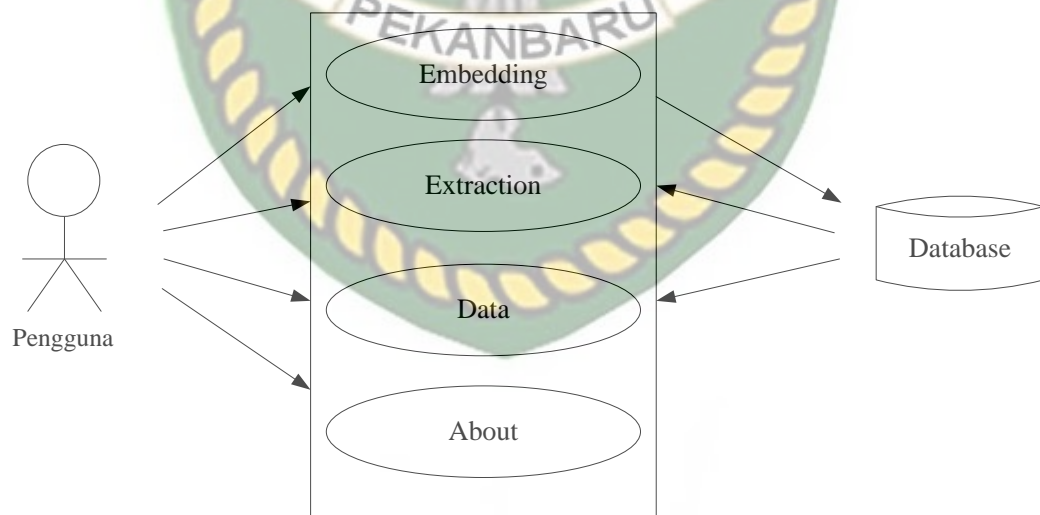


Gambar 3.4 Activity Diagram Extraction

Pada gambar 3.4 dapat dijelaskan bahwa proses *extraction* terdiri dari beberapa tahap, yaitu tahap pertama pilih file citra yang akan didekripsi. Dari hasil ekstraksi tersebut akan dihasilkan berupa file citra yang masih dalam bentuk *chiperimage*. Kemudian selanjutnya akan dilakukan dekripsi dengan menggunakan kombinasi algoritma *Baker's Map* dan *Logistic Map* untuk mengubah *Chiperimage* tersebut menjadi file citra agar file citra dapat dilihat oleh pengguna.

### 3.4.3 Use Case Diagram

Pada perancangan sistem keamanan citra digital ini terdiri dari dua proses utama yang dilakukan oleh pengguna yaitu, proses Embedding pesan dan Extraction file citra. *User Case* aplikasi yang akan dibangun dapat dilihat pada gambar 3.5 dibawah ini.



**Gambar 3.5** Use Case Sistem Yang Dibangun

### 3.4.4 Class Diagram

*Class Diagram* menggambarkan struktur dan dekripsi *class*, *package*, dan objek yang saling terhubung. *Class Diagram* yang dijelaskan pada analisa ini

adalah *class Diagram* pada aplikasi yang akan dibangun, seperti gambar 3.8 dibawah ini.

<b>Embedding</b>	<b>Extraction</b>
<ul style="list-style-type: none"> <li>- File_Citra</li> <li>- Kunci</li> </ul>	<ul style="list-style-type: none"> <li>- Cipherimage</li> <li>- Kunci</li> </ul>
<ul style="list-style-type: none"> <li>+ Acak_Pixel_Baker's_Map()</li> <li>+ Encoding_Logistic_Map()</li> <li>+ Embed()</li> <li>+ Simpan()</li> </ul>	<ul style="list-style-type: none"> <li>+ Balik_pixel_Baker's_Map()</li> <li>+ Decoding_Logistic_Map()</li> <li>+ Extact()</li> <li>+ Simpan()</li> </ul>

**Gambar 3.6** *Class Diagram*

### 3.5 Perancangan Input

Desain input merupakan perancangan desain masukan dari pengguna kepada sistem.

#### 3.5.1 Desain Input

Desain input embed ini merupakan bentuk tampilan yang digunakan untuk melakukan proses input file citra, input kunci. Tampilan input embedding dan *extraction* dapat dilihat pada gambar 3.7 dan 3.8 dibawah ini.

**Gambar 3.7** Desain Input Embedding

**Gambar 3.8** Desain Input Extraction

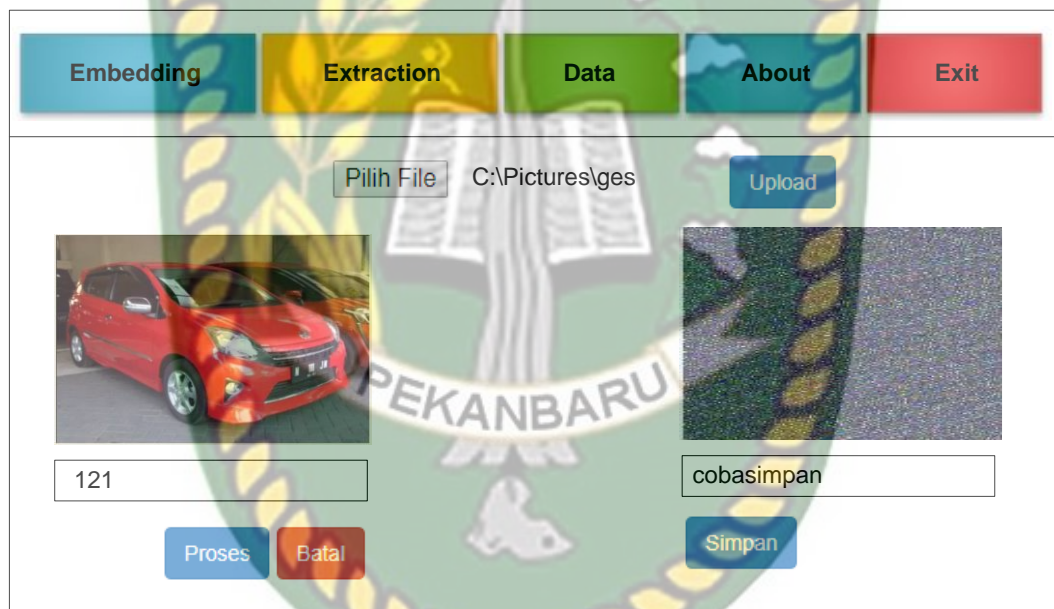
Pada gambar 3.8 diatas dapat dilihat, yang menjadi input pada proses ini yaitu citra cipher, kunci dekripsi dan akan menampilkan file cistra original.

### 3.6 Perancangan *Output*

Desian *output* merupakan rancangan tampilan *output* atau hasil dari sistem setelah melakukan proses yang terdiri dari *embedding* dan *extraction*.

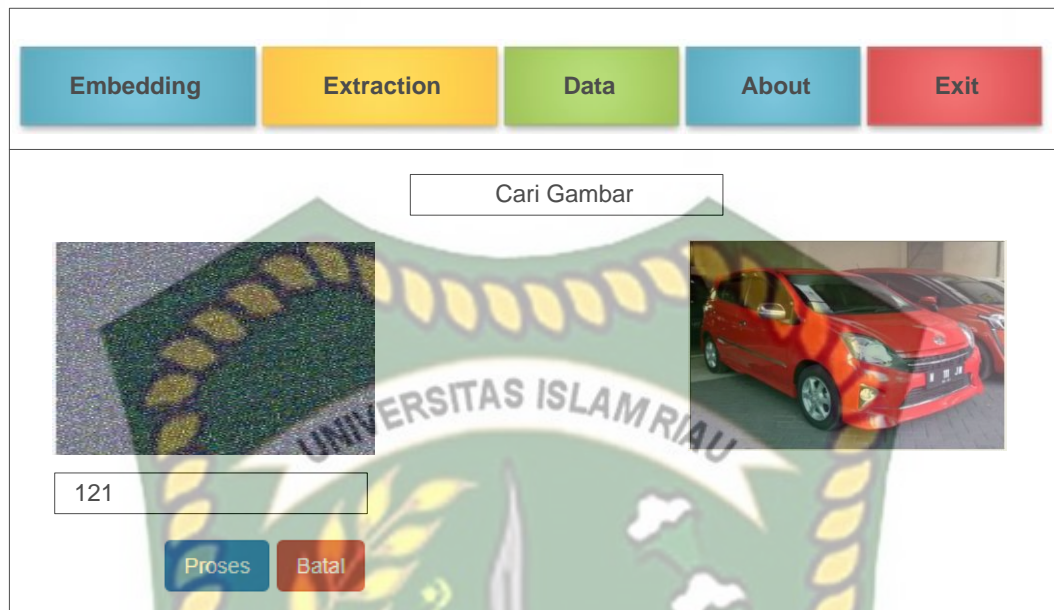
#### 3.6.1 Desain *Output*

Hasil *output* merupakan rancangan bentuk tampilan *output* dari sistem setelah melakukan proses *embedding* dan *extraction* berupa pesan rahasia. Adapun hasil dari *output* dapat dilihat pada gambar 3.9 dan 3.10 dibawah ini.

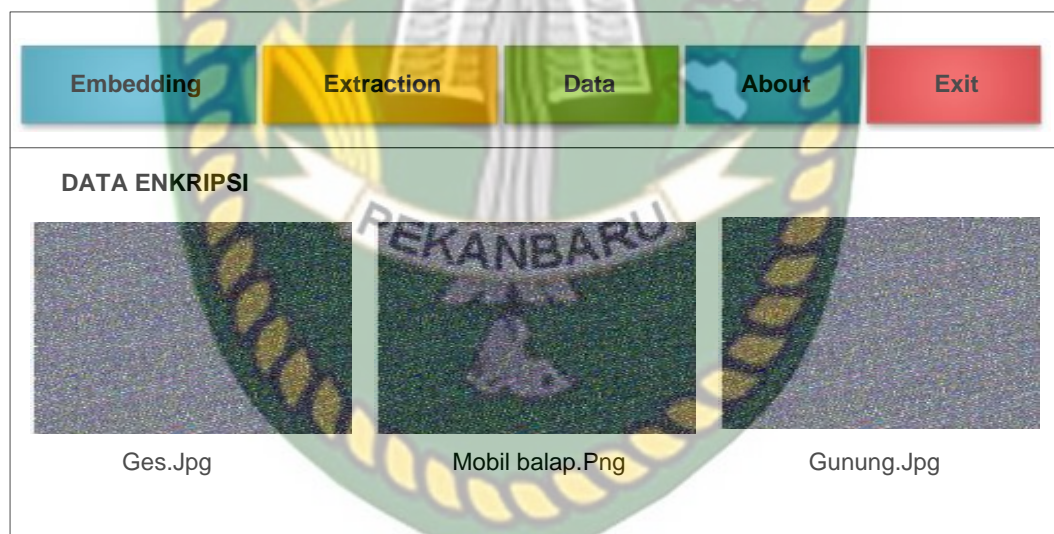


Gambar 3.9 Desain *Output* Embedding





**Gambar 3.10** Desain Output Ekstraksi



**Gambar 3.11** Desain Output Data

### 3.7 Desain Interface

#### 3.7.1 Halaman Utama

Pada halaman utama akan menampilkan halaman awal pada sistem pertama kali dijalankan. Adapun tampilan halaman utama dapat dilihat pada Gambar 3.12



**Gambar 3.12** Halaman Utama

Pada gambar 3.12 diatas terdapat 5 menu pilihan yaitu pertama *embedding*, merupakan menu untuk menyembunyikan, penyandian file citra dan mengenkripsi file citra. Kedua *extraction*, merupakan menu yang bertugas mengembalikan file citra *cipher* ke citra original. Ke tiga menu data yaitu hasil dari enkripsi yang telah dilakukan sebelumnya. Keempat menu about yang bertujuan menampilkan tata cara penggunaan sistem. Dan yang terakhir menu Exit (Keluar dari sistem).

### 3.8 Perancangan Logika Program

Perancangan logika program akan memberikan gambaran bagaimana sistem bekerja mulai dari proses *input* sampai dengan proses *output*. Dan memberikan gambaran kinerja sistem yang terstruktur dan sistematis.



Gambar 3.13 Citra Original



Gambar 3.14 Citra Original (Crop)

Tabel 3.1 Citra dalam bentuk Matriks

(Row) = R  
 (Sel) = S  
 (Pixel) = P

(I,j)	0	1	2	3	4	5	6	7
0	168	157	154	161	170	171	169	169
1	169	158	152	157	167	170	169	168
2	173	160	150	153	163	168	169	167
3	178	165	153	153	161	169	170	168
4	181	171	160	157	162	169	172	170
5	180	176	169	163	164	169	172	170
6	177	178	175	168	165	168	170	169
7	172	178	178	170	165	166	168	167

Matriks = 8x8

M = 8

N = 11

Keterangan :

Size Citra Asli = 40,4 Kb

Size Crop Citra = 309 bytes

Dimensions Citra Asli = 640 x 360

Dimensions Crop Citra = 8 x 8

### 1. Enkripsi *Baker's Map* dan *Logistic Map*

$$\begin{aligned} EBM &= \frac{m}{n} (R + P) + S \bmod \left(\frac{m}{n}\right) \\ &= \frac{8}{11} (0 + 168) + 0 \bmod \left(\frac{8}{11}\right) \end{aligned}$$

$$EBM = 122,1818182$$

Lakukan langkah diatas sampai  $P_i \dots n$

$$\begin{aligned} ELM &= (EBM + n) \bmod (256) \\ &= (122,1818182 + 11) \bmod (256) \\ &= 133,1818182 \bmod (256) \end{aligned}$$

$$ELM = 133,1818182$$

Lakukan langkah diatas sampai  $P_i \dots n$

### 2. Dekripsi *Logistic Map* dan *Baker's Map*

$$\begin{aligned} DLM &= (P - n) \bmod (256) \\ &= (133,1818182 - 11) \bmod (256) \end{aligned}$$

$$DLM = 122,1818182$$

Lakukan langkah diatas sampai  $P_i \dots n$

$$\begin{aligned} DBM &= \frac{DLM - \left(\frac{m}{n} (R) + S \bmod \left(\frac{m}{n}\right)\right)}{\left(\frac{m}{n}\right)} \\ &= \frac{122,1818182 - \left(\frac{8}{11} (0) + 0 \bmod \left(\frac{8}{11}\right)\right)}{\left(\frac{8}{11}\right)} \end{aligned}$$

$$\left(\frac{8}{11}\right)$$

$$= \frac{122,1818182 - (0 + 0)}{0,727272727}$$

$$\text{DBM} = 168$$

**Tabel 3.2** Matriks Citra Hasil Enkripsi

(I,j)	0	1	2	3	4	5	6	7
0	133,18 18	125,909 1	124,454 5	130,272 7	137,545 5	139	138,272 7	139
1	134,18 18	126,181 8	123,272 7	127,636 4	135,636 4	138,545 5	138,545 5	138,545 5
2	137,36 36	128,636 4	122,090 9	125	133	137,363 6	138,818 2	138,545 5
3	140,54 55	131,818 2	123,818 2	124,545 5	131,090 9	137,363 6	138,818 2	138,363 6
4	143	136,454 5	129,181 8	127,727 3	132,090 9	137,909 1	140,818 2	140,090 9
5	142,54 55	140,363 6	136	132,363 6	133,818 2	138,181 8	141,090 9	140,363 6
6	139,90 91	141,363 6	139,909 1	135,545 5	134,090 9	137	139,181 8	139,181 8
7	136,54 55	141,636 4	142,363 6	137,272 7	134,363 6	135,818 2	138	138

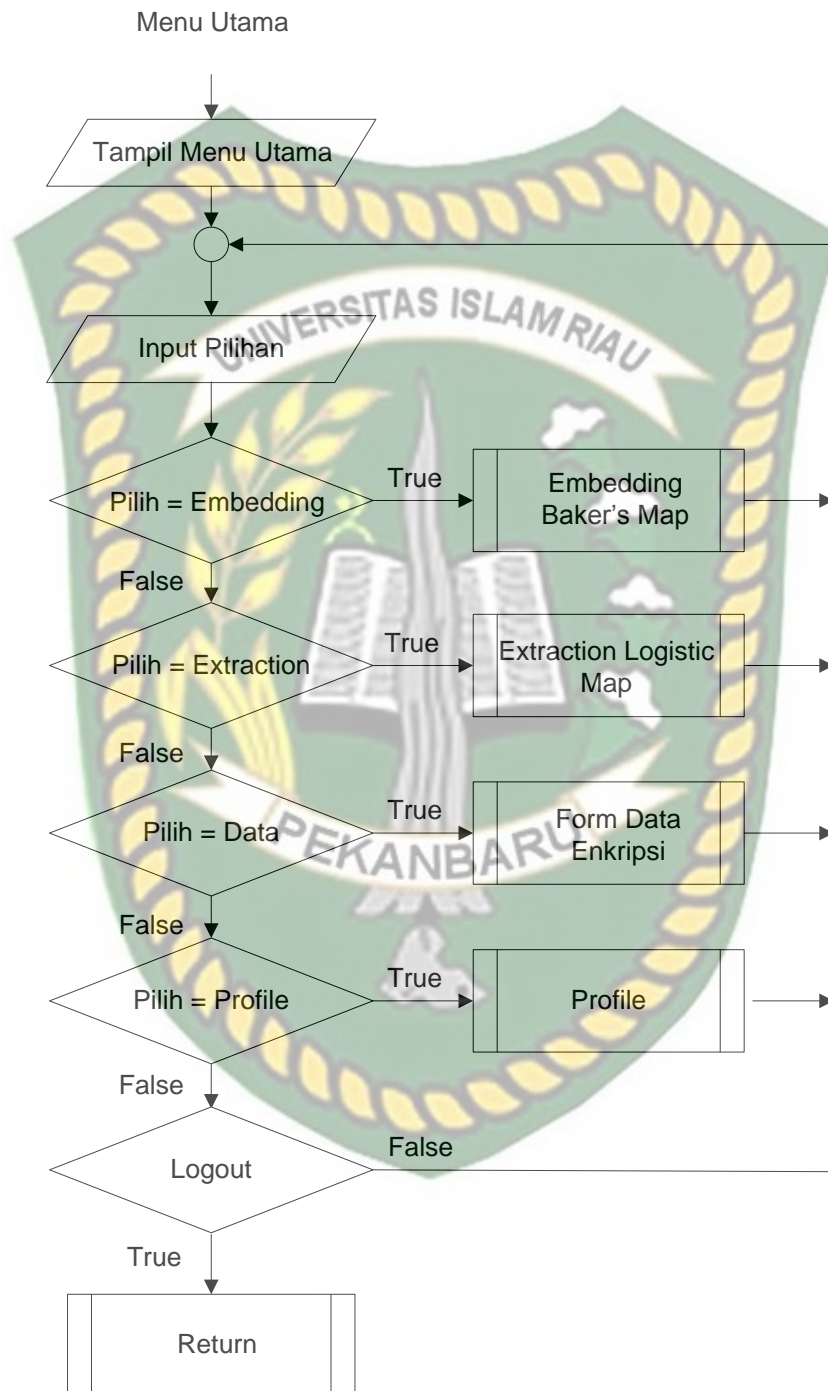
### 3.8.1 Flowchart Login



**Gambar 3.15** Flowchart Login

Pada gambar 3.15 program *flowchart* login diatas merupakan tampilan awal. Hal pertama yang dilakukan setelah membuka sistem ini yaitu dengan menginputkan *username* dan *password* untuk mengoperasikan sistem selanjutnya.

### 3.8.2 Flowchart Menu Utama



**Gambar 3.16** Flowchart Menu Utama

Pada gambar 3.16 diatas dapat dilihat, pada saat program dijalankan atau *start* akan ditampilkan menu utama dan terdapat menu pilihan yaitu *Embedding*,

*Extraction, Data, Profile, dan Exit.* Ketika salah satu menu dipilih, akan menampilkan tampilan menu tersebut dan ketika selesai akan kembali ketampilan menu utama, setelah *stop* program akan keluar.

### 3.8.3 Flowchart Embedding



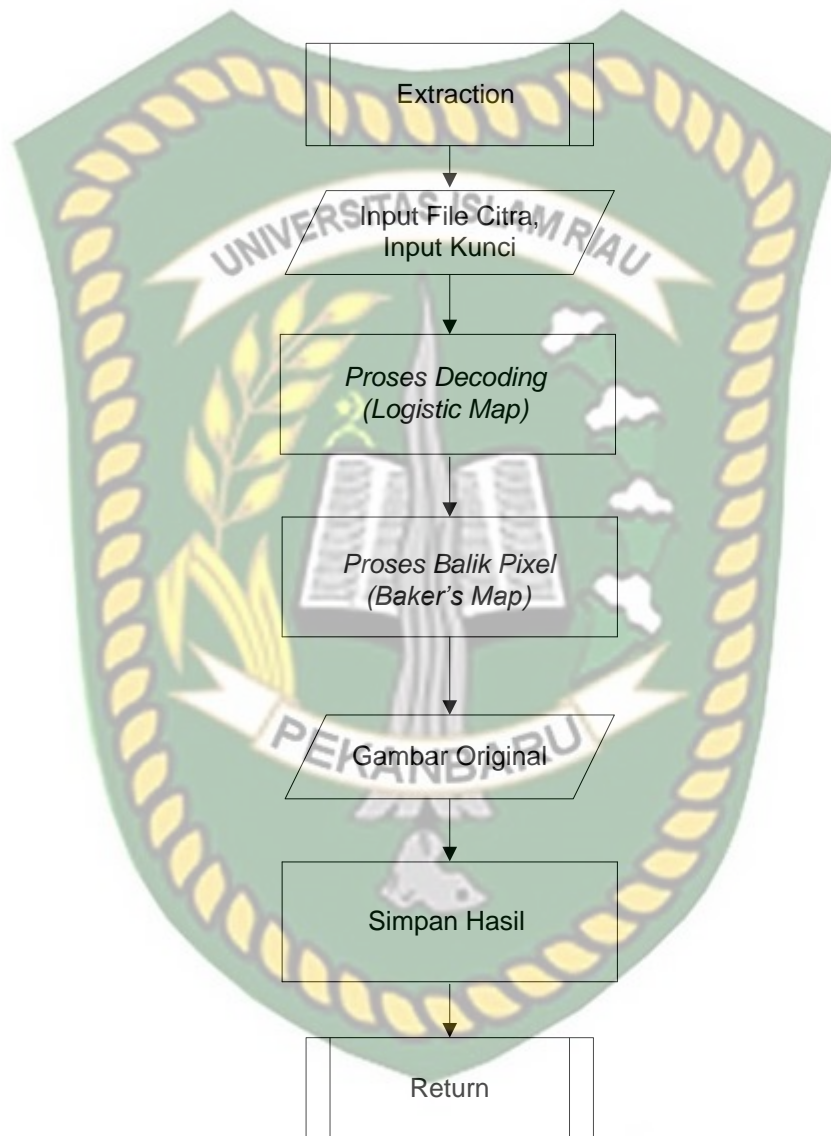
**Gambar 3.17** Flowchart Menu Embedding

Pada gambar 3.17 diatas dapat dilihat, pada saat menu embedding maka akan tampil menu embedding maka pilih embedding. Pada menu embedding terdapat beberapa inputan yaitu, input file citra, input kunci. Setelah dilakukan 2



inputan tersebut selanjutnya akan dienkrripsikan file citra yang telah diinputkan sebelumnya, dan hasil enkripsi atau gambar cipher akan tersimpan ke database.

#### 3.8.4 *Flowchart Extraction*



**Gambar 3.18** *Flowchart Menu Extraction*

Pada gambar 3.18 diatas dapat dilihat, pada saat menu *extraction* dipilih akan menampilkan menu *extraction*. Pada menu ini terdapat menu *extraction* dan terdapat beberapa inputan, yang menjadi outputnya gambar original dan setelah direturn program akan kembali ke menu utama.

## BAB IV

### PEMBAHASAN DAN HASIL

Dalam pembuatan sistem yang telah dirancang dan dibangun maka dilakukan pengujian terlebih dahulu, pengujian yang dilakukan untuk mengetahui hasil yang diberikan oleh sistem dari kombinasi kriptografi baker's map dan Logistic map untuk keamanan citra. Pengujian yang akan dilakukan pada sistem ini dengan metode *black box*.

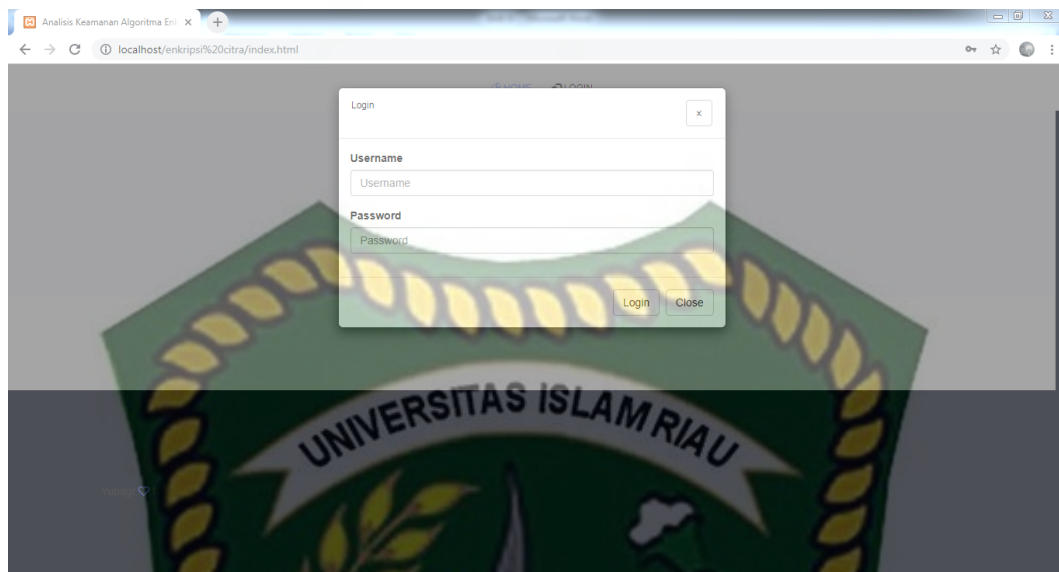
#### 4.1 Pengujian Black Box

Pengujian black box (*Black Box Testing*) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas sistem, khususnya pada input dan output, apakah sistem telah sesuai dengan apa yang diharapkan atau belum. Maka hasil dari pengujian *black box* pada sistem kombinasi kriptografi baker's map dan Logistic map untuk keamanan citra adalah sebagai berikut dapat dilihat dibawah ini.

#### 4.2 Penjelasan Sistem

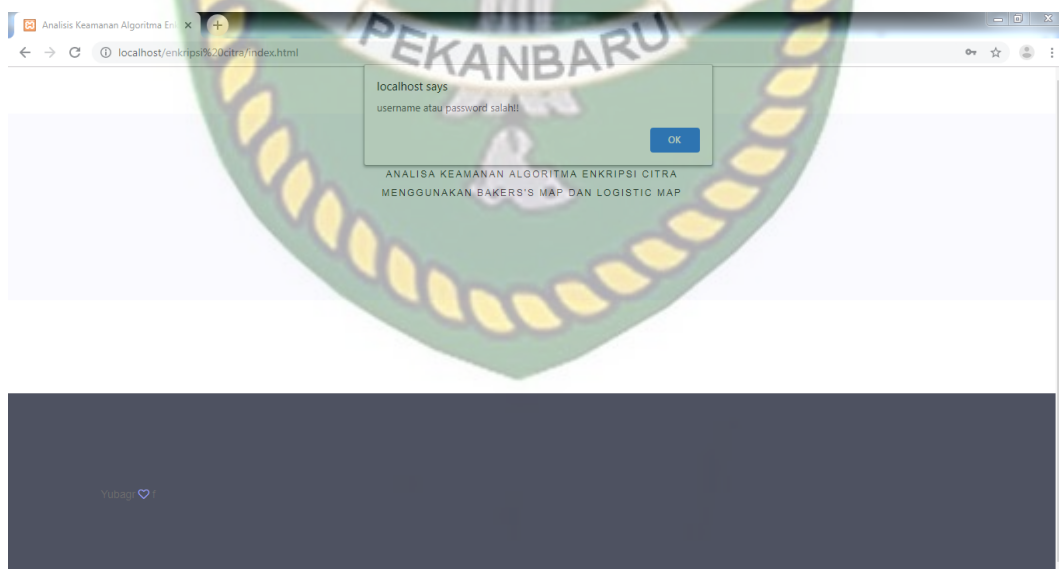
##### 4.2.1 Form Login

Form login ini bertujuan untuk pengamanan sistem bagi pengguna karena tidak sembarangan orang bisa masuk dengan bebas kedalam sistem dan hanya bagi pengguna yang sudah terdaftar saja yang dapat masuk. Untuk lebih jelasnya dapat dilihat pada gambar 4.1



**Gambar 4.1** Form Login

Pada gambar 4.1 dapat dijelaskan bahwa jika pengguna ingin masuk kedalam sistem pengguna harus terlebih dahulu menginputkan *username* dan *password* dengan benar yang sudah terdaftar didalam sistem.



**Gambar 4.2** Peringatan gagal login

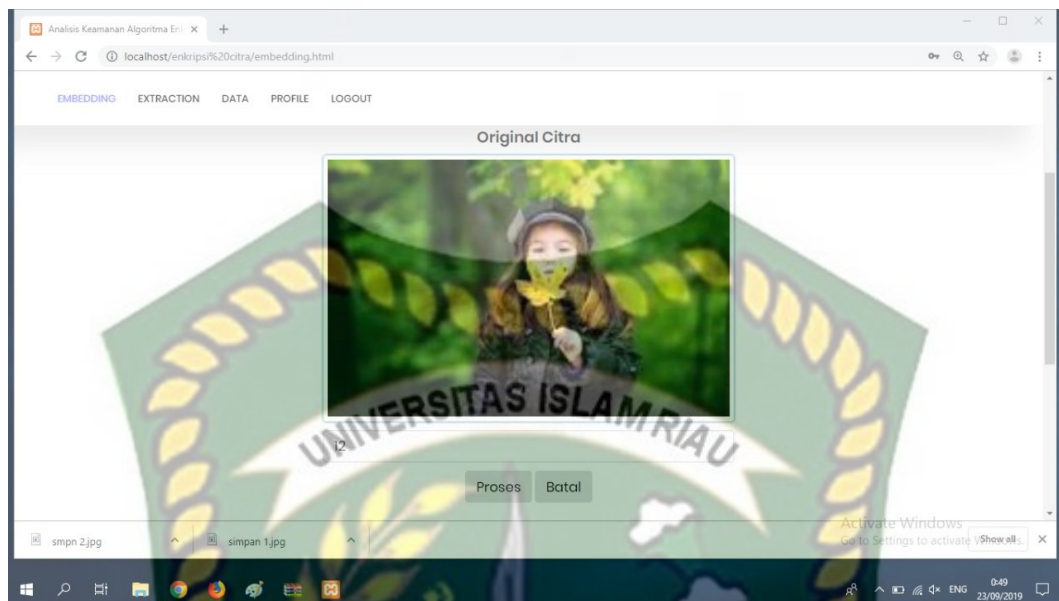
Pada gambar 4.2 dapat dijelaskan apabila pengguna menginputkan username atau password yang salah akan keluar tampilan pesan yang berisi username atau password salah.

**Tabel 4.1** Pengujian Form Login

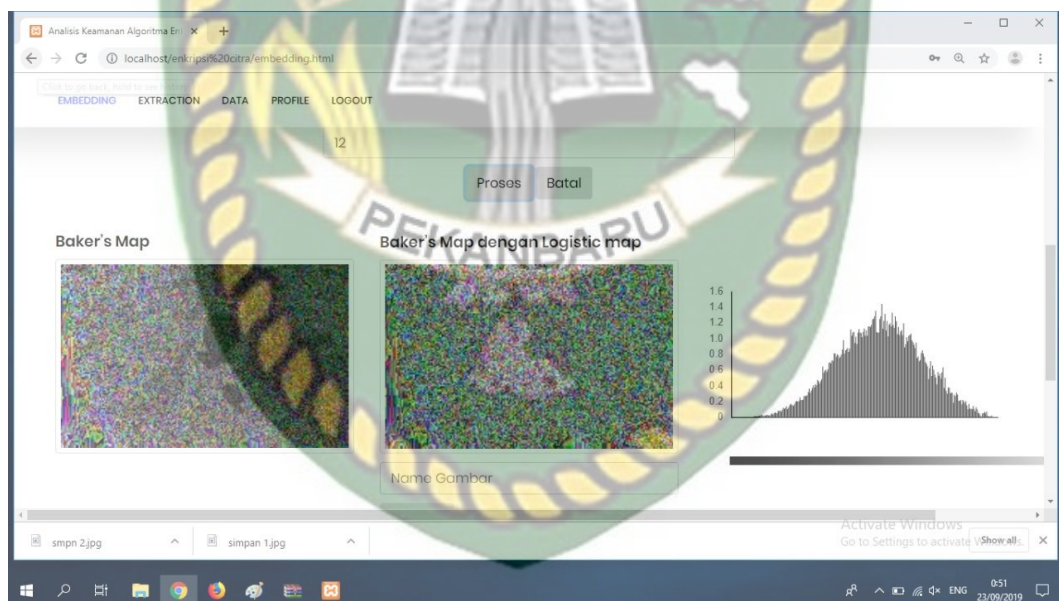
No	Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Form login	Username :- Password : - Kemudian klik <i>login</i>	Sistem menolak dengan menampilkan pesan : “Username dan password salah”.	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
		Username : uji (salah) Password : uji (salah) Kemudian klik <i>login</i>	Sistem menolak dengan menampilkan pesan : “Username dan password salah”.	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
		Username : user123 Password : citra Kemudian klik <i>login</i>	Sistem menerima dan menampilkan halaman menu utama	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai

#### 4.2.2 Form Menu Embedding

Form Menu Embedding merupakan menu yang disediakan untuk proses enkripsi citra. Hasil enkripsi citra tersebut berupa chiper image. Untuk melakukan enkripsi citra, maka user diharuskan mengisi semua form yang ada pada menu embedding. Proses enkripsi pesan dapat dilihat pada gambar 4.3.



**Gambar 4.3** Form Menu Embedding (Input Gambar)



**Gambar 4.4** Form Menu Embedding (Hasil Enkripsi)



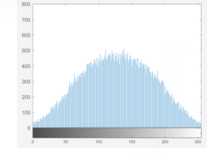
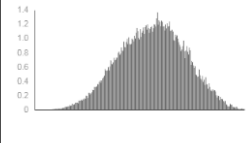

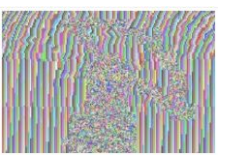
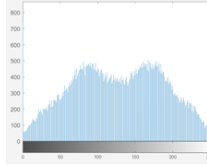
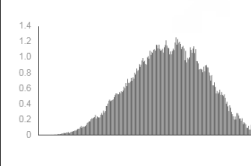
Pada gambar 4.3 dan gambar 4.4 dapat dijelaskan ketika pengguna ingin melakukan enkripsi maka pengguna harus menginputkan beberapa form yang tersedia seperti pilih citra yang akan dienkrpsi kemudian menginputkan kunci. Dan setelah gambar berhasil dienkrpsi dapat dilihat perbedaan antara hasil

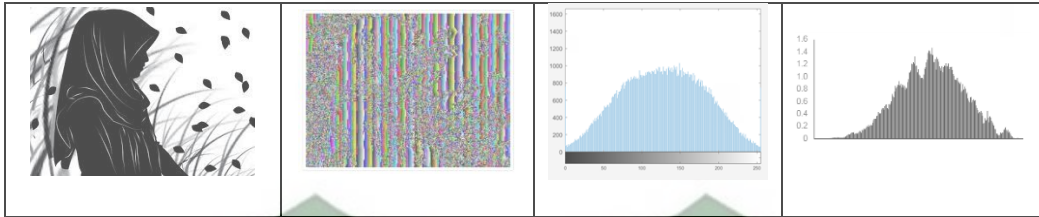
enkripsi hanya menggunakan algoritma *baker's map* dan hasil menggunakan algoritma *baker's map* dan ditambah algoritma *logistic map*. Dan selanjutnya pengguna diharuskan mengisi nama file jika pengguna ingin menyimpan hasil enkripsi kedalam database.

**Tabel 4.2** Pengujian Form Embedding

No	Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Form Embedding	Mengupload atau memilih file citra	File citra berhasil ditampilkan	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
		Menginputkan <i>key</i>	Kunci yang diinputkan tidak melebihi 3 digit	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
		Menampilkan hasil proses enkripsi	Tampil <i>cipher image</i>	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
		Menyimpan hasil enkripsi ( <i>cipher image</i> )	Berhasil tersimpan ke <i>database</i>	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai

**Tabel 4.3** Kesimpulan Analisa Histogram

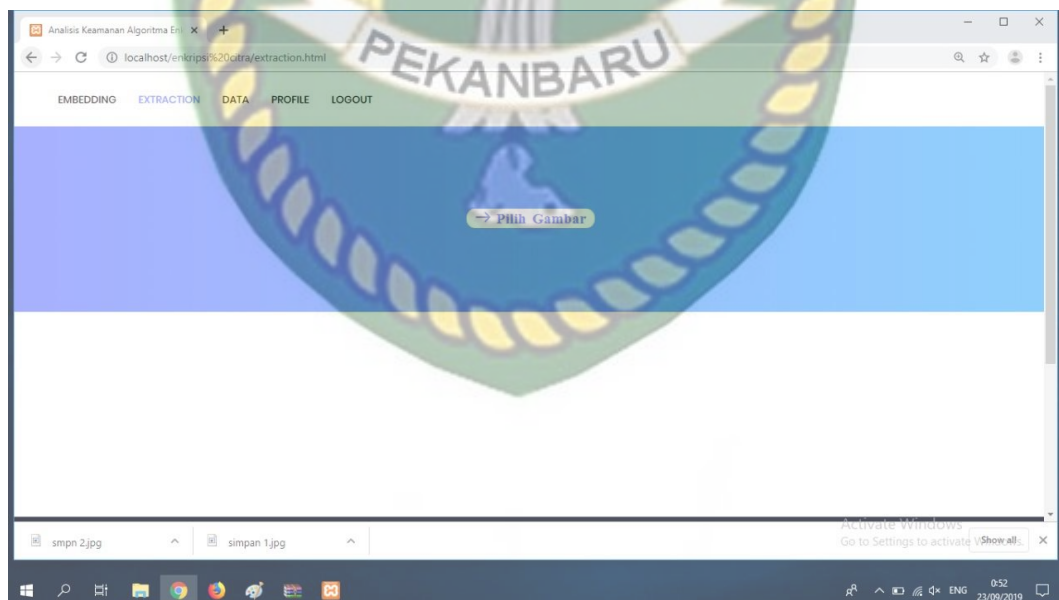
<i>Plain image</i>	<i>Cipher image</i>	Histogram <i>Plain image</i>	Histogram <i>Cipher image</i>
			
			



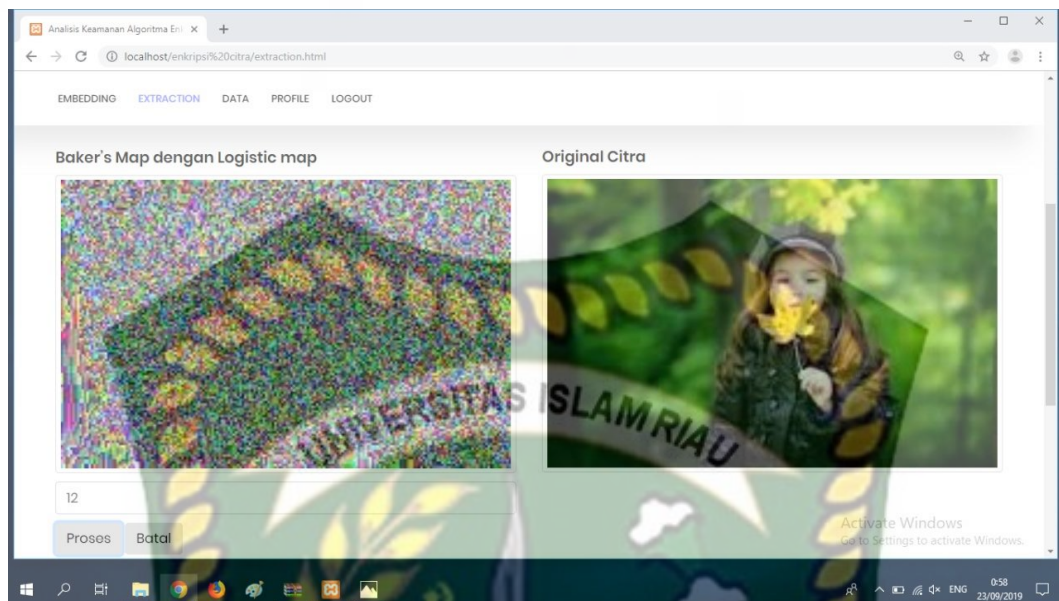
Pada tabel 4.3 diatas dapat diambil kesimpulan berdasarkan analisa histogram terlihat bahwa histogram *plain image* berbeda dengan histogram *cipher image*. Terlihat histogram *plain image* bervariasi, sedangkan histogram *cipher image* terlihat datar.

#### 4.2.3 Form Menu Extraction

Form menu extraction merupakan menu yang disediakan untuk mengekstrak citra yang telah di enkripsi sebelumnya. Sehingga cipher image menjadi gambar original. Proses extraction dapat dilihat pada gambar 4.5.



**Gambar 4.5** Form Menu Extraction (pilih gambar)



**Gambar 4.6** Form Menu Extraction (proses dekripsi)

Pada gambar 4.5 dan gambar 4.6 dapat dijelaskan jika pengguna ingin melakukan extraction atau pengembalian cipher image menjadi citra original maka ada beberapa yang harus dilakukan yaitu pertama pengguna mencari file yang ingin didekripsi kemudian pengguna menekan tombol proses agar sistem memproses file tersebut.

**Tabel 4.4** Pengujian Form Extraction

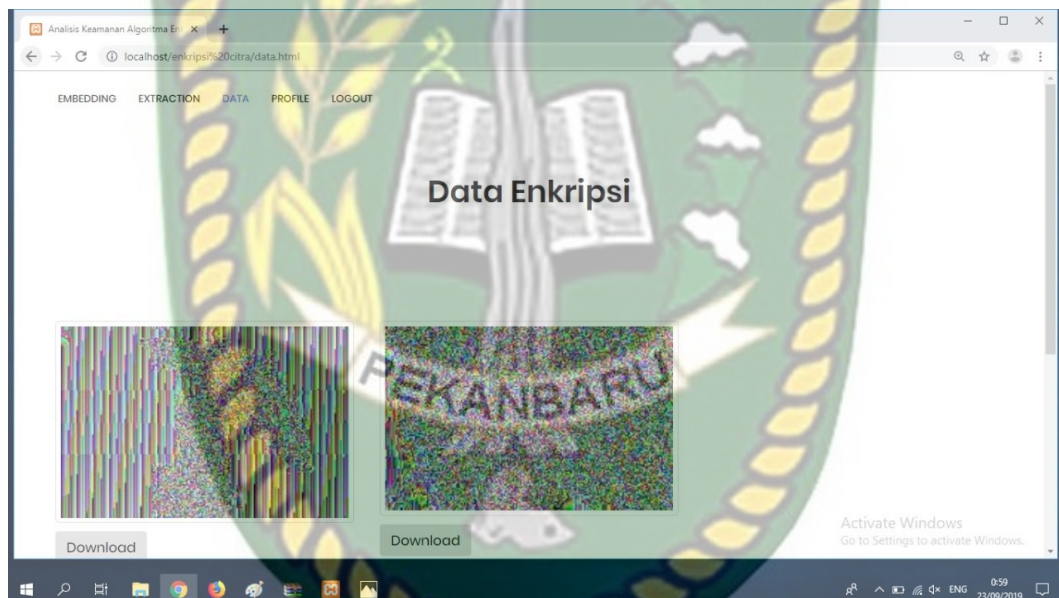
No	Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Form Extraction	Memilih file yang akan didekripsi atau pengembalian ke citra original dengan cara menginputkan nama file yang telah disimpan sebelumnya	File berhasil diambil dari dalam <i>database</i>	[✓] Sesuai [ ] Tidak Sesuai



		Klik tombol proses	<i>Cipher image</i> kembali ke citra original	<input checked="" type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai
--	--	--------------------	---	---

#### 4.2.4 Form Menu Data

Form menu data merupakan menu yang disediakan untuk menampilkan hasil enkripsi atau cipher image yang tersimpan sebelumnya didalam database. Berikut isi dari menu data dapat dilihat pada gambar 4.7.



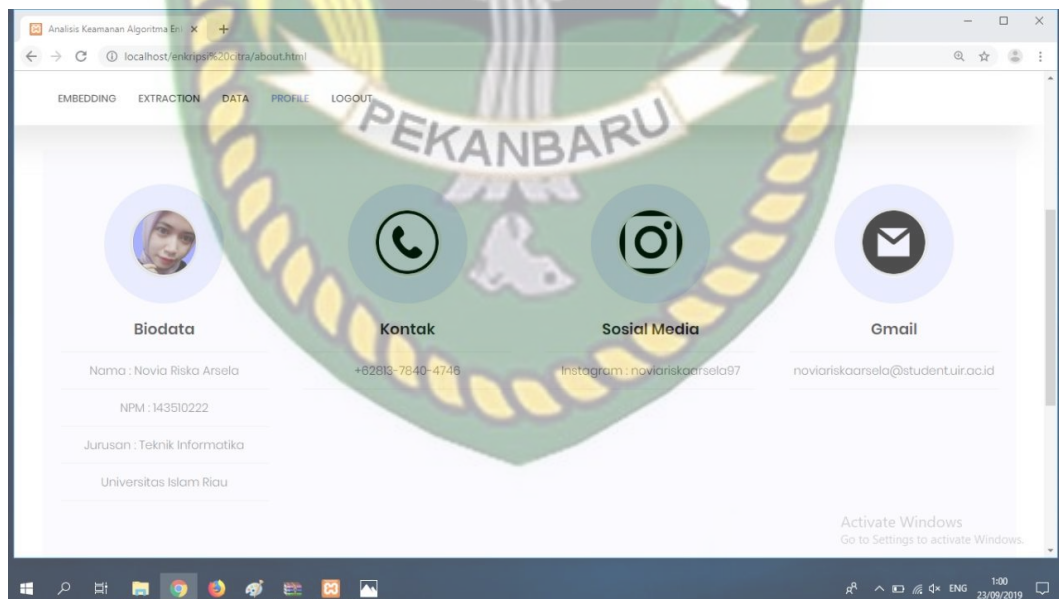
Gambar 4.7 Form Menu Data

Tabel 4.5 Pengujian Form Menu Data

No	Komponen yang Diuji	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Form Menu Data	Menampilkan <i>cipher image</i> atau file hasil enkripsi yang telah disimpan oleh pengguna ke dalam <i>database</i>	<i>Cipher image</i> berhasil tampil	<input type="checkbox"/> Sesuai <input type="checkbox"/> Tidak Sesuai

#### 4.2.5 Form Menu Profile

Form menu About merupakan menu yang disediakan untuk menampilkan informasi tentang penulis. Menu profile dapat dilihat pada gambar 4.8.



Gambar 4.8 Form Menu Profile

### 4.3 Kesimpulan Hasil Pengujian Black Box

Dari hasil pengujian Kombinasi kriptografi Baker's Map dan Logistic Map untuk keamanan citra yang dilakukan dengan metode black box maka dapat diperoleh kesimpulan sebagai berikut:

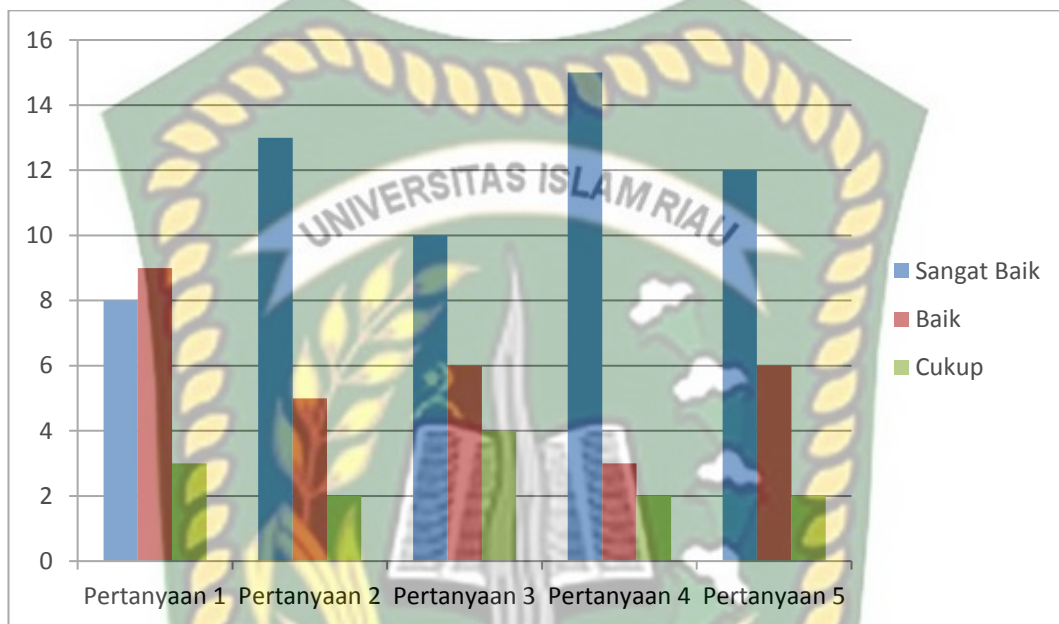
1. Dari seluruh pengujian yang dilakukan pada setiap bagian sistem ini semuanya dapat berfungsi dan berjalan dengan baik.
2. Pengujian pada sisi user dalam kombinasi kriptografi seluruhnya berjalan dengan baik dan sesuai harapan.
3. Pengujian fitur yang terdapat pada sistem dapat berjalan dengan normal dan sesuai dengan output yang diharapkan.

### 4.4 Kesimpulan Hasil Implementasi

Pengujian sistem dari kombinasi kriptografi ini juga dilakukan dari sisi pengguna, yang dalam hal ini adalah user. Pada pengujian ini dibuat dengan 4 pertanyaan yang disebarakan kepada 20 responden (Mahasiswa dan Masyarakat). Adapun lima pertanyaan tersebut adalah sebagai berikut:

1. Bagaimana pendapat anda mengenai desain tampilan Aplikasi ini?
2. Apakah Aplikasi mudah digunakan (*User Friendly*)?
3. Apakah bahasa yang digunakan dalam aplikasi ini dapat dimengerti dengan baik?
4. Apakah sistem ini bermanfaat?
5. Apakah sistem kombinasi Kriptografi ini dapat menjaga keamanan gambar atau citra dengan baik?

Dari pertanyaan-pertanyaan diatas, maka hasil jawaban atau tanggapan dari responden terhadap kinerja dari sistem berdasarkan pertanyaan yang diajukan adalah sebagai berikut:



**Gambar 4.9** Grafik Hasil Kuisisioner

1. Bagaimana pendapat anda mengenai desain tampilan Aplikasi ini memiliki nilai Sangat Baik: 8 responden, Baik: 9 responden, Cukup: 3 responden.
2. Apakah Aplikasi mudah digunakan (*User Friendly*) memiliki nilai Sangat Baik: 13 responden, Baik: 5 responden, Cukup: 2 responden.
3. Apakah bahasa yang digunakan dalam aplikasi ini dapat dimengerti dengan baik memiliki nilai Sangat Baik: 10 responden, Baik: 6 responden, Cukup: 4 responden.
4. Apakah sistem ini bermanfaat memiliki nilai Sangat Baik: 15 responden, Baik: 3 responden, Cukup: 2 responden.

5. Apakah sistem kombinasi Kriptografi ini dapat menjaga keamanan data dengan baik memiliki nilai Sangat Baik: 12 responden, Baik: 6 responden, Cukup: 2 responden.

Berdasarkan hasil kuisioner mahasiswa/i dan masyarakat tersebut maka dapat disimpulkan dengan menggunakan skala likert yang telah dimodifikasi, yaitu responden memilih 3 jawaban yang tersedia dengan keterangan, yakni Sangat Baik, Baik dan Cukup. berdasarkan Kombinasi kriptografi Baker's map dan Logistic Map untuk keamanan Citra ini memiliki persentase sebagai berikut :

**Tabel 4.6** Hasil Nilai Presentase Tiap Pertanyaan Kuisioner

No	Keterangan	Jumlah Presentase Responden		
		Sangat Baik	Baik	Cukup
1	Bagaimana pendapat anda mengenai desain tampilan aplikasi ini?	40%	45%	15%
2	Apakah Aplikasi mudah digunakan ( <i>User Friendly</i> )?	65%	25%	10%
3	Apakah bahasa yang digunakan dalam aplikasi ini dapat dimengerti dengan baik?	50%	30%	20%
4	Apakah sistem ini bermanfaat?	75%	15%	10%
5	Apakah sistem kombinasi Kriptografi ini dapat menjaga keamanan data dengan baik?	60%	30%	10%
Total		58%	29%	13%

Dari hasil persentase tabel diatas, yang didasarkan pada 5 pertanyaan yang diajukan secara langsung oleh penulis kepada 20 responden (Mahasiswa dan Masyarakat), dapat diambil kesimpulan bahwa kombinasi kriptografi baker's map dan logistic map untuk keamanan citra ini memiliki *performance* baik dengan

nilai  $(40\% + 65\% + 50\% + 75\% + 60\%)/5 = 58\%$ , jadi persentase rata-rata terbesar 58%, sehingga sistem ini dapat diimplementasikan.



Dokumen ini adalah Arsip Miik :

**Perpustakaan Universitas Islam Riau**

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 Kesimpulan

Berdasarkan hasil analisa dan pengujian pada bab sebelumnya dalam Analisis Keamanan Algoritma Enkripsi Citra Menggunakan Baker's Map dan Logistic Map, maka dapat ditarik beberapa kesimpulan yaitu :

1. Dengan adanya sistem Keamanan Enkripsi Citra Menggunakan Baker's Map dan Logistic Map dapat membantu user menjaga kerahasiaan sebuah citra.
2. Dapat menghalangi serangan yang dilakukan oleh pihak tidak bertanggung jawab dengan menggunakan Kriptografi.
3. Hasil simulasi program kriptografi dengan menggunakan algoritma *baker's map* dan *logistic map* memiliki hasil citra yang lebih terjaga kerahasiaannya dibandingkan citra asli.
4. Berdasarkan hasil analisa yang diperoleh, sistem kriptografi ini memiliki batasan citra yang dapat dienkripsi atau diproses yaitu hanya citra yang memiliki ukuran dimensi yang kecil dari 3000x4000 pixel.

#### 5.2 Saran

Adapun saran dari penulis dalam Analisis Keamanan Algoritma Enkripsi Citra Menggunakan Baker's Map dan Logistic Map ini adalah sebagai berikut:

1. Penelitian selanjutnya diharapkan dapat mengembangkan sistem ini untuk perangkat *mobile* agar lebih mudah digunakan oleh masyarakat luas.

2. Mengkaji lebih lanjut mengenai kombinasi algoritma baker's map dan logistic map dengan algoritma lain atau sejenisnya agar lebih menemukan hasil yang lebih sempurna.



Dokumen ini adalah Arsip Miik :

Perpustakaan Universitas Islam Riau



## DAFTAR PUSTAKA

- Irfan Pahrul, 2016, *Aplikasi Enkripsi Citra Menggunakan Algoritma Kriptografi Arnold Cat Map Dan Logistic Map*, STMIK Bumigora, Mataram
- Purba Ronsen, Dkk, 2014, *Enkripsi Citra Digital Menggunakan Arnold's Cat Dan Nonlinear Chaotic Algorithm*, STMIK MIKROSKIL, Medan
- Fitria Aida, Dkk, 2017, *Implementasi Algoritma Baker Map Untuk Enkripsi Citra Pada Perangkat Android*, Universitas Islam Madura, Madura
- Wijaya Halim Futu, Dkk, 2015, *Analisis Algoritma Catmap Untuk Keamanan Data Citra Satelit-Nano Pada Low Earth Orbit*, Telkom University, Bandung
- Munir Rinaldi, 2012, *Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map*, Institut Teknologi Bandung
- Munir,S., 2004, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika : Bandung.
- Anhar., 2010, *Panduan Menguasai PHP & MYSQL Secara Otodidak*, Media Kita, Jakarta