IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMANT* (RSA) PADA FILE CITRA

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Persyaratan dalam Memperoleh Gelar Sarjana Matematika (S.Mat)

OLEH :

NOFA RAIHANA FAJRIYAH
H72214018

PROGRAM STUDI MATEMATIKA
JURUSAN SAINS
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
SURABAYA

2018

PERNYATAAN KEASLIAN

Yang bertandatangan dibawah ini:

Nama : Nofa Raihana Fajriyah

NIM : H72214018

Program Studi : Matematika

Angkatan : 2014

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: **Implementasi Algoritma *Rivest Shamir Adlemant* (RSA) Pada File Citra**. Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya akan menerima sanksi yang telah ditetapkan. Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 3 Agustus 2018

Nofa Raihana Fajriyah

NIM.H72214018

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMANT* (RSA) PADA FILE CITRA

Disusun oleh
Nofa Raihana Fajriyah
NIM.H72214018

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 18 Juli 2018
Dan dinyatakan telah memenuhi syarat
untuk memperoleh gelar
Sarjana Matematika (S.Mat)

Dewan Penguji

Penguji I

Nurissaidah Ulinnuha, M.Kom
NIP.199011022014032004

Penguji II

Aris Fanani, M.Kom
NIP.198701272014031002

Penguji III

Dian C. Rini Novitasari, M.Kom
NIP.198511242014032001

Penguji IV

Putroue Keumala Intan, M.Si
NIP.198805282018012001

Mengesahkan
Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. Eni Purwati, M.Ag
NIP.196512211990022001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : NOFA RAIHANA FAJRIYAH
NIM : H72214018
Fakultas/Jurusan : SAINTEK/ MATEMATIKA
E-mail address : nofaraihana@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
☑ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :
IMPLEMENTASI ALGORITMA RIVEST SHAMIR ADLEMANT (RSA) PADA FILE CITRA

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 2 Agustus 2018

Penulis

(NOFA RAIHANA F.)

IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMANT* (RSA) PADA FILE CITRA

ABSTRAK

Keamanan data merupakan hal yang sangat penting bagi instansi maupun perusahaan. Salah satu data penting yang perlu diamankan adalah data citra. Citra merupakan pesan multimedia yang sering disalahgunakan. Sehingga diperlukan aplikasi untuk pengamanan data citra. Salah satu ilmu yang berkaitan dengan pengamanan adalah kriptografi. Algoritma *Rivest Shamir Adlemant* (RSA) merupakan salah satu algoritma kriptografi yang dapat digunakan untuk enkripsi dan dekripsi data. Keunggulan dari algoritma RSA adalah belum ditemukan algoritma yang tepat untuk melakukan dekripsi algoritma RSA dengan memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Oleh karena itu pada penelitian ini akan diimplementasikan algoritma RSA pada file citra. Proses pengamanan data citra pada penelitian ini dimulai dari pembangkitan kunci, enkripsi, dekripsi, dan pengujian. Pengujian yang dilakukan dalam penelitian ini meliputi pengujian pembangkitan kunci, pengujian citra terenkripsi, dan pengujian kemiripan menggunakan nilai MSE dan PSNR. Hasil dari penelitian ini dapat digunakan untuk mengenkripsi dan mendekripsi citra dengan baik. Pada pengujian pembangkitan kunci didapatkan hasil penggunaan kunci dengan rentang yang lebih besar dapat menghasilkan citra enkripsi yang sulit dikenali. Namun, hasil enkripsi pada algoritma ini ketika diuji menggunakan *enhancement*, *bluring*, dan *cropping* tidak dapat kembali sesuai citra aslinya. Dari hasil MSE dan PSNR antara citra asli dengan citra hasil dekripsi nilainya mendekati 0, namun tidak 100% mirip. Hal itu disebabkan ketika proses dekripsi ada beberapa nilai *pixel* citra yang tidak kembali sesuai nilai semula.

Kata Kunci : Kriptografi, RSA, Citra Digital

IMPLEMENTATION RIVEST SHAMIR ADLEMANT (RSA) ALGORITHM ON THE IMAGE FILE

ABSTRACT

Data security is a very important for an institution or company. One of the important data that needs to be secured is image data. Image is a multimedia message that is often misused. Therefore required an application for data security in the form of images. One of concept which is discuss about security is cryptography. In cryptography there are many algorithms used for image security. Rivest Shamir Adlemant (RSA) algorithm is one of cryptography algorithm which is used to encrypt and decrypt data. Advantage of RSA algorithm there is no decryption algorithm that effective to factoring large number into prime factor. This research will implement RSA algorithm in image file. Process of this research starts from key generation, encryption, decryption, and testing. In this research testing include key generation testing, encrypted image testing, and similarity testing using MSE and PSNR value. The result of this research RSA algorithm can be used to encrypt and decrypt the image well. The result of key generation testing if using key with a large range can produce the encrypted image is difficult to recognize. The encryption result of this algorithm when tested using enhancement, bluring, and cropping can not return according to the original image. From MSE result between the original image and decrypted image the value is close to 0, but not 100% similar, because when the decryption process there are some pixel image values that do not return according to the original image.

Keyword : Cryptography, RSA, Citra Digital.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam suatu instansi salah satu hal yang sangat penting adalah keamanan data, apalagi untuk menghadapi persaingan bisnis. Dibutuhkan sistem penyimpanan dan pengiriman yang akurat untuk data yang bersifat rahasia. File citra merupakan salah satu bentuk data yang berharga pada suatu instansi. Misalnya pada konsultan desain ada pemesan yang membatalkan pesanannya, namun rancangan design yang telah dikirim pada pemesan tetap digunakan, tentunya hal tersebut merugikan kosultan desain tersebut. Adapun permasalahan lain yang berkaitan dengan pengamanan data adalah adanya gambar atau file citra yang diubah atau digunakan tanpa sepengetahuan pemiliknya. Permasalahan tersebut merupakan salah satu tindak pencurian. Tindak pencurian sendiri merupakan tindakan yang dilarang oleh Allah SWT, sebagaimana yang tercantum pada QS Al – Maidah ayat 38, yang bunyinya:

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيم

Artinya : "*Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. Dan Allah Maha Perkasa lagi Maha Bijaksana.*"

Pada ayat tersebut menjelaskan tentang pembalasan bagi orang yang mencuri. Maka bagi setiap orang yang melakukan tindakan manipulasi citra akan mendapat balasan yang setimpal dengan orang yang mencuri.

Berdasarkan kasus keamanan file citra yang ada, maka diperlukan adanya sistem untuk mengamankan citra. Dalam hal ini khususnya untuk membatasi penggunaan gambar yang tidak digunakan sebagaimana mestinya oleh pihak yang tidak bertanggung jawab. Salah satu solusi atas kasus tersebut adalah mengamankan citra digital tersebut dengan cara menyamarkan gambar digital sehingga tidak dapat dilihat tanpa menggunakan kode yang telah dibuat oleh pemilik gambar tersebut.

Kriptografi adalah salah satu ilmu yang mempelajari tentang keamanan data. Kriptografi merupakan ilmu yang membahas teknik matematika yang berkaitan dengan topik keamanan informasi, semisal tentang kerahasiaan.Kriptografi bertujuan agar pesan yang bersifat rahasia dapat dikirim melalui suatu jaringan tanpa diketahui dan dimanfaatkan oleh pihak yang tidak berkepentingan.

Pada ilmu kriptografi terdapat beberapa algoritma yang digunakan untuk pengamanan data. Telah banyak algoritma kriptografi kunci publik yang digunakan untuk pengamanan data. Namun, algoritma yang cukup terkenal adalah *Rivest Shamir Adlement* (RSA) (Munir, Kriptografi, 2006). Nama Algoritma RSA merupakan singkatan dari ketiga peneliti dari dari *Massachussets Institute of Technology* (MIT) , yaitu Ronald Linn Rivest, Adi Shamir, dan Len Adleman. (Ashari Arief, 2016). Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor-faktor prima dari bilangan yang besar.Hasil pemfaktoran tersebut yang digunakan untuk memperoleh kunci privat. Selama belum ditemukan algoritma yang tepat untuk

memfaktorkan bilangan yang besar menjadi faktor prima, maka selama itu pula keamaanan algoritma RSA tetap terjaga.

Ada beberapa penelitian terdahulu mengenai implementasi algoritma RSA. Algoritma RSA dapat diimplementasikan untuk enkripsi dekripsi, pesan teks, email, maupun pesan gambar (Pahrizal & Pratama, 2016). Salah satu penelitian yang menerapkan algortima RSA pada *image* adalah penelitian dari Sukaesih dan Sri Wahyuni. Dalam penelitian tersebut didapatkan hasil bahwa algoritma RSA dapat mengenkripsi dan dekripsi gambar dengan baik (Sukaesih & Wahyuni, 2016). Hal ini dikarenakan kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi pada algoritma RSA ini.

Pada penelitian sebelumnya telah terdapat pula penelitian mengenai penerapan algoritma RSA pada image. Pada penelitian tersebut menggunakan gambar bitmap sebagai plainteksnya. Dalam penelian tersebut disebutkan bahwa perlu dilakukan penelitian penerapan algoritma RSA pada file citra dengan menggunakan format lainnya (Rakhman & Kurniawan, 2015). Berdasarkan uraian latar belakang ini, peneliti akan melakukan penerapan algoritma RSA pada file citra.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah yang dapat diambil pada penelitian ini adalah :

1. Bagaimana pembentukan kunci dengan menggunakan Algoritma RSA ?

2. Bagaimana penerapan metode RSA dalam proses enkripsi dan dekripsi file citra?
3. Bagaimana evaluasi pengujian algoritma RSA?

C. Tujuan

Tujuan yang ingin didapatkan dalam penelitian ini adalah:

1. Mengetahui proses pembentukan kunci dengan menggunakan Algoritma RSA.
2. Mengetahui penerapan metode RSA dalam proses enkripsi dan dekripsi file citra.
3. Mengetahui hasil keakuratan algoritma RSA melalui pengujian.

D. Batasan Penelitian

Ada beberapa batasan untuk penelitian ini, adapun batasan tersebut adalah:

1. Data citra yang digunakan adalah data citra dengan ukuran 256×256 *pixel*.
2. Pada penelitian ini tidak dibangun protokoler file dalam pengiriman file citra.
3. Pada penelitian ini menggunakan citra *grayscale* (keabuan).
4. Pada penelitian ini nilai p dan q yang akan digunakan dibatasi dengan rentang $2 - 997$.

E. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memiliki manfaat sebagai berikut :

1. Bagi Peneliti

   Menambah pengetahuan mengenai penerapan kriptografi, khususnya pada Algoritma RSA pada file citra.

2. Bagi Universitas

   Supaya dapat memenuhi referensi bagi penelitian selanjutnya, dan diharapkan dapat dijadikan referensi bagi pihak perpustakaan UIN Sunan Ampel Surabaya.

F. Sistematika Penyusunan

Sistematika penyusunan proposal penelitian ini dibagi mejadi tiga bab, yaitu:

1. **BAB I Pendahuluan,** berisi mengenai latar belakang penelitian, rumusan masalah, tujuan penenlitian, dan sistematika penyusunan penelitian.
2. **BAB II Tinjauan Pustaka,** berisi mengenai teori-teori yang digunakan sebagai dasar penelitian ini yaitu mengenai citra, kriptografi, dan juga Algortima RSA.
3. **BAB III Metode Penelitian,** berisi mengenai alur atau jalannya penelitian ini yaitu mengenai tahap-tahapan yang dilakukan dalam penelitian ini.
4. **BAB IV Hasil dan Pembahasan,** berisi mengenai hasil enkripsi dan dekripsi algoritma RSA.
5. **BAB V Penutup**, berisi tentang kesimpulan yang didapatkan pada penelitian ini dan saran untuk penelitian selanjutnya..

BAB II

TINJAUAN PUSTAKA

Pada bab ini berisikan teori – teori yang bersesuaian dengan penelitian ini, antara lain tentang data citra, kriptografi, dan juga Algoritma RSA.

A. Data Citra

Citra merupakan kumpulan piksel yang disusun dalam struktur dua dimensi (x, y), dimana x menunjukkan indeks baris dan y menunjukkan indeks kolom (Iriyanto & Zaini, 2014). Citra (*image*) merupakan nama lain dari gambar yang menjadi salah satu bentuk multimedia yang mempunyai peran penting sebagai penyampaian informasi visual (Sukaesih & Wahyuni, 2016).Bahkan, ada pepatah yang mengatakan bahwa gambar menyimpan ribuan informasi yang tak mampu diungkapkan oleh kata-kata. Dalam penyampaian informasi, gambar dinilai sebagai media yang lebih efektif digunakan dibandingkan dengan tulisan. Informasi tentang hal-hal yang berhubungan dengan pengetahuan seperti seminar, *talkshow*, kuliah umum lebih banyak disampaikan menggunakan gambar. Format yang dimiliki citra cukup banyak, antara lain JPG, PNG, *Bitmap*, GIF, dan lain-lain. Diantara pesan multimedia lainnya, citra sangat rentan untuk disalahgunakan seperti digandakan, diubah isinya, ataupun dipalsukan. Dikarenakan citra sangat rentan untuk disalahgunakan, maka keamanan citra sangat dibutuhkan.

Citra digital merupakan fungsi intensitas cahaya $f(x, y)$, dimana x dan y merupakan koordinat pada bidang dua dimensi dan harga fungsi tersebut pada setiap titik (x, y) merupakan tingkat kecemerlangan citra pada titik tersebut . Citra digital dapat pula diartikan sebagai suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya menyatakan tingkat keabuan pada titik tersebut. Citra digital biasanya dinyatakan dengan matriks berukuran $m \times n$, dengan m merupakan jumlah baris dan n merupakan jumlah kolom.

$$f(x, y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0, m-1) \\ f(1,0) & f(1,1) & \cdots & f(1, m-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(m-1,0) & f(m-1,1) & \cdots & f(m-1, n-1) \end{bmatrix}$$

B. Kriptografi

1. Definisi Kriptografi

Asal kata kriptografi berasal dari bahasa Yunani yang berasal dari dua kata, yaitu *crypto* dan *graphia. Crypto* dapat diartikan rahasia, dan arti kata *graphia* adalah tulisan, sehingga kriptografi dapat diartikan suatu tulisan yang bersifat rahasia. Menurut istilah, kriptografi merupakan ilmu yang digunakan untuk menjaga keaslian sebuah pesan agar orang lain tidak mudah menyalahgunakan. Menurut Menezes, kriptografi adalah sebuah ilmu yang membahas teknik matematis yang berkaitan dengan topik keamanan informasi(Munir, 2006). Semakin berkembangnya zaman, kegunaan kriptografi bertambah pula. Kegunaan lain dari kriptografi antara lain digunakan

untuk mengidentifikasi pengiriman pesan, mengenalitanda tangan digital dan menguji keaslian pesan dengan sidik jari digital.

Pada algoritma kriptografi aman tidak suatu algoritma ditentukan oleh bagaimana algoritma tersebut bekerja. Algoritma yang seperti ini biasa disebut dengan algoritma terbatas (Arifani, 2016). Algoritma terbatas adalah algoritma yang digunakan oleh suatu organisasi atau sekelompok manusia untuk merahasiakan pesan yang mereka kirim. Pesan tersebut hanya akan diketahui oleh sekelompok manusia pada kumpulan tersebut. Jika suatu hari ada salah satu anggota yang keluar dari kumpulan tersebut, maka algoritma yang digunakan untuk mengirim pesan harus diganti. Jika tidak diganti, akan didapatkan masalah dikemudian hari.

Keamanan kriptografi modern terletak pada bagaimana cara kita merahasiakan kunci yang kita miliki, tanpa harus merahasiakan algoritma tersebut kepada orang lain. Kegunaan dari kunci ini sama dengan kegunaan *password*. Jika seluruh keamanan algoritma bergantung pada kunci yang akan digunakan, maka algoritma tersebut dapat diumumkan dan dianalisis oleh orang lain (Rahmawati, 2014). Jika algoritma yang telah diumumkan dapat dipecahkan oleh orang lain dalam waktu yang singkat, maka algoritma tersebut kurang aman untuk digunakan.

Kerumitan dalam mengolah data ataupun mengolah pesan yang akan disampaikan bukanlah syarat dari algoritma kriptografi yang

baik. Yang lebih penting, algoritma kriptografi yangbaik harus memenuhi empat persyaratan berikut :

1. Kerahasiaan.

   Kerahasiaan yang dimaksud dalam hal ini adalah menjaga informasi dari orang lain, kecuali yang memiliki akses terhadap kunci untuk membuka pesan tersebut.

2. Autentikasi.

   Autentikasi adalah berhubungan dengan pengenalan informasi. Pengirim dan penerima harus dapat dikenali dengan baik. Serta harus memastikan tidak ada penyusup dalam proses pengiriman pesan.

3. Integritas data.

   Integritas data yang dimaksudkan adalah sistem yang digunakan harus dapat mendeteksi bahwa benar-benar tidak ada manipulasi data oleh pihak manapun yang tidak memiliki kepentingan.

4. Non-repudiasi

   Non-repudiasi atau disebut juga nirpenyangkalan merupakan usaha untuk mencegah penyangkalan. Penyangkalan yang dimaksud bisa pada proses pengiriman maupun penerima pesan.

2. Pesan, *Plaintext*, dan *Chipertext*

Pesan merupakan istilah dalam ilmu kriptografi yang dapat diartikan sebagai data atau informasi yang mudah dimengerti maknanya (Rosnawan, 2011). Pada ilmu kriptografi pesanlebih sering

disebut sebagai *plaintext* (pesan asli). Pada file citra pesan asli biasa disebut *plain-image*, sedangkan citra yang terenkripsi biasa disebut *cipher-image.* Pesan biasanya berupa infomasi yang dikirim menggunakan saluran komunikasi ataupun disimpan dalam bentuk teks, gambar, video, dan lain-lain. Supaya pesan tersebut tidak mudah disalahgunakan oleh pihak yang tidak berwenang, maka pesan tersebut perlu disandikan. Bentuk pesan yang telah disandikan adalah *ciphertext.* Pesan yang telah tersandi (*ciphertext*) harus dapat diubah kembali menjadi pesan asli (*plaintext*).

3. Enkripsi dan Dekripsi

Pada ilmu kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah proses mengubah *plaintext* (pesan asli) menjadi *chipertext* (pesan tersandi). Sedangkan dekripsi merupakan tahapan mengembalikan *ciphertext* (pesan tersandi) menjadi *plaintext* sesuai pesan asli. Pada bidang kriptografi, enkripsi dapat diartikan sebagai sebuah proses mengamankan sebuah informasi dengan cara mengubah informasi tersebut agar tidak mudah dibaca tanpa bantuan pengetahuan/ilmu khusus.

Konsep matematis pada algoritma kriptografi ditunjukkan pada relasi dari dua buah himpunan. Himpunan yang pertama merupakan himpunan yang elemennya *plaintext* dan himpunan kedua merupakan himpunan yang elemennya berisi *chipertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen dari kedua himpunan

tersebut.Misalkan P menyatakan *plaintext* dan C menyatakan *chipertext*, maka fungsi enkripsi E memetakan P ke C,

$$E(P) = C \quad (2.1)$$

Dan fungsi dekripsi D memetakan C ke P,

$$D(C) = P \quad (2.2)$$

Kemudian proses dekripsi mengembalikan pesan ke pesan asal maka persamaannya menjadi :

$$D(E(P)) = P \quad (2.3)$$

4. Macam-macam Algoritma Kriptografi

Berdasarkan kunci yang digunakan algoritma kriptografi dibagi menjadi 3, algoritma simetris, algoritma asimetris, dan fungsi *hash*.

a. Algoritma Simetri

Algoritma simetri atau yang sering disebut algoritma klasik merupakan algoritma yang menggunakan kunci yang sama untuk proses enkripsi maupun dekripsi. Algoritma ini telah ada sejak 4000 tahun yang lalu. Untuk mengirimkan pesan dengan menggunakan algoritma ini, penerima pesan harus mengetahui kunci dari pesan yang akan di terimanya. Keamanan pesan yang menggunakan algoritma asimetri tergantung pada kunci yang ditentukan di awal. Jika kunci yang ditentukan tersebut diketahui oleh orang lain, maka orang itu

dapat melakukan enkripsi dan dekripsi pesan. Algoritma yang menggunakan kunci simetri antara lain:

- RC2, RC4, RC5, RC6
- *Internatonal Data Encryption Algoritihm* (IDEA)
- *Advanced Encryption Standard* (AES)
- *Data Encryption Standard* (DES)
- *One Time Pad* (OTP)

b. Algoritma Asimetri

Algoritma asimetri sering juga disebut algoritma kunci publik. Kunci yang digunakan untuk proses enkripsi berbeda dengan kunci yang digunakan untuk proses dekripsi. Ada dua kunci yang digunakan pada algoritma asimetri, yaitu :

- Kunci Umum (*public key*) : kunci yang dapat diketahui oleh semua orang.
- Kunci Privat (*private key*) : kunci yang hanya diketahui oleh pengirim dan penerima pesan.

Kedua kunci tersebut saling berhubungan satu sama lain. Dengan menggunakan kunci publik pesan dapat dienkripsi, namun jika tidak mengetahui kunci privatnya pesan tidak dapat didekripsi. Konsep penerimaan pesan pada algoritma asimetri adalah dimisalkan ada dua orang pengirim dan penerima pesan, maka si penerima pesan yang membangkitkan kunci dan menyimpan

semua kunci. Ketika ada yang akan mengirim pesan kepada penerima, maka penerima memberikan kunci publik kepada pengirim untuk mengenkripsi pesan. Namun, kunci rahasianya hanya disimpan oleh penerima pesan selaku yang akan membuka pesan dari pengirim. Algoritma asimetri dapat mengirimkan pesan lebih aman daripada algoritma simetri. Contoh algoritma asimetri antara lain:

- RSA
- ElGamal
- *Digital Signature Algorithm* (DSA)
- *Diffle-Hellman* (DH)
- *Eliptic Curve Cryptography* (ECC)

c. Fungsi *Hash*

Fungsi *hash* juga sering disebut fungsi hash satu arah (*One-Way Function*), *message digest*, *fingerprint*, fungsi kompresi, dan *message authentication code* (MAC) merupakan salah satu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi *hash* biasanya digunakan untuk membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda untuk memastikan bahwa pesan tersebut benar-benar terjadi.

C. RSA (*Rivest-Shamir-Adleman*)

Ide awal penemuan algoritma RSA yaitu dari Clifford Cocks yang ditemukan kembali oleh tiga orang peneliti yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Mereka mengumumkan temuannya pada tahun 1976, sebuah algoritma kriptografi kunci asimetri yang dikenal dengan nama algoritma kriptografi RSA. RSA merupakan singkatan dari nama belakang penemunya (Rivest, Shamir, dan Adleman) (Sadikin & Rifki, 2012).

Algoritma RSA adalah salah satu algoritma kriptografi asimetri, yakni jenis kriptografi yang menggunakan dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Dua kunci tersebut antara lain kunci publik (*public key*) dan kunci pribadi (*private key*). Kunci publik merupakan kunci yang dapat dikirimkan melalui saluran bebas, tanpa perlu adanya keamanan tertentu. Hal tersebut berbeda dengan kriptografi simetri yang hanya memiliki satu jenis kunci dan kunci tersebut harus dijaga keamanannya. Algoritma RSA mempunyai dasar konsep untuk proses enkripsi dan dekripsi yaitu bilangan prima dan aritmatika modulo. RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci privat.

Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor-faktor prima dari bilangan yang besar, yang dalam hal ini adalah memfaktorkan n menjadi a dan b. Kemudian sekali n berhasil difaktorkan menjadi a dan b, maka $m = (a-1)(b-1)$dapat dihitung. Selanjutnya karena kunci enkripsi diutamakan e bebas (tidak rahasia),

maka kunci dekripsi d dapat dihitung dari persamaan $e.d = 1\ (mod\ m)$. Hal tersebut merupakan proses dekripsi yang dilakukan oleh orang yang tidak berhak.

1. Parameter Algoritma RSA

Pada algoritma RSA terdapat parameter-parameter yang akan digunakan dalam pengerjaan algoritma ini. Pada parameter tersebut terdapat parameter rahasia dan tidak rahasia, parameter tersebut ditunjukkan pada tabel 2.1,

Tabel 2.1 Parameter RSA

No	Parameter	Sifat
1	p dan q bilangan prima	Rahasia
2	$n = p.q$	Tidak rahasia
3	$\phi(n) = (p-1)(q-1)$	Rahasia
4	e (kunci enkripsi)	Tidak rahasia
5	d (kunci dekripsi)	Rahasia
6	m (*plainteks*)	Rahasia
7	c (*chipertext*)	Tidak rahasia

2. Algoritma Pembangkit Kunci

Sebagai algoritma kriptografi asimetri, perumusan algoritma RSA membutuhkan dua kunci yang berbeda untuk enkripsi dan dekripsi. Berikut langkah pembangkitan kunci algoritma RSA :

a. Bangkitkan dua bilangan prima untuk nilai p dan q

b. Hitung nilai $n = p \times q$ (2.4)

c. Hitung nilai $\phi(n) = (p-1)(q-1)$ (2.5)

d. Pilih nilai bilangan bulat e acak sebagai kunci publik, yang telah memenuhi syarat *Greater Common Divisor* (GCD) $(e, \phi(n)) = 1, 1 < e < \phi(n)$(2.6)

e. Hitung kunci privat d maka $d \times e = 1 \ (mod \phi(n))$

(2.7)

3. Enkripsi dan Dekripsi RSA

Berikut langkah-langkah proses enkripsi dan dekripsi pada algoritma RSA :

a. Ambil kunci publik yang telah dibangkitkan pada proses sebelumnya yaitu (e, n).

b. Untuk proses enkripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.8.

$$c_i = m_i^e mod n \quad (2.8)$$

c. Ambil kunci privat yang telah dibangkitkan pada proses sebelumnya yaitu (d, n).

d. Untuk proses dekripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.9.

$$m_i = c_i^d mod\ n \quad (2.9)$$

dimana :

c = *chipertext*

m = *Plaintext*

e, n = kunci publik

d, n = kunci privat

4. Contoh Perhitungan Algoritma RSA pada Matiks Citra :

Diberikan plainteks berupa matriks citra ukuran 5×5, $\mathrm{M} = \begin{bmatrix} 116 & 116 & 116 & 116 & 116 \\ 116 & 116 & 116 & 116 & 116 \\ 115 & 115 & 115 & 115 & 115 \\ 115 & 115 & 115 & 115 & 115 \\ 115 & 115 & 115 & 115 & 115 \end{bmatrix}$. Maka perhitungan enkripsi dan dekripsi menggunakan algoritma RSA dapat dilihat dibawah ini:

a. Pembangkitan kunci

1. Pada perhitungan ini ditetapkan $\mathrm{p} = 11$ dan $\mathrm{q} = 7$.
2. Lalu menghitung nilai $n = p \times q$dan $\Phi(n) = (p-1)(q-1)$

$$n = p \times q$$
$$= 11 \times 7$$
$$= 77$$
$$\Phi(n) = (p-1)(q-1)$$
$$= (11-1) \times (7-1)$$
$$= 60$$

3. Ambil sembarang nilai e dengan syarat $\mathrm{GCD}(\mathrm{e}, \Phi(\mathrm{n})) = 1$

Misal $\mathrm{e} = 7$, apakah $\mathrm{GCD}(7{,}60) = 1$.

$7 \mod 60 = 7$

$60 \mod 7 = 4$

$7 \mod 4 = 1$

Karena GCD (7, 60) = 1, maka dapat digunakan e = 7

4. Cari nilai $d = e^{-1} mod \Phi(\mathrm{n}) = \frac{1+\mathrm{k}.60}{\mathrm{e}}$

misal $k = 1$, maka d = 8,7

misal $k = 2$, maka d = 17,2

misal $k = 3$, maka d = 25,8

misal $k = 4$, maka d = 34,4

misal $k = 5$, maka d = 43

sehingga didapat nilai d = 43

Setelah didapatkan kunci publik (e,n) = (7, 77) dan kunci privat (d, n) = (43, 77) proses selanjutnya adalah enkripsi dan dekripsi.

b. Enkripsi

Lalu dilanjutkan proses enkripsi menggunakan rumus $c_i = m_i^e mod\ n$. Matriks citra tersebut sebelum diproses menggunakan rumus enkripsi, matriks M diubah menjadi matriks ukuran 1×25, sehingga matriks M menjadi :

[116 116 115 115 115 116 116 115 115 115 116
116 115 115 115 116 116 115 115 115 116 116
115 115 115]

Tiap elemen dari matriks ukuran 1×25 tersebut dihitung menggunakan rumus enkripsi yang terdapat pada Persamaan 2.8, sehingga didapatkan nilai matriks hasil enkripsi

[76 76 3 3 3 76 76 3 3 3 76
76 3 3 3 76 76 3 3 3 76 76
3 3 3]

Hasil dari matriks tersebut diubah menjadi matriks semula sehingga menghasilkan matriks citra *chipertext* :

$$C = \begin{bmatrix} 76 & 76 & 76 & 76 & 76 \\ 76 & 76 & 76 & 76 & 76 \\ 3 & 3 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 \end{bmatrix}.$$

c. Dekripsi

Pada proses dekripsi ini menggunakan rumus $m_i = c_i^d mod\ n$.

Matriks hasil enkripsi tersebut diproses menggunakan rumus dekripsi, setiap elemen dari matriks tersebut sebagai *chiperteks*. Sehingga menghasilkan:

$$D = \begin{bmatrix} 116 & 116 & 116 & 116 & 116 \\ 116 & 116 & 116 & 116 & 116 \\ 115 & 115 & 115 & 115 & 115 \\ 115 & 115 & 115 & 115 & 115 \\ 115 & 115 & 115 & 115 & 115 \end{bmatrix}$$

Hasil dari dekripsi matriks tersebut sesuai dengan matriks aslinya, sehingga proses enkripsi dan dekripsi matriks citra tersebut berhasil.

D. MSE (*Mean Square Error*) dan PSNR (*Peak Signal-to-Noise Ratio*)

MSE (*Mean Square Error*) dan PSNR (*Peak Signal-to-Noise Ratio*) merupakan contoh parameter yang biasa digunakan sebagai indikator dalam mengukur kemiripin dua buah citra (Pamungkas, 2017). Parameter tersebut sering digunakan untuk membandingkan hasil pengolahan citra dengan citra asli. Persamaan yang digunakan untuk menghitung MSE dan PSNR seperti yang ditunjukkan pada Persamaan 2.10 dan 2.11.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n} \sum_{j=0}^{m} [S_{xy} - C_{xy}]^2 \quad (2.10)$$

$$PSNR = 10\ log_{10} \frac{C_{max}^2}{MSE} \quad (2.11)$$

Dimana:

(*m,n)* = dimensi citra

S_{xy} = piksel citra yang telah diolah

C_{xy} = piksel citra asli

Nilai MSE pada umumnya tidak memiliki satuan. Jika nilai MSE hasil pengujian mendekati nilai 0, tingkat kemiripan kedua citra tersebut lebih baik. Sedangkan nilai PSNR dinyatakan dalam satuan decibel (dB). Nilai PSNR yang baik terletak diatas angka 30 dB. Jika nilai PSNR dibawah 30 dB menunjukkan bahwa nilai citra hasil dekripsi masih banyak yang tidak sesuai dengan nilai citra asli.

Dengan demikian semakin kecil nilai MSE menunjukkan bahwa dua buah citra tersebut semakin mirip, begitu pula sebaliknya jika semakin besar nilai MSE menunjukkan perbedaan dari dua buah citra. Pada hasil nilai PSNR semakin kecil nilai PSNR semakin terlihat perbedaan citra asli dan citra hasil pengolahan.

BAB III

METODE PENELITIAN

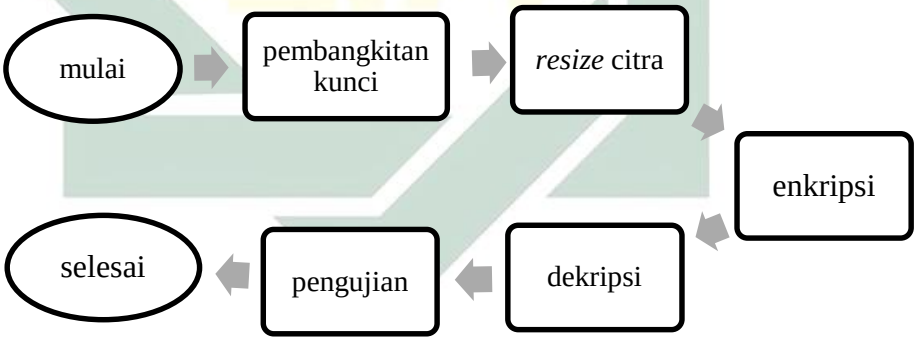
A. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kuantitatif, karena data yang digunakan dalam penelitian merupakan data berupa citra yang kemudian diubah dalam bentuk matriks.

B. Pengumpulan Data

Data citra digital yang digunakan pada penelitian ini merupakan citra digital yang sering digunakan dalam percobaan citra digital. Gambar yang diambil pada laman tersebut sebanyak 5 gambar.

C. Alur Penelitian

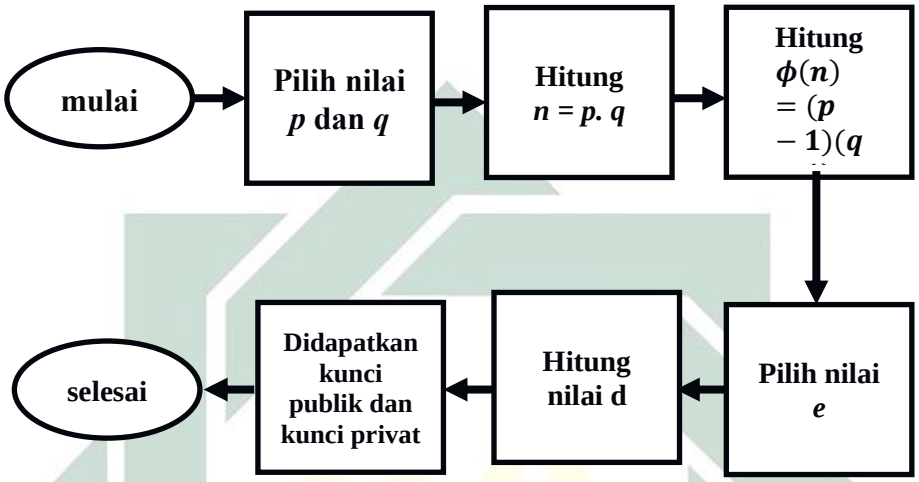


Gambar 3.1. Alur penelitian

Pada Gambar 3.1 menunjukkan alur dari penelitian penerapan algoritma RSA untuk enkripsi dan dekripsi yang dimulai dengan menentukan variabel RSA. Selanjutnya adalah membangkitkan kunci RSA yang nantinya akan menghasilkan kunci publik dan kunci privat. Lalu langkah selanjutnya adalah dengan melakukan enkripsi pada pesan yang ingin

disampaikan dan setelah itu melakukan dekripsi pada pesan. Untuk alur dari masing-masing proses akan dijelaskan pada subbab berikut

1. Pembangkitan Kunci RSA



Gambar 3.2 Pembentukkan Kunci RSA

Sebagai algoritma kriptografi asimetris, perumusan algoritma RSA membutuhkan dua kunci yang berbeda untuk enkripsi dan dekripsi. Bilangan yang dipilih sebagai kunci adalah bilangan prima yang besar dikarenakan pemfaktoran bilangan hasil perkalian dari dua bilangan prima yang besar menjadi dua bilangan prima yang sesuai akan sangat sulit. Oleh karena itu keamanan dari RSA dapat terjamin. Setelah menghitung perkalian antar dua bilangan prima tersebut, langkah selanjutnya adalah menghitung nilai $\phi(n)$dimana $\phi(n) = (p - 1)(q - 1)$ dan setelah itu memilih sebarang nilai e yang sesuai dengan syaratnya yaitu 1 <e<$\phi(n)$, dengan gcd(e, $\phi(n)$) = 1. Selanjutnya adalah menghitung nilai d, dimana $de = 1 \ (mod \phi(n)$. Nilai d yang telah dihitung akan digunakan sebagai

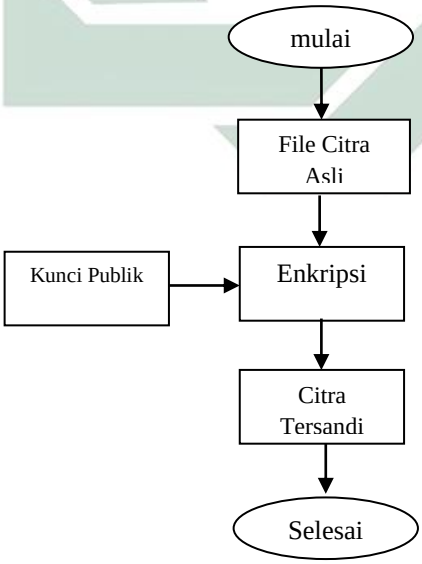
kunci privat. Sehingga didapatkan kunci publik (*e,n*) yang digunakan untuk enkripsi dan kunci publik (*d,n*) yang digunakan untuk dekripsi.

2. *Resize* Citra

Pada tahap ini merupakan proses mengubah ukuran citra yang diinputkan menjadi ukuran 256×256 *pixel*. Pada penelitian ini, untuk mengubah ukuran citra menjadi 256×256 *pixel* digunakan *function* pada matlab yaitu "imresize (namavariabel, [256 256])". Nama variabel disini merupakan varibel yang menyimpan nilai piksel citra.

3. Enkripsi

Dari tahap sebelumnya yaitu tahap pembentukan kunci yang direpresantasikan pada Gambar 3.2 diperoleh variabel – variabel diantaranya (*e,n*) yang merupakan kunci publik pada algoritma ini. Alur dari proses enkripsi ditunjukkan pada Gambar 3.3

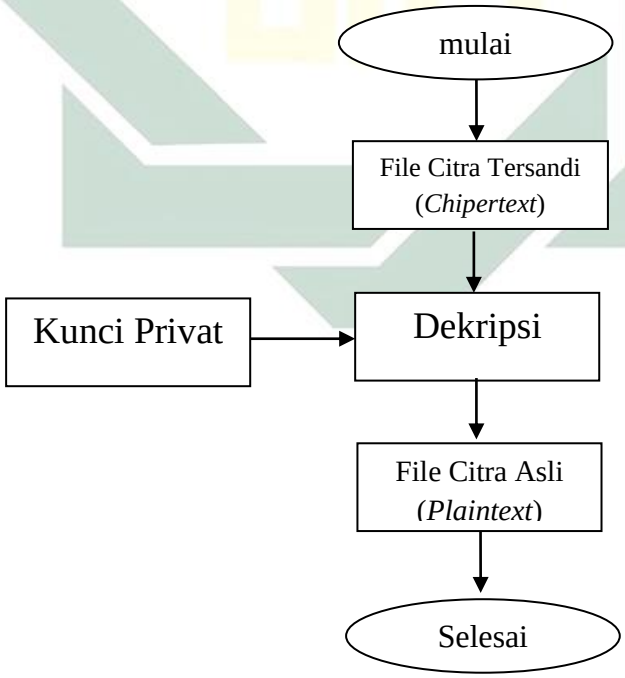


Gambar 3.3 Alur Enkripsi Algoritma RSA

Pada tahap ini file citra akan mulai dienkripsi kemudian didapatkan file citra yang tersandi. Untuk proses enkripsi digunakan persamaan $C = M^e mod n$, dimana C merupakan *chipertext*, M merupakan *plaintext* yang dalam kasus ini berupa file citra, dan (e, n) merupakan kunci publik.

4. Dekripsi

Dari proses pembentukan kunci RSA yang direpresentasikan oleh gambar 3.2 diperoleh kunci publik dan kunci rahasia. Setelah kunci rahasia $(d,\ n)$ dipersiapkan maka langkah selanjutnya adalah memasukkan file citra yang tersandi untuk diproses ke tahap dekripsi. Rumus yang digunakan untuk proses dekripsiadalah persamaan $m_i = c_i^d mod\ n$.Hasil pada tahap akan didapatkan file citra semula. Alur pada proses dekripsi ditunjukkan pada Gambar 3.4



Gambar 3.4 Alur proses deskripsi

5. Pengujian

Pengujian Algoritma RSA pada penelitian ini dibagi menjadi 3, yaitu pengujiian pembangkitan kunci, pengujian hasil dekripsi terhadap *enhancement*, cropping, dan blurring, dan pengujian nilai MSE dan PSNR citra asli dengan citra hasil enkripsi dekripsi.

a. Pengujian Pembangkitan Kunci RSA

Pada tahap akan dicoba kunci dengan nilai kecil dan kunci dengan nilai yang besar. Kunci dengan nilai kecil tersebut mulai rentang 2 sampai 97. Kunci dengan nilai besar tersebut mulai rentang 97 sampai 997. Dari hasil tersebut akan dianalisis hasil enkripsi mana yang lebih bagus. Untuk menilai bagus tidaknya enkripsi akan dilihat dari histogram hasil enkripsi. Hasil histogram yang baik dapat dilihat jika hasilnya relatif datar.

b. Pengujian terhadap Enhancement, Cropping, dan Blurring

Pada tahap ini citra yang telah berhasil dienkripsi akan diuji menggunakan *enhancement*, cropping, dan blurring.

1. *Enchancement* (Penajaman)

   Pengujian ini dilakukan dengan cara menajamkan gambar hasil enkripsi. Gambar hasil enkripsi yang telah ditajamkan akan didekripsi kembali menggunakan kunci yang sama. Jika gambar yang telah ditajamkan warnanya dapat kembali ke gambar semula maka pengujiannya berhasil.

2. Cropping (Pemotongan)

Pengujian ini dilakukan dengan cara memotong sebagian gambar hasil enkripsi. Gambar hasil enkripsi yang telah dipotong akan didekripsi kembali menggunakan kunci yang sama. Jika gambar yang telah dipotong dapat kembali ke gambar semula maka pengujiannya berhasil.

3. Blurring (Penyamaran)

Pengujian ini dilakukan dengan cara menyamarkan gambar hasil enkripsi. Gambar hasil enkripsi yang telah disamarkan akan didekripsi kembali menggunakan kunci yang sama. Jika gambar yang telah disamarkan warnanya dapat kembali ke gambar semula maka pengujiannya berhasil.

c. Pengujian Nilai MSE dan PSNR

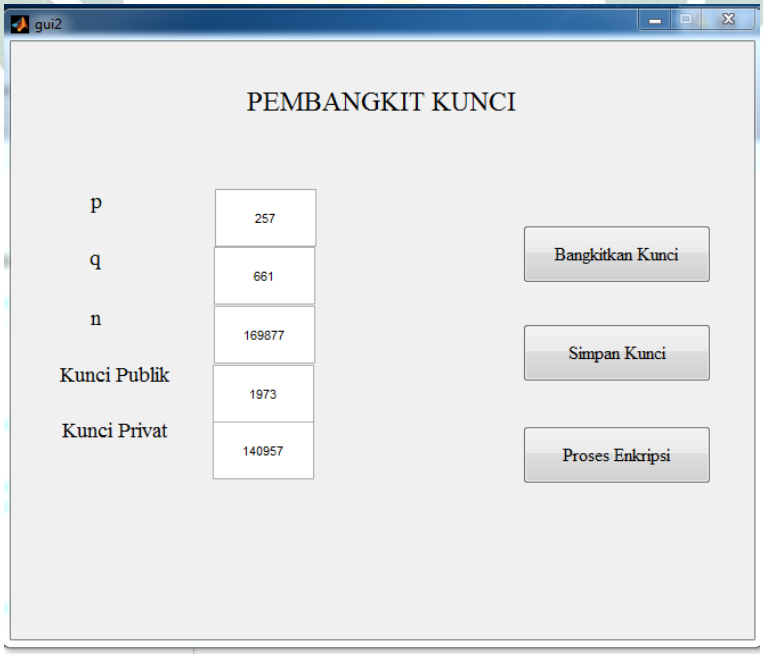
Pada tahap ini akan menguji kemiripan citra asli dengan citra hasil enkripsi dekripsi. Pada pengujian citra asli dengan hasil enkrisi akan diuji ketidakmiripannya, sedangkan untuk citra asli dengan hasil dekripsi akan diuji kemiripannya. Nilai MSE dari 2 citra yang memiliki kemiripan harusnya tidak jauh dari angka 0, untuk nilai PSNR yang baik untuk kemiripan dua citra adalah diatas 30 dB. Jadi, pada penelitian ini jika nilai MSE mendekati 0 dan PSNRnya >30dB maka dua citra tersebut memliki kemiripan. Begitu pula sebaliknya jika nilai MSE jauh dari angka 0 dan nilai PSNR<30 dB maka dua citra yang diuji tidak memiliki kemiripan.

BAB IV

HASIL DAN PEMBAHASAN

A. Pembangkitan Kunci

Tahap ini merupakan tahap pembentukan kunci yang akan digunakan dalam algoritma RSA. Kunci tersebut terdiri dari kunci publik dan kunci privat. Kunci publik yang dimaksud adalah (e,n) dan Kunci privatnya (d,n). Dalam pembangkitan kunci ini nilai p, q terlebih dulu dibangkitkan, dengan cara merandom nilai prima yang kemudian digunakan untuk nilai n, $\Phi(n)$, menggunakan rumus yang ada telah dijelaskan di Bab II. Setelah di dapatkan nilai n, $\Phi(n)$, nilai tersebut digunakan untuk mendapatkan nilai e dan d. Pada Gambar 4.1 menunjukkan tampilan GUI matlab.



Gambar 4.1 Tampilan Pembangkit Kunci

Pada pembentukkan kunci ini, nilai p dan q yang dibangkitkan adalah bilangan prima dengan rentang 2 – 997. Semakin besar nilai kunci yang dihasilkan, akan semakin bagus hasil enkripsinya.

Pada penelitian ini, dalam satu kali pembangkitan kunci digunakan untuk mengenkripsi dan dekripsi satu citra. Sehingga dalam penelitian ini didapatkan lima pasang kunci publik dan kunci privat.

B. *Imresize* Citra

Pada tahap ini akan dilakukan perubahan citra menjadi ukuran 256×256 piksel. Setiap citra yang ukurannya kurang atau lebih dari 256×256 akan diubah menjadi ukuran 256×256 piksel. Pada penelitian ini menggunakan fungsi matlab "imresize (namavariabel,[256 256])". Dimana nama variabel merupakan variabel yang menyimpan nilai piksel citra. Berikut adalah *source code* untuk proses *imresize* citra:

```
mm = imresize (m0,[256 256])
```

C. Enkripsi dan Dekripsi Citra

Pada tahap ini dilakukan enkripsi untuk gambar yang di inputkan. Gambar yang diinputkan dalam proses ini sebanyak 5 gambar. Sebelum proses enkripsi, terlebih dahulu menginputkan *plaintext* berupa gambar dalam format .jpg dengan ukuran $256 \times 256\, pixel$, kemudian gambar tersebut diubah menjadi citra *grayscale* (keabuan). Fungsi pada matlab yang digunakan untuk mengubah citra berwarna menjadi citra keabuan adalah "g = rgb2gray(I);", dimana I merupakan variabel yang menyimpan citra berwarna. Contoh inputan citra yang telah diubah menjadi *grayscale* ditunjukkan pada Gambar 4.2.

Gambar 4.2 Gambar Input

Berdasarkan citra yang diinputkan didapatkan matriks berukuran 256×256 yang tersimpan pada variabel *g* sebagai berikut :

$$g = \begin{bmatrix} 56 & 56 & \cdots & 43 & 47 \\ 57 & 58 & \cdots & 44 & 46 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 60 & 65 & \cdots & 63 & 66 \\ 78 & 68 & \cdots & 63 & 65 \end{bmatrix}$$

Dengan menggunakan fungsi matlab "*reshape*" yang digunakan untuk mengubah matriks asal 256×256 menjadi bentuk vektor baris berukuran $1 \times [256 \times 256]$ atau (1, 65536), *source code reshape* adalah sebagai berikut :

"`m = reshape (g,1,65536).`" Sehingga menghasilkan matrik *reshape* sebagai berikut:

$$re = [56 \quad 57 \quad \cdots \quad \cdots \quad \cdots \quad 66 \quad 65]$$

Fungsi *reshape* ini digunakan dengan tujuan mempermudah dalam proses perhitungan enkripsi algoritma RSA. Karena, pada proses perhitungan RSA matriks yang akan diproses untuk enkripsi berupa vektor baris. Selanjutnya, dilakukan proses enkripsi dengan menggunakan

Persamaan 2.8 pada Bab II, dimana setiap elemen pada matriks yang telah di *reshape* merupakan plainteks. Sehingga matriks hasil enkripsi sebagai berikut :

$$Ie = [10046 \quad 3011 \quad \cdots \quad \cdots \quad \cdots \quad 2215 \quad 1455]$$

Untuk mengembalikan hasil matriks enkripsi ke dalam bentuk matriks persegi ukuran 256×256, akan digunakan fungsi *reshape*. Sehingga matriks citra enkripsi sebagai berikut:

$$e = \begin{bmatrix} 10046 & \cdots & 458 & 15873 \\ 3011 & \cdots & 16960 & 3818 \\ \vdots & \ddots & \vdots & \vdots \\ 1158 & \cdots & 13166 & 2215 \\ 11405 & \cdots & 13166 & 14557 \end{bmatrix}$$

Matriks hasil enkripsi tersebut berupa citra enkripsi yang terlihat pada GUI matlab ditunjukkan pada Gambar 4.3

Gambar 4.3 Proses Enkripsi Citra

Pada Gambar 4.3 hasil proses enkripsi terletak di sebelah kanan, sedangkan yang sebelah kiri merupakan citra asli. Pada gambar terlihat

perbedaan gambar asli dengan gambar yang telah terenkripsi. Langkah selanjutnya adalah dekripsi pesan.

Tahap dekripsi merupakan tahap akhir dalam algoritma RSA, yaitu tahap mengembalikan citra yang telah dienkripsi kembali ke citra semula. Pada tahap ini akan mengubah matriks enkripsi menjadi matriks citra semula. Langkahnya pun hampir sama dengan proses enkripsi, hanya saja persamaan yang digunakan berbeda. Pada proses dekripsi ini digunakan kembali matriks hasil enkripsi (*chipertext*) berikut :

$$Ie = [10046 \quad 3011 \quad \cdots \quad \cdots \quad \cdots \quad 2215 \quad 1455]$$

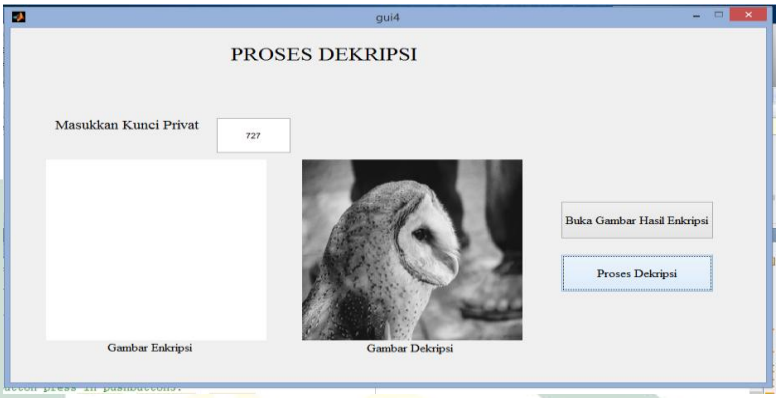
Matriks vektor hasil enkripsi tersebut dihitung menggunakan Persamaan 2.9 yang ada pada Bab II, dimana setiap elemen dari matrik Ie merupakan *chipertext*. Pada perhitungan dekripsi mengahasilkan matriks vektor hasil dekripsi berikut :

$$Id = [56 \quad 57 \quad \cdots \quad \cdots \quad \cdots \quad 66 \quad 65]$$

Untuk mengetahui hasil citra dekripsi, matriks vektor hasil dekripsi harus diubah kembali menjadi matriks persegi ukuran 256×256 menggunakan fungsi *reshape*, sehingga menghasilkan matriks citra dekripsi berikut :

$$d = \begin{bmatrix} 56 & 56 & \cdots & 43 & 47 \\ 57 & 58 & \cdots & 44 & 46 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 60 & 65 & \cdots & 63 & 66 \\ 78 & 68 & \cdots & 63 & 65 \end{bmatrix}$$

Matriks dekripsi tersebut berupa citra dekripsi yang ditunjukkan pada gambar 4.4. Pada gambar tersebut menunjukkan bahwa citra hasil dekripsi sama dengan citra asli yang di inputkan. Hal tersebut juga terlihat matriks dekripsi yang sama dengan matriks citra yang dinputkan.



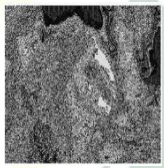
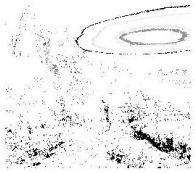
Gambar 4.4 Hasil Dekripsi Algoritma RSA

Dari hasil pada Gambar 4.4 menunjukkan bahwa pada gambar sebelah kiri adalah hasil enkripsi yang telah di dapat dari proses sebelumnya. Dari gambar tersebut terlihat bahwa gambar yang sebelah kanan sama dengan Gambar 4.2 yang merupakan gambar input. Hal tersebut berarti hasil dari algoritma RSA pada penelitian ini mampu mengembalikan gambar yang telah dienkripsi dapat kembali ke gambar semula. Namun, ketika kita salah memasukkan kunci privat pada proses dekripsi, citra terenkripsi tidak dapat kembali ke citra semula.

Dari hasil rancangan sistem keamaan gambar yang dibuat, diperoleh hasil gambar yang dienkripsi dan dekripsi dapat kembali ke gambar semula sesuai dengan yang diinputkan. Namun ada beberapa gambar yang kembali ke gambar semula, namun tidak sempurna. Hal

tersebut disebabkan perbedaan kunci yang digunakan. Hasil enkripsi dan dekripsi algoritma RSA ditunjukkan pada Tabel 4.1.

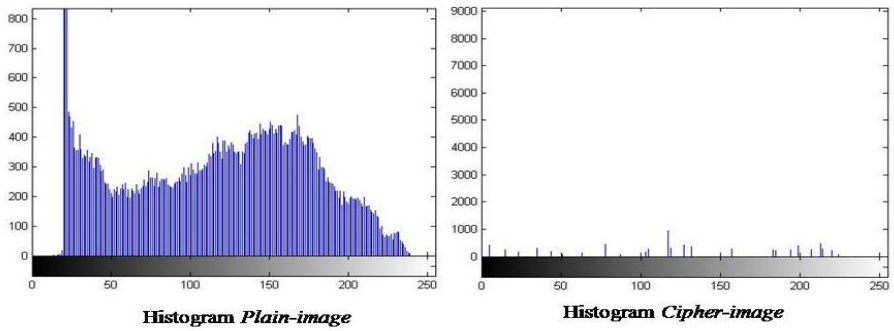
Tabel 4.1 Hasil Enkripsi dan Dekripsi

No	Gambar Asli	Kunci yang Digunakan	Citra Enkripsi	Citra Dekripsi
1	 (Gambar 1)	Kunci Publik (29663, 193909) Kunci Privat (55547, 193909)		
2	 (Gambar 2)	Kunci Publik (4547, 38579) Kunci Privat (20507, 38579)		
3	 (Gambar 3)	Kunci Publik (1973, 169877) Kunci Privat (140957, 169877)		
4	 (Gambar 4)	Kunci Publik (40063, 65623) Kunci Privat (54159, 65623)		
5	 (Gambar 5)	Kunci Publik (1831, 4757) Kunci Privat (2011, 4757)		

Dari Tabel 4.1 menunjukkan citra yang terenkripsi memiliki perbedaan secara signifikan dengan citra aslinya. Namun dari setiap citra memiliki perbedaan bintik hitam pada citra yang terenkripsi, hal itu

disebabkan perbedaan nilai kunci yang digunakan. Semakin besar kunci yang digunakan, akan semakin sedikit bintik hitam pada citra terenkripsi. Untuk citra hasil dekripsi secara kasat mata terlihat sama dengan citra asli. Hal itu menunjukkan algoritma RSA ini dapat mendekripsi gambar dengan baik.

Hasil enkripsi dan dekripsi algoritma RSA ini dapat pula ditunjukkan dari analisis histogram citra asli dan histogram citra yang telah dienkripsi. Seharusnya histogram *plain-image* dan histogram *cipher-image* memliki perbedaan secara signifikan atau secara statistik tidak ada kemiripan (Prawira & Sutojo, 2014). Oleh karena itu, histogram *cipher-image* seharusnya datar atau secara statistik distibusinya seragam. Distribusi yang relatif seragam pada *chiper-image* adalah sebuah indikasi bahwa algoritma enkripsi citra memiliki tingkat keamanan yang bagus. Pada penelitian ini untuk mengetahui histogram citra asli dan citra terenkripsi digunakan fungsi pada matlab yaitu “imhist(I)”, dimana I merupakan variabel yang menyimpan piksel citra yang akan ditunjukkan histogramnya. Histogram citra sebelum dienkripsi dan yang telah dienkripsi ditunjukkan pada Gambar 4.5. Pada Gambar tersebut menunjukkan bahwa histogram *plain-image* dan *cipher-image* berbeda secara signifikan. Serta terlihat bahwa histogram *cipher-image*nya datar atau distribusi statistikanya seragam. Dari hasil histogram dapat disimpulkan bahwa algoritma RSA cukup aman digunakan untuk enkripsi.



Gambar 4.5 Histogram Citra Asli dan Citra Enkripsi

D. Pengujian

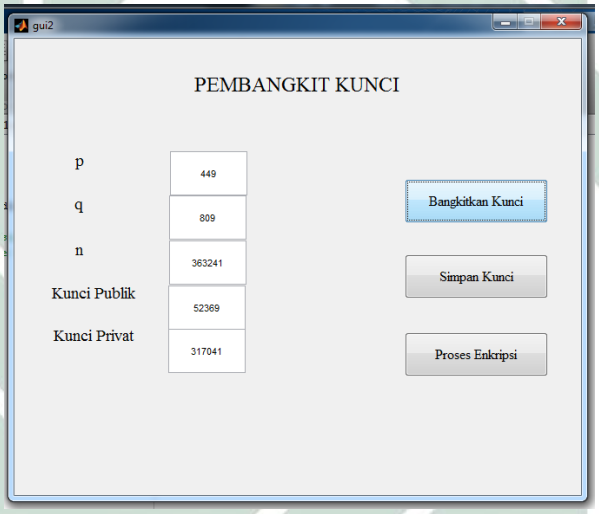
Pada tahap pengujian ini akan dilakukan pengujian kunci, pengujian citra terenkripsi terhadap *enhancement, croping,* dan *bluring,* dan juga pengujian nilai MSE dan PSNR citra asli dengan citra hasil enkripsi dekripsi.

1. Pengujian Kunci

Pengujian kunci yang dilakukan dalam penelitian ini adalah menguji besar kecilnya kunci yang dibangkitkan. Dalam pengujian ini pembangkit kunci dibagi menjadi dua, yaitu kunci nilai p dan q dengan rentang 2 – 97 dan 97 – 997. Hasil kunci yang didapatkan untuk kedua rentang tersebut ditunjukkan pada Gambar 4.6 dan 4.7.

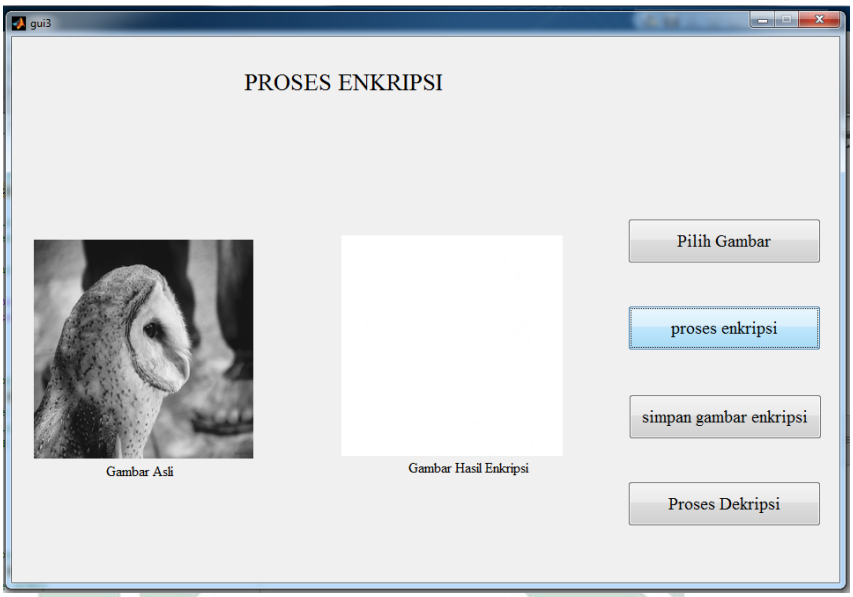
Dari hasil pembangkitan kunci tersebut digunakan untuk mengenkripsi gambar yang sama dengan kunci yang berbeda. Hasil enkripsi dari dua kunci yang telah dibangkitkan akan ditunjukkan pada Gambar 4.8 dan 4.9.

Gambar 4.6 Pembangkitan Kunci Rentang 2 – 97



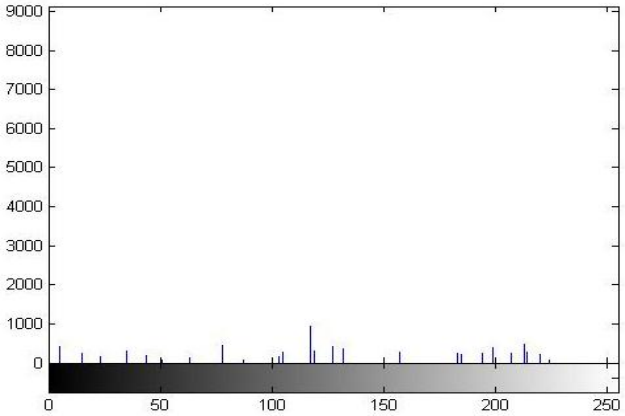
Gambar 4.7 Pembangkitan Kunci Rentang 97 – 997

Gambar 4.8 Hasil Enkripsi Kunci Rentang 2 – 97

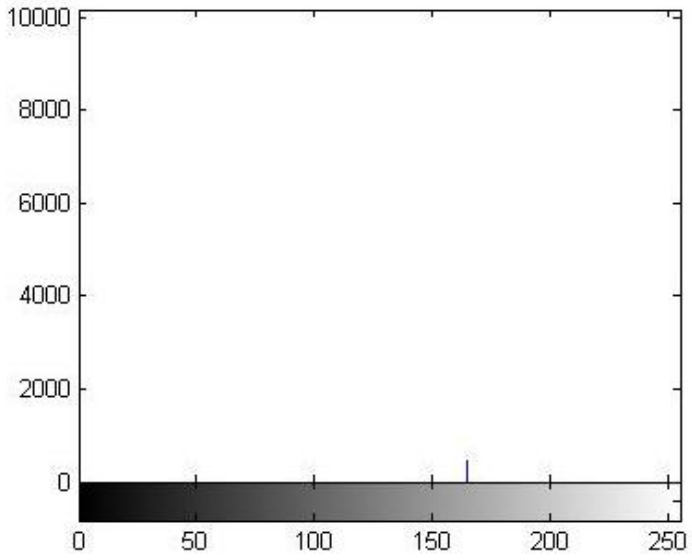


Gambar 4.9 Hasil Enkripsi Kunci Rentang 97 – 997

Dari hasil enkripsi kedua citra dengan rentang kunci yang berbeda, dapat dilihat bahwa hasil enkripsi yang menggunakan kunci lebih besar lebih berbeda dengan gambar aslinya. Hal tersebut menunjukkan bahwa citra enkripsi dengan menggunakan kunci yang lebih besar lebih sulit untuk ditebak. Perbedaan hasil enkripsi dapat pula dilihat dari histogram kedua citra tersebut. Histogram dari hasil enkripsi kedua citra dengan kunci yang berbeda dapat ditunjukkan pada Gambar 4.10 dan 4.11



Gambar 4.10 Histogram Citra Enkripsi dengan Kunci Rentang 2 – 97



Gambar 4.11 Histogram Citra Enkripsi dengan Kunci Rentang 97 – 997

Dari hasil histogram tersebut menunjukkan kedua citra hampir tidak memiliki perbedaan. Namun keduanya sama-sama memiliki grafik yang datar. Hal tersebut menunjukkan bahwa citra yang dienkripsi menggunakan kunci kecil dan kunci besar sama-sama memiliki distribusi yang seragam. Jadi hasil keduanya sama-sama bagus digunakan untuk enkripsi.

Pada pengujian kunci tersebut juga diperhitungkan lama waktu enkripsinya. Pada proses yang menggunakan kunci dengan rentang 2 – 97 waktu yang diperlukan 16,87 detik. Sedangkan waktu untuk proses yang menggunakan kunci dengan rentang 97 – 997 memerlukan waktu 16,97 detik.

2. Pengujian Citra

Pada tahap ini citra yang telah dienkripsi akan di uji menggunakan *enhancement, cropping,* dan *blurring.* Seperti yang dijelaskan pada bab sebelumnya, gambar yang telah enkripsi akan diuji menggunakan penajaman, pemotongan, dan penyamaran. Hasil matriks enkripsi sebelum di uji menggunakan penajaman, pemotongan adalah sebagai berikut:

$$e = \begin{bmatrix} 10046 & \cdots & 458 & 15873 \\ 3011 & \cdots & 16960 & 3818 \\ \vdots & \ddots & \vdots & \vdots \\ 1158 & \cdots & 13166 & 2215 \\ 11405 & \cdots & 13166 & 14557 \end{bmatrix}$$

Penajaman dan penyamaran pada proses ini dilakukan menggunakan aplikasi *picArt*. Setelah dilakukan penajaman menggunakan aplikasi *picArt* maka matriks enkripsi berubah menjadi :

$$en = \begin{bmatrix} 255 & \cdots & 255 & 255 \\ 255 & \cdots & 254 & 255 \\ \vdots & \ddots & \vdots & \vdots \\ 255 & \cdots & 255 & 255 \\ 255 & \cdots & 254 & 255 \end{bmatrix}$$

Sedangkan matriks enkripsi setelah disamarkan adalah sebagai berikut:

$$bl = \begin{bmatrix} 255 & \cdots & 255 & 255 \\ 255 & \cdots & 254 & 255 \\ \vdots & \ddots & \vdots & \vdots \\ 188 & \cdots & 255 & 255 \\ 188 & \cdots & 254 & 255 \end{bmatrix}$$

Pada proses pemotongan gambar menggunakan fungsi pada matlab yaitu: “crop = imcrop (mn,[116 115 130 120])”, dimana [116, 115] merupakan koordinat (x,y) tepat awal pemotongan, dan [130, 120] merupakan

ketebalan dan ketinggian dari proses *cropping.* Hasil matriks enkripsi yang telah dipotong adalah sebagai berikut :

$$cr = \begin{bmatrix} 5509 & \cdots & 10562 & 10562 \\ 5509 & \cdots & 18817 & 18817 \\ \vdots & \ddots & \vdots & \vdots \\ 3911 & \cdots & 17044 & 17044 \\ 3358 & \cdots & 2849 & 15499 \end{bmatrix}$$

Matriks enkripsi yang telah ditajamkan, disamarkan, dan dipotong tersebut didekripsi menggunakan Persamaan 2.9 yang terdapat di Bab II, sehingga menghasilkan matriks hasil dekripsi sebagai berikut :

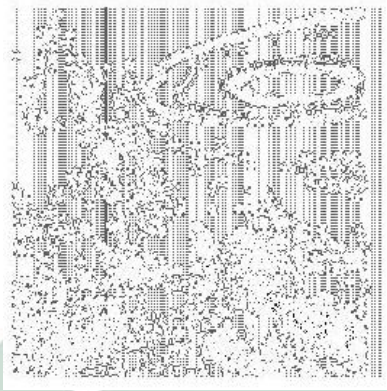
$$hasil\ dekripsi\ enhancement = \begin{bmatrix} 255 & \cdots & 255 & 255 \\ 255 & \cdots & 94 & 255 \\ \vdots & \ddots & \vdots & \vdots \\ 255 & \cdots & 255 & 255 \\ 255 & \cdots & 94 & 255 \end{bmatrix}$$

$$hasil\ dekripsi\ bluring = \begin{bmatrix} 255 & \cdots & 255 & 255 \\ 255 & \cdots & 94 & 255 \\ \vdots & \ddots & \vdots & \vdots \\ 255 & \cdots & 255 & 255 \\ 255 & \cdots & 94 & 94 \end{bmatrix}$$

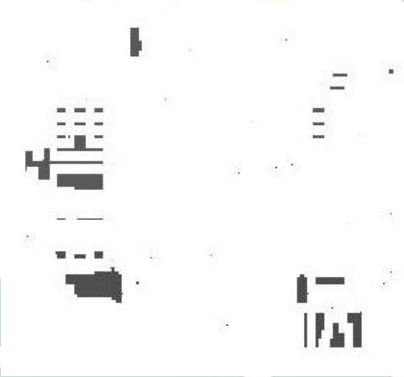
$$hasil\ dekripsi\ croping = \begin{bmatrix} 4928 & \cdots & 9947 & 9963 \\ 5003 & \cdots & 11546 & 11521 \\ \vdots & \ddots & \vdots & \vdots \\ 4097 & \cdots & 13325 & 1647 \\ 2996 & \cdots & 12355 & 1633 \end{bmatrix}$$

Berdasarkan hasil pengujian tersebut menunjukkan bahwa hasil pengujian terhadap *enhancement, cropping*, dan *blurring* citra yang telah dienkripsi tidak dapat sesuai dengan matriks dekripsi dari citra asli. Hasil dekripsi

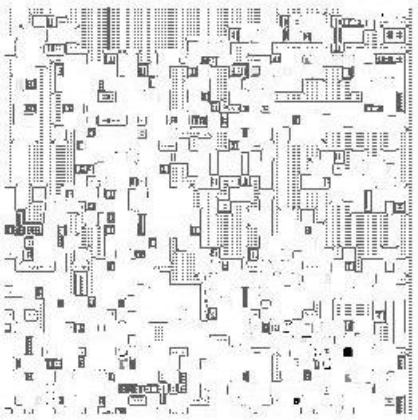
citra enkripsi yang telah diuji terhadap *enhancement*, *cropping*, dan *bluring* ditunjukkan pada Gambar 4.12 – Gambar 4.14.



Gambar 4.12 Hasil Dekripsi Citra Enkripsi *Enhancement*



Gambar 4.13 Hasil Dekripsi Citra Enkripsi *Cropping*



Gambar 4.14 Hasil Dekripsi Citra Enkripsi *Bluring*

3. Pengujian Nilai MSE dan PSNR

Pengujian enkripsi dan dekripsi ini dapat pula dilihat dari menghitung nilai MSE dan PSNR antara citra asli dengan citra hasil dekripsi, serta citra asli dengan *cipher-image.* Nilai MSE dan PSNR ini akan digunakan untuk mengetahui persamaan citra asli dengan citra hasil dekripsi dan juga perbedaan citra asli dengan *cipher-image*. Semakin kecil nilai MSE akan menunjukkan bahwa kedua citra tersebut mirip, begitu pula sebaliknya begitu besar nilai MSE menunjukkan besarnya kedua gambar tersebut (Prawira & Sutojo, 2014). Untuk nilai PSNR memiliki satuan decibel (dB). Nilai PSNR yang baik adalah di atas 30dB. Jika nilai PSNR ≥ 30, menunjukkan kedua citra memiliki kemiripan yang baik. Sebaliknya jika nilai PSNR < 30 menunjukkan bahwa kedua citra jauh berbeda. Hasil MSE dan PSNR antara citra asli dengan citra hasil enkripsi dekripsi ditunjukkan pada Tabel 4.3 dan 4.4

Tabel 4.2 Nilai MSE dan PSNR antara Citra Asli dan Citra Hasil Enkripsi

No	Nama Gambar	Nilai MSE	Nilai PSNR
1	Gambar 1	$1{,}1122e+10$	$-52,3310$
2	Gambar 2	$1{,}3415e+11$	$-63,1452$
3	Gambar 3	$2,9227e+06$	$-16,5271$
4	Gambar 4	$5{,}5673e+10$	$-59,3257$
5	Gambar 5	$1{,}1979e+04$	$7,3466$

Pada Tabel 4.3 menunjukkan bahwa nilai MSE relatif besar, hal tersebut menunjukkan bahwa citra asli dan citra hasil enkripsi memiliki

perbedaan yang signifikan. Jika dilihat dari nilai PSNRnya rata-rata nilainya kurang dari 30 sehingga dapat disimpulkan bahwa citra asli dengan citra hasil enkripsi memiliki perbedaan yang signifikan.

Tabel 4.3 Nilai MSE dan PSNR antara Citra Asli dan Citra Hasil Dekripsi

No	Nama Gambar	Nilai MSE	Nilai PSNR
1	Gambar 1	*0*	Inf
2	Gambar 2	0,*3374*	5*2,8838*
3	Gambar 3	0,3411	52, 8355
4	Gambar 4	0,*3332*	5*2,9383*
5	Gambar 5	7,*5892*	39, 0520

Pada Tabel 4.4 menunjukkan bahwa nilai MSE dari pengujian citra asli dengan citra hasil dekripsi relatif mendekati 0, hal itu berarti citra asli dan citra hasil dekripsi memiliki kemiripan yang cukup bagus. Bahkan ada satu gambar yang memiliki nilai MSE 0, dan PSNR Inf, hal tersebut menunjukkan bahwa citra asli dan citra dekripsi memiliki kemiripan 100%. Namun, tidak semua gambar memiliki nilai MSE mendekati 0. Hal itu disebabkan saat proses dekripsi ada beberapa nilai citra yang tidak bisa kembali ke nilai yang sesuai dengan citra asli.

Untuk nilai PSNR pada pengujian citra asli dan citra hasil dekripsi menunjukkan angka diatas 30 dB, hal itu berarti kualitas kemiripannya dapat dikatakan bagus.

BAB V

PENUTUP

A. Simpulan

Berdasarkan hasil pembahasan dan evaluasi dari bab-bab terdahulu, dapat ditarik kesimpulan sebagai berikut :

1. Pembangkitan kunci pada algoritma RSA menggunakan nilai *p* dan *q* yang dibangkitkan dari random bilangan prima. Sehingga didapatkan kunci publik dan kunci privat yang digunakan untuk enkripsi dan dekripsi. Semakin besar nilai kunci publik dan kunci privat akan menghasilkan enkripsi yang lebih bagus. Namun, kunci dengan nilai lebih besar diperlukan waktu sedikit lebih lama untuk proses enkripsi dan dekripsi citra.
2. Hasil enkripsi dan dekripsi algoritma RSA pada penelitian ini mampu menyamarkan citra saat proses enkripsi. Serta dapat mengembalikan ke citra semula pada proses dekripsi. Hal ini dapat dilihat pula dari histogram citra terenkripsi memiliki distribusi yang seragam.
3. Hasil nilai MSE citra asli dengan citra enkripsi jauh dari angka 0, hal tersebut menunjukkan bahwa tidak ada kemiripan antara citra asli dengan citra hasil enkripsi. Untuk pengujian MSE antara citra asli dengan citra hasil dekripsi nilainya mendekati 0, namun tidak 100% mirip. Hal itu disebabkan ketika proses dekripsi ada beberapa nilai *pixel* citra yang tidak kembali sesuai nilai semula.

B. Saran

Berdasarkan hasil yang telah didapatkan dalam penelitian ini, maka penulis dapat menyarankan beberapa saran untuk penelitian selanjutnya. Saran tersebut antara lain:

1. Algoritma RSA ini dapat digunakan untuk file citra dengan jenis yang lain ataupun juga ukuran yang berbeda.
2. Untuk penelitian selanjutnya bisa tambahkan metode lainnya untuk mempercepat proses dekripsi, misalnya metode Chinese Remainder Theorem ataupun metode lainnya.

DAFTAR PUSTAKA

Arifani, Y. D. (2016). Enkripsi dan Dekripsi Kriptografi Metode RSA.

Ariyus, D. (2006). *Kriptografi* . Yogyakarta: Graha Ilmu.

Ashari Arief, R. S. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics* .

Gumelar, A. (2017). *Pengamanan File Citra Dengan Skema Hybrid Cryptosystem Menggunakan RSA - CRT* . Medan: Universitas Sumatera Utara.

Iriyanto, S., & Zaini, T. (2014). *Pengolahan Citra Digital*. Bandar Lampung: Anugrah Utama Raharja (AURA).

Kromodimoeljo, S. (2009). *Teori & Aplikasi Kriptografi.* SPK IT Consulting.

Munir, R. (2012). Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif. *JUTI* , 89-95.

Munir, R. (2006). *Kriptografi*. Bandung: Informatika.

Pahrizal, & Pratama, D. (2016). Implementasi Algortima RSA Untuk Pengamanan Data Berbentuk Teks. *Pseucode Volume III No.1* .

Pamungkas, A. (2017, 06 04). *Cara Menghitung Nilai MSE, RSME, dan PSNR pada Citra Digital*. Diambil kembali dari Pemograman Matlab: https://pemrogramanmatlab.com/2017/06/04/cara-menghitung-nilai-mse-rmse-dan-psnr-pada-citra-digital/amp/#referrer=https://www.google.com&amp_tf=Dari%20%251%24s

Prawira, A. Y., & Sutojo, T. (2014). Implementasi Algoritma RC4 dan Cipher Block Chaninig (CBC) Pada Pengamanan Gambar.

Rahmawati, W. I. (2014). Analisis Perolehan Kecepatan Operasi Enkripsi/Dekripsi RSA. *ISSN: 1979-911X* .

Rakhman, A. A., & Kurniawan, A. W. (2015). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) dan Vigenere Chiper Pada Gambar Bitmap 8 Bit. *Techno.COM Vol 14 No.2* , 122-134.

Rosnawan, D. (2011). *Aplikasi Algoritma RSA untuk Keamanan Data Pada Sistem Informasi Berbasis Web.* Semarang: Universitas Negeri Semarang.

Sadikin, & Rifki. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: ANDI.

Sukaesih, & Wahyuni, S. (2016). Penerapan Algoritma Kriptografi Rives Shamir Adleman (RSA) pada Sebuah Image. *Jurnal Informatika SIMANTIK* , 32-39.