IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) DAN VIGENERE CIPHER PADA GAMBAR BITMAP 8 BIT

Andro Alif Rakhman
Teknik Informatika S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
androalif@rocketmail.com

Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang sangat penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi atau yang dikenal juga dengan kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Beberapa algoritma kriptografi yang sering digunakan saat ini adalah algoritma *Rivest Shamir Adleman (RSA)* dan *Vigenere Cipher*. Penerapan algoritma kriptografi dapat diimplementasikan pada berbagai jenis file, salah satunya adalah citra gambar. Dalam penelitian ini, citra gambar yang akan digunakan yaitu file bitmap dengan kedalaman piksel 8 bit. Citra gambar akan diolah dengan cara mengenkripsi nilai indeks warna RGB pada masing-masing piksel dengan menggunakan algoritma kriptografi RSA terlebih dahulu kemudian dilanjutkan dengan menggunakan algoritma *Vigenere Cipher*. Hal ini dilakukan agar citra gambar yang dihasilkan tampak lebih sulit untuk diprediksi ataupun dibobol oleh pihak ketiga.

Kata Kunci : Kriptografi, *Rivest Shamir Adleman* (*RSA*), *Vigenere Cipher*, Citra Gambar, Enkripsi Citra.

1. Latar Belakang

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan, dan menyembunyikan data pada file digital dari pihak-pihak yang tidak mempunyai otoritas untuk mengakses file-file tersebut. Salah satu usaha untuk mengamankan data dan informasi diantaranya dengan menggunakan kriptografi. Berbagai macam algoritma kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data. Diantaranya

yaitu algoritma kriptografi *Rivest Shamir Adleman (RSA)* dan *Vigenere Cipher* yang telah digunakan untuk menjaga keamanan data atau informasi saat ini.

Akan tetapi masing-masing teknik kriptografi memiliki kelemahan dalam mengamankan suatu informasi. Salah satunya informasi berupa media gambar. Penggunaan informasi melalui media gambar mempunyai beberapa kelemahan. Menurut Chin-Chen Chang (*Department of Computer Science and Information Engineering, National Chung Cheng University*, Chaiyi, Taiwan) menyebutkan bahwa jumlah kejahatan di bidang teknologi informasi telah meningkat akhir-akhir ini. Tingkat keamanan menggunakan media citra gambar telah menjadi topik penting dalam dunia komputer. Salah satu kelemahan penggunaan media informasi media gambar adalah mudah dimanipulasi oleh pihak-pihak yang memiliki kepentingan lain di dalamnya.

Melalui penelitian ini, dibangun suatu aplikasi untuk mengimplementasikan pengamanan citra gambar dengan memanfaatkan kombinasi algoritma kriptografi *Rivest Shamir Adleman (RSA)* dan *Vigenere Cipher*.

2. Landasan Teori

2.1 Implementasi

Menurut Kamus Besar Bahasa Indonesia, implementasi adalah pelaksanaan dan penerapan, dimana kedua hal ini bermaksud untuk mencari bentuk tentang hal yang disepakati terlebih dahulu.

2.2 Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Prinsip-prinsip yang mendasari kriptografi yaitu :

a. *Confidentiality* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin).
b. *Data Integrity* (keutuhan data) yaitu layanan yang mampu mengenali atau mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
c. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data atau informasi.
d. *Non-Repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan, kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

2.3 Metode Rivest Shamir Adleman (RSA)

Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci privat. Keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA masih dipercaya dan digunakan secara luas di internet.

2.3.1 Pembangkitan Kunci RSA

Berikut ini akan disampaikan pembentukan kunci privat dan kunci publik dengan menggunakan algoritma RSA :

1. Pilih dua bilangan prima p dan q secara acak.
2. Hitung $n = p.q$. Untuk kemudian bilangan n disebut parameter sekuriti. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n.
3. Pilih bilangan e secara acak di mana e tidak memiliki faktor pembagi yang sama dengan $(p-1)(q-1)$ selain bilangan 1. Atau dengan kata lain bersifat relatif prima.
4. Hitung d sedemikian sehingga $e.d \bmod (p-1)(q-1) = 1$. Dengan menggunakan sebuah algoritma yang disebut algoritma *Euclid* akan menghitung d sehingga, $d = e^{-1} \bmod ((p-1)(q-1))$.
5. Bilangan n dan e kita sebarkan ke publik. e ini adalah yang akan menjadi kunci publik. d menjadi kunci privat. Sementara itu bilangan p dan q dihilangkan, dan dicegah agar tidak pernah sampai bocor ke publik.

Kini sudah didapatkan sebuah kunci publik dan kunci privat. Selanjutnya berikut ini adalah algoritma untuk menyandi dan menterjemahkan pesan :

1. Untuk menyandi sebuah pesan m dengan menggunakan kunci publik e, kita melakukan operasi $m^e \bmod n$, sementara untuk membuka pesan tersandi c dengan menggunakan kunci privat, kita lakukan $c^d \bmod n$.
2. Untuk memudahkan enkripsi dan dekripsi maka pesan m dibagi menjadi beberapa blok yang kecil.

Algoritma di atas adalah algoritma yang digunakan dalam penyandian RSA, maka hanya menggunakan operasi pemangkatan bilangan dan modulus bilangan, dalam melakukan proses enkripsi dan dekripsi sebuah pesan. Kesederhanaan inilah yang menjadikan RSA menjadi popular karena relatif mudah dimengerti.

2.3.2 Enkripsi RSA

Untuk enkripsi pada RSA digunakan fungsi perpangkatan modular dengan blok plainteks $m < n$, dimana fungsi cipherteksnya adalah

$c = m^e \bmod n$..... **(2-1)**

Untuk penjelasan lebih lanjutnya, maka akan diaplikasikan penerapan algoritma RSA pada perhitungan berikut ini :

1. Misalkan $p = 47$ dan $q = 71$.
2. $n = p.q = 3337$.
3. $(p-1)(q-1) = 46 * 70 = 3220$.
4. Pilih e secara acak dan memenuhi syarat, misalkan $e = 79$.
5. Kunci privat, $d = 79 \bmod 3220 = 1019$.

Misalkan pesan yang akan dikirim adalah $m = 688232687966668003$. Sehingga penyandian pesan m tersebut adalah sebagai berikut :

1. m dibagi menjadi blok-blok. Dalam kasus ini m dibagi menjadi 6 blok yang masing-masingnya terdiri dari 3 digit, sehingga
   $m_1 = 688$ $m_2 = 232$
   $m_3 = 687$ $m_4 = 966$
   $m_5 = 668$ $m_6 = 003$
2. Enkripsi blok pertama adalah $m_1^e \bmod n$, sehingga :
   $688^{79} \bmod 3337 = 1570 = c_1$
3. Dengan cara yang sama untuk setiap blok maka diperoleh :
   $c = 1570\ 2765\ 209\ 2276\ 2423\ 158$

2.3.3 Dekripsi RSA

Untuk mendekripsi cipherteks dibutuhkan kunci privat atau kunci rahasia, dimana penerima harus memiliki kunci privat yang tepat untuk dapat melakukan dekripsi terhadap cipherteks yang dikirimkan oleh pengirim. Untuk mendekripsikan cipherteks agar penerima mengetahui plainteks, maka digunakan fungsi berikut ini:

$m = c^d \bmod n$ ..... **(2-2)**

Untuk pendekripsian pada perhitungan di atas adalah $c^d \bmod n$, sehingga :

$1570^{1019} \bmod 3337 = 688 = m_1$

$2765^{1019} \bmod 3337 = 232 = m_2$

begitu seterusnya hingga akan didapatkan plainteksnya.

2.4 Metode Vigenere Cipher

2.4.1 Dasar Teori *Vigenere Cipher*

Vigenere Cipher termasuk kode abjad - majemuk (*polyalphabetic substitution cipher*). *Vigenere Cipher* merupakan algoritma kriptografi simetris, yaitu *cipher* klasik abjad majemuk. Karena setiap huruf dienkripsikan dengan fungsi yang berbeda. *Vigenere Cipher* merupakan bentuk pengembangan dari *Caesar Cipher*. Teknik enkripsi *Vigenere Cipher* bisa diselesaikan dengan menggunakan dua cara, yaitu dengan menggunakan substitusi angka dan bujursangkar *vigènere*.

2.4.2 Enkripsi *Vigenere Cipher*

Metode untuk melakukan proses enkripsi dengan menggunakan *tabula recta* (disebut juga bujursangkar *vigènere*).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1 : Contoh Tabula Recta Algoritma Kriptografi Vigenere Cipher

Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar cipher, yang mana jumlah pergeseran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A=0, B=1, C=2, …, Z=25). Sebagai contoh, huruf kunci C (=2) menyatakan huruf-huruf plainteks digeser sejauh 2 huruf ke kanan (dari susunan alfabetnya), sehingga huruf-huruf cipherteks pada baris C adalah :

C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Gambar 2 : Potongan Tabula Recta Baris ke-C

Bujursangkar *vigenere* digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang penggunaannya (sistem periodik). Bila panjang kunci adalah *m*, maka periodenya dikatakan *m*. Sebagai contoh, jika plainteks adalah THIS PLAINTEXT dan kunci adalah SONY, maka penggunaan kunci secara periodik sebagai berikut :

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS

Untuk mendapatkan cipherteks dari teks dan kunci di atas, untuk huruf plainteks pertama T, ditarik garis vertikal dari huruf T dan ditarik garis mendatar dari huruf S, perpotongannya adalah pada kotak yang berisi huruf L. Dengan cara yang sama, ditarik garis vertikal dari huruf H dan ditarik garis mendatar pada huruf O, perpotongannya adalah pada kotak yang juga berisi berisi huruf V. hasil enkripsi seluruhnya adalah sebagai berikut :

Plainteks : THIS PLAINTEXT
Kunci : SONY SONYSONYS
Cipherteks : LVVQ HZNGFHRVL

Sedangkan secara matematis atau substitusi angka, enkripsi *Vigenere Cipher* dengan jumlah karakter sebanyak 26 dapat ditulis dalam bentuk :

$C_i = (P_i + K_j) \bmod 26$ atau $C_i = (P_i + K_j) \bmod n$ ..... **(2-3)**

Contoh :

Terdapat 10 karakter (n = 10) yang digunakan, yaitu A, B, C, D, E, F, G, H, I, dan _ yang bersesuaian dengan bilangan bulat 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (modulo 10).

A	B	C	D	E	F	G	H	I	_
0	1	2	3	4	5	6	7	8	9

Tabel 1 : Tabel Dengan 10 Karakter

Misalkan plainteks yang akan dienkripsikan adalah ADA_ECI.
Plainteks : ADA_ECI yang bersesuaian dengan 0309428
Kunci : DIA yang bersesuaian dengan 380

A	D	A	_	E	C	I
0	3	0	9	4	2	8
D	I	A	D	I	A	D
3	8	0	3	8	0	3

Tabel 2 : Tabel Enkripsi ADA_ECI Dengan Kunci DIA

Berdasarkan tabel 2 :
E(A) = (0+3) mod 10 = 3 = D
E(D) = (3+8) mod 10 = 1 = B
E(A) = (0+0) mod 10 = 0 = A
E(_) = (9+3) mod 10 = 2 = C
E(E) = (4+8) mod 10 = 2 = C
E(C) = (2+0) mod 10 = 2 = C
E(I) = (8+3) mod 10 = 1 = B.
Cipherteks : DBACCCB

2.4.3 Dekripsi *Vigenere Cipher*

Proses dekripsi pada *Vigenere Cipher* pada dasarnya sama dengan proses enkripsinya. Secara matematis, dekripsi *Vigenere Cipher* dengan jumlah karakter sebanyak 26 dapat ditulis dalam bentuk :
$P_i = (C_i - K_j) \bmod 26$ atau $P_i = (C_i - K_j) \bmod n$ ..... **(2-4)**
Contoh :

Terdapat 10 karakter (n = 10) yang digunakan, yaitu A, B, C, D, E, F, G, H, I, dan _ yang bersesuaian dengan bilangan bulat 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (modulo 10). Seperti tabel 2.

Misalkan plainteks yang akan dienkripsikan adalah DBACCCB.
Plainteks : DBACCCB yang bersesuaian dengan 3102221
Kunci : DIA yang bersesuaian dengan 380

D	B	A	C	C	C	B
3	1	0	2	2	2	1
D	I	A	D	I	A	D
3	8	0	3	8	0	3

Tabel 3 : Tabel Dekripsi DBACCB Dengan Kunci DIA

Berdasarkan tabel (3) :
D(D) = (3-3) mod 10 = 0 = A
D(B) = (1-8) mod 10 = 3 = D
D(A) = (0-0) mod 10 = 3 = A
D(C) = (2-3) mod 10 = 9 = _
D(C) = (2-8) mod 10 = 4 = E
D(C) = (2-0) mod 10 = 2 = C
D(B) = (1-3) mod 10 = 8 = I.
Sehingga cipherteks DBACCCB kembali menjadi plainteks ADA_ECI

2.5 Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan.

2.5.1 Format File Bitmap

Citra Bitmap sering disebut juga dengan citra raster. Citra bitmap menyimpan data kode citra secara digital dan lengkap (cara penyimpanannya adalah per piksel). Cara bitmap dipresentasikan dalam bentuk matriks atau dipetakan dengan menggunakan bilangan biner atau sistem bilangan lain. Citra ini memiliki kelebihan untuk memanipulasi warna, tetapi untuk mengubah objek lebih sulit. Tampilan bitmap mampu menunjukkan kehalusan gradasi bayangan dan warna dari sebuah gambar. Oleh karena itu, bitmap merupakan media elektronik yang paling tepat untuk gambar-gambar dengan perpaduan gradasi warna yang rumit, seperti foto dan lukisan digital. Citra bitmap biasanya diperoleh dengan cara *Scanner*, *Camera Digital*, *Video Capture*, dan lain-lain.

2.5.2 *Most Significant Bit* dan *Least Significant Bit*

Most Significant Bit (MSB) yaitu angka yang paling berarti atau paling besar dan letaknya di sebelah paling kiri. Misalnya pada *byte* **0**0011001, maka bit MSB-nya adalah bit yang terletak di paling kiri yaitu **0**.

Least Significant Bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti atau paling kecil. Letaknya adalah paling kanan dari barisan bit. Misalnya pada *byte* 0001100**1**, maka bit LSB-nya adalah bit yang terletak di paling kanan yaitu **1.**

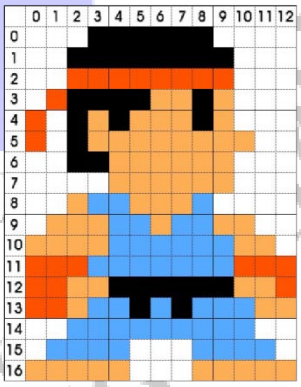
3. Metode Penelitian

3.1 Objek Penelitian

Objek penelitian yang akan digunakan dalam penelitian ini adalah citra gambar Bitmap (*bmp) dengan kedalaman piksel 8 bit yang mempunyai variasi warna serta dimensi ukuran citra yang beragam.

3.2 Tahap Pengenalan Citra

Dikarenakan tiap-tiap komponen RGB piksel memiliki panjang 8 bit (0-255), maka sistem modulo yang dipakai dalam penyandian adalah 256. Penulis mengambil contoh gambar bitmap sederhana untuk bahan analisa.



Gambar 3 : Representasi bitmap 8 bit (256 color)

Berdasarkan gambar 3, karena berbasis gambar 8 bit maka sistem warna yang digunakan adalah sistem *indexed color* yaitu sistem pengindeksan pada warna. Sistem indeks warna adalah sebuah nilai numerik sederhana yang menentukan warna suatu obyek. Sehingga tiap-tiap piksel yang diperoleh mewakili nilai

indeks warna, seperti yang ditunjukkan pada gambar 4.

Y \ X	0	1	2	3	4	5	6	7	8	9	10	11	12
0	214	214	214	108	108	108	108	108	108	214	214	214	214
1	214	214	108	108	108	108	108	108	108	108	214	214	214
2	214	214	228	228	228	228	228	228	228	228	214	214	214
3	214	228	108	108	108	108	163	163	108	163	214	214	214
4	228	214	108	163	108	163	163	163	108	163	214	214	214
5	228	214	108	163	163	163	163	163	163	163	163	214	214
6	214	214	108	108	163	163	163	163	163	163	214	214	214
7	214	214	214	214	163	163	163	163	163	163	214	214	214
8	214	214	163	58	58	163	163	163	58	214	214	214	214
9	214	163	163	163	58	58	163	58	58	163	163	214	214
10	163	163	163	163	58	58	58	58	58	58	163	163	214
11	228	228	228	58	58	58	58	58	58	58	228	228	228
12	228	228	163	163	108	108	108	108	108	108	163	163	228
13	228	228	163	58	58	108	58	108	58	58	58	163	163
14	214	214	58	58	58	58	58	58	58	58	58	214	214
15	214	58	58	58	58	214	214	214	58	58	58	58	214
16	163	163	163	163	163	214	214	214	163	163	163	163	163

Gambar 4 : Nilai indeks warna dari bitmap

3.3 Metode Yang Diusulkan

Proses enkripsi pertama-tama dilakukan dengan cara mengambil nilai warna dari sebuah citra, seperti yang telah dijelaskan pada gambar 3 dan gambar 4. Nilai-nilai tersebut merupakan nilai indeks dari komponen warna merah (*Red*), hijau (*Green*), dan biru (*Blue*). Setelah diperoleh nilai indeks warna dari citra gambar tersebut, kemudian menentukan sebuah kunci publik dan kunci privat dengan menggunakan algoritma RSA.

3.3.1 Prosedur Enkripsi Citra Gambar Yang Diusulkan

Enkripsi pada citra dilakukan dengan memanfaatkan algoritma *Rivest Shamir Adleman (RSA)* dan *Vigenere Cipher*. Proses enkripsi pertama-tama dilakukan dengan cara mengambil nilai warna dari sebuah citra, seperti yang telah dijelaskan pada Gambar 3 dan Gambar 4. Nilai-nilai tersebut merupakan nilai indeks dari komponen warna merah (*Red*), hijau (*Green*), dan biru (*Blue*). Setelah diperoleh nilai indeks warna dari citra gambar tersebut, kemudian menentukan sebuah kunci publik dan kunci privat dengan menggunakan algoritma RSA.

3.3.1.1 Tahap Pembentukan Kunci RSA

Untuk proses pembentukan kunci RSA pada pengujian ini dilakukan langkah-langkah seperti berikut :

1. Menentukan 2 bilangan prima, dengan nama *p* dan *q*. Misal nilai *p* = 61 dan *q* = 53.
2. Menghitung nilai modulus (*n*) :
   → $n = p * q$ ..... **(3-1)**
   → $n = 61 \times 53$
   → $n = 3233$
3. Menghitung nilai totient n :
   → $\phi(n) = (p-1) * (q-1)$ ..... **(3-2)**
   → $\phi(n) = (61-1) * (53-1)$
   → $\phi(n) = (60 * 52)$
   → $\phi(n) = 3120$
4. Menentukan nilai *e* dengan syarat gcd (e, $\phi(n)$) = 1. Dimana *e* = bilangan prima, dan $1 < e < \phi(n)$. Pilih kunci publik *e* adalah 17 (relatif prima terhadap 3120).
5. Mencari nilai *deciphering exponent* (*d*), maka :
   → $d = (1 + (k \times \phi(n)) / e)$ ..... **(3-3)**
   → $d = (1 + (k \times 160)) / 7$
   Nilai *k* merupakan sembarang angka untuk pencarian hingga dihasilkan suatu nilai integer atau bulat. Dengan mencoba nilai *k* = 1,

2, 3, ..., hingga diperoleh nilai *d* yang bulat, yaitu *d* = 2753.

6. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai *n*, *e*, dan *d* telah didapatkan sehingga pasangan kunci telah terbentuk.
   → Pasangan kunci publik (*n*, *e*) = (3233, 17)
   → Pasangan kunci rahasia (*n*, *d*) = (3233, 2753)

3.3.1.2 Enkripsi RSA

Berdasarkan gambar 4, penulis mengambil beberapa *sample* nilai indeks sebanyak 2 x 2 piksel untuk mewakili citra gambar secara keseluruhan yang akan dienkripsi. Berikut adalah tabel nilai indeks berdasarkan koordinat *x* dan *y* yang akan dijadikan percobaan.

No	Koordinat (*x*, *y*)	Nilai Indeks Warna (*a*)	R	G	B
1	1,13	228	250	85	1
2	2,13	163	252	176	82
3	1,14	214	255	255	255
4	2,14	58	85	169	255

Tabel 4 : Nilai indeks warna bitmap untuk proses enkripsi

Dari tabel 4, nilai indeks warna yang mewakili masing-masing warna RGB merupakan nilai plainteks yang akan dienkripsi. Untuk menjalankan proses enkripsi, digunakan kunci publik yang telah dibentuk sebelumnya, yaitu kunci publik (*n*, *e*) = (3233, 17) dengan rumus $y = a^e \bmod n$.

Enkripsi		
Nilai Indeks Warna (*a*)	$y = a^e \bmod n$	Nilai Enkripsi RSA (*y*)
228	$228^{17} \bmod 3233$	293
163	$163^{17} \bmod 3233$	698
214	$214^{17} \bmod 3233$	2971
58	$58^{17} \bmod 3233$	436

Tabel 5 : Nilai hasil enkripsi RSA

Dari tabel di atas telah dihasilkan nilai enkripsi terhadap nilai indeks warna dengan perhitungan menggunakan algoritma kriptografi RSA. Langkah selanjutnya yaitu menentukan panjang kunci dan variasi bilangan kunci dengan mengunakan metode *Vigenere Cipher*.

3.3.1.3 Tahap Pembentukan Kunci *Vigenere Cipher*

Pada fase ini, proses yang dilakukan pertama kali adalah menentukan panjang variasi kunci (*r*) yang akan digunakan. Penulis membatasi panjang nilai variasi kunci *r* antara 1-4. Sedangkan bilangan yang digunakan (*r1*, *r2*, *r3*, *r4*) berkisar antara 0-999. Penulis mengambil contoh variasi nilai bilangan untuk bahan analisa.

Panjang kunci *r* = 3
Bilangan r1 = 875
Bilangan r2 = 736
Bilangan r3 = 789

Banyaknya bilangan kunci r1, r2, r3, r4 menyesuaikan dengan panjang kunci r yang diinputkan. Jika panjang nilai bilangan r kurang dari 4, maka nilai bilangan r akan diulang kembali mulai dari r1.

3.3.1.4 Enkripsi *Vigenere Cipher*

Nilai kunci *r* yang telah ditentukan pada proses sebelumnya kemudian dihitung kembali dengan cara dimodulasikan dengan angka 1000. Angka 1000 mengacu pada banyaknya nilai bilangan yang digunakan berkisar antara 0-999. Rumus matematik dari *Vigenere Cipher* yaitu $s = (y + r_{1,2,3,4}) \bmod 1000$.

Enkripsi		
Nilai Enkripsi RSA (*y*)	**$s = (y + r_{1,2,3,4}) \bmod 1000$**	**Nilai Enkripsi Vigenere (*s*)**
293	(293 + 875) mod 1000	1168
698	(698 + 736) mod 1000	1434
2971	(2971 + 789) mod 1000	3760
436	(436 + 875) mod 1000	1311

Tabel 6 : Nilai hasil enkripsi *Vigenere Cipher*

3.3.1.5 Konversi Biner MSB dan LSB (1 byte)

Nilai enkripsi sesuai tabel di atas tidak dapat langsung digunakan menjadi nilai indeks warna untuk enkripsi. Karena nilai di atas memiliki panjang 2 *byte*, sedangkan maksimal nilai indeks sebuah warna adalah 1 *byte* (0-255). Nilai tersebut harus dibagi menjadi 2 blok 1 *byte* yaitu *Most Significant Bit* (MSB) dan *Least Significant Bit* (LSB).

Untuk analisa percobaan, penulis mengambil nilai desimal hasil enkripsi pada tabel di atas, yaitu 1168. Kemudian nilai 1168 akan dikonversikan ke binari (bit) MSB dan LSB. Didapat nilai MSB adalah 00000100, dan LSB adalah 10010000. Kemudian nilai biner MSB dan LSB tersebut dibagi tiap 1 *byte* dan dikonversikan ke desimal maka hasil nilai indeks warna enkripsi adalah 4 dan 144. Hasil lengkapnya ditunjukkan pada tabel berikut.

Nilai Enkripsi Vigenere (*s*)	**Konversi Ke Biner**		**Nilai Enkripsi Indeks Warna Akhir (*m*)**
1168	MSB	00000100	4
	LSB	10010000	144
1434	MSB	00000101	5
	LSB	10011010	154
3760	MSB	00001110	14
	LSB	10110000	176
1311	MSB	00000101	5
	LSB	00011111	31

Tabel 7 : Pembagian nilai enkripsi menjadi blok 8 bit

Dari tabel di atas sudah diperoleh nilai enkripsi indeks warna yang telah dipisahkan menjadi 1 *byte*. Sehingga dapat langsung dicocokkan dengan tabel warna. Dikarenakan hasil enkripsi menghasilkan blok sebanyak 2 *bytes* maka jumlah piksel juga akan bertambah menjadi 2 kali lipat, dimana setiap nilai indeks enkripsi diatur kembali dengan tidak mengubah lebar gambar asli dan hanya menambah tingginya sehingga menghasilkan ukuran 2 x 4 piksel seperti yang ditunjukkan pada tabel 8.

No	Koordinat (x, y)	Nilai Indeks Warna (m)	R	G	B
1	1,13	4	130	83	13
2	2,13	144	162	157	122
3	1,14	5	175	225	233
4	2,14	154	47	156	221
5	1,15	14	223	43	32
6	2,15	176	254	194	124
7	1,16	5	242	215	250
8	2,16	31	96	129	231

Tabel 8 : Nilai indeks warna bitmap hasil enkripsi

3.3.2 Prosedur Dekripsi Citra Gambar Yang Diusulkan

Untuk membuktikan analisa enkripsi telah berhasil, maka proses dekripsi harus menggunakan prosedur algoritma *Vigenere Cipher* dan RSA dengan benar, selain itu konversi dari nilai indeks warna enkripsi ke binari (bit) juga harus benar, sehingga proses dekripsi sesuai dengan analisa perhitungan awal penelitian.

3.3.2.1 Konversi Nilai Indeks Ke Binari (bit)

Untuk melakukan dekripsi, mula-mula nilai dari 2 bagian piksel yang masing-masing berukuran 1 *byte* disatukan menjadi nilai 2 *byte* atau 16 bit.

Untuk analisa percobaan, penulis mengambil nilai indeks warna enkripsi (m) pada tabel 8, yaitu 4 dan 144. Kemudian nilai indeks warna enkripsi 4 dan 144 dikonversikan ke binari (bit) MSB dan LSB. Didapat nilai MSB dari 4 adalah 00000100, dan nilai LSB dari 144 adalah 10010000. Kemudian nilai biner masing-masing MSB dan LSB yang bernilai 1 *byte* tersebut digabungkan menjadi 2 *byte*, sehingga menjadi 0000010010010000 merupakan nilai binari dari desimal 1168. Hasil lengkapnya ditunjukkan pada tabel berikut.

Nilai Indeks Warna Enkripsi (m)	Konversi Ke Biner		Nilai Enkripsi Vigenere (s)
4	MSB	00000100	1168
144	LSB	10010000	
5	MSB	00000101	1434
154	LSB	10011010	
14	MSB	00001110	3760
176	LSB	10110000	
5	MSB	00000101	1311
31	LSB	00011111	

Tabel 9 : Gabungan 2 nilai suatu piksel menjadi 2 *byte*

3.3.2.2 Dekripsi Vigenere Cipher

Untuk tahap dekripsi *Vigenere Cipher*, prosesnya hampir sama dengan proses enkripsinya. Hanya saja proses matematisnya yaitu $y = (s - r_{1,2,3,4}) \bmod 1000$. Hasil lengkapnya ditunjukkan pada tabel berikut.

Dekripsi		
Nilai Enkripsi Vigenere (s)	$y = (s - r_{1,2,3,4}) \bmod 1000$	Nilai Enkripsi RSA (y)
1168	(1168 - 875) mod 1000	293
1434	(1434 - 736) mod 1000	698
3760	(3760 - 789) mod 1000	2971
1311	(1311 - 875) mod 1000	436

Tabel 10 : Tabel dekripsi *Vigenere Cipher*

3.3.2.3 Dekripsi Rivest Shamir Adleman

Dalam proses dekripsi RSA digunakan kunci rahasia yang sudah ditentukan sejak awal perhitungan. Pasangan kunci rahasia (n, d) = (3233,

2753) dengan rumus $a = y^d \bmod n$. Untuk hasil lengkapnya ditunjukkan pada tabel berikut.

Dekripsi RSA		
Nilai Enkripsi RSA (*y*)	**$a = y^d \bmod n$**	**Nilai Indeks Warna (*a*)**
293	$293^{2753} \bmod 3233$	228
698	$698^{2753} \bmod 3233$	163
2971	$2971^{2753} \bmod 3233$	214
436	$436^{2753} \bmod 3233$	58

Tabel 11 : Tabel dekripsi nilai indeks warna

Selanjutnya dari hasil nilai dekripsi di atas maka dicocokkan dengan tabel warna atau *palette* untuk mendapatkan komponen warna sebenarnya.

4. Analisis Hasil Penelitian dan Pembahasan

4.1 Data Penelitian

Untuk mengetahui kemampuan maksimal algoritma RSA dan *Vigenere Cipher*, aplikasi ini diuji dengan melakukan enkripsi dan dekripsi terhadap dataset citra yang diperoleh dari HDW (http://hdw.eweb4.com/search/bmp/).

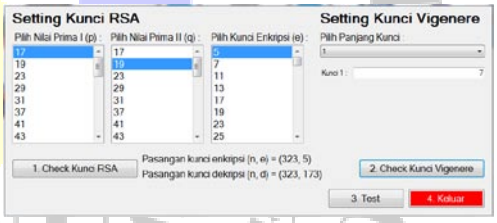
4.2 Kasus dan Hasil Pengujian

Pada pengujian ini digunakan pasangan kunci yang telah dibuat sebelumnya pada proses pembentukan kunci. Pasangan kunci ini untuk mewakili semua proses enkripsi maupun dekripsi terhadap file gambar. Percobaan ini menggunakan pasangan kunci yang bervariasi untuk membuktikan bahwa aplikasi dapat menjalankan proses enkripsi dan dekripsi sesuai algoritma yang telah dirancang.

Untuk pengujian pertama, penulis melakukan percobaan enkripsi dan dekripsi pada citra gambar seperti yang ditunjukkan pada gambar 5.

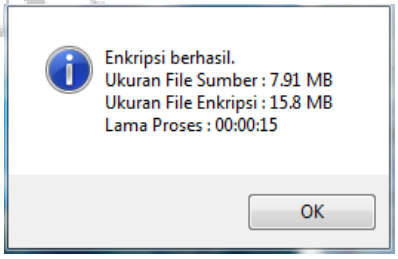
Gambar 5 : Objek Pengujian Pertama

Pasangan kunci RSA dan *Vigenere Cipher* yang digunakan pada pengujian pertama dapat dilihat pada gambar 6.

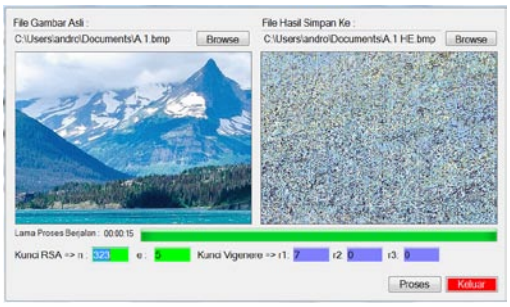


Gambar 6 : Pasangan Kunci RSA dan *Vigenere Cipher* Pengujian Pertama

Pengujian pertama dilakukan pada tipe file bitmap 8 bit dengan dimensi file 3840 X 2160 piksel dan ukuran file 7,91 MB.



Gambar 7 : Tampilan Proses Enkripsi Pengujian Pertama Berhasil



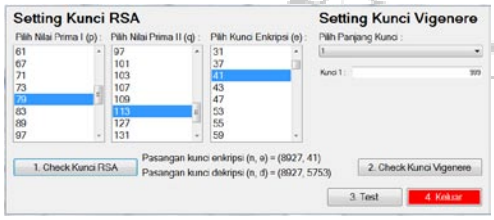
Gambar 8 : Tampilan Form Enkripsi Pengujian Pertama

Dapat dilihat pada pengujian pertama, proses enkripsi citra gambar telah berhasil dan pola warna menjadi teracak.

Untuk pengujian kedua, penulis melakukan percobaan enkripsi dan dekripsi pada citra gambar seperti yang ditunjukkan pada gambar 9.

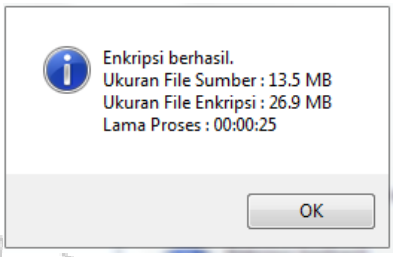
Gambar 9 : Objek Pengujian Kedua

Pasangan kunci RSA dan *Vigenere Cipher* yang digunakan pada pengujian kedua dapat dilihat pada gambar 10.

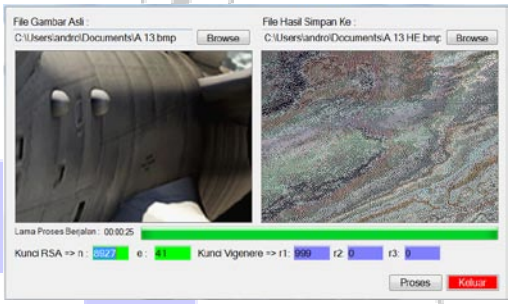


Gambar 10 : Pasangan Kunci RSA dan *Vigenere Cipher* Pengujian Kedua

Pengujian kedua dilakukan pada tipe file bitmap 8 bit dengan dimensi file 5012 x 2819 piksel dan ukuran file 13,4 MB.

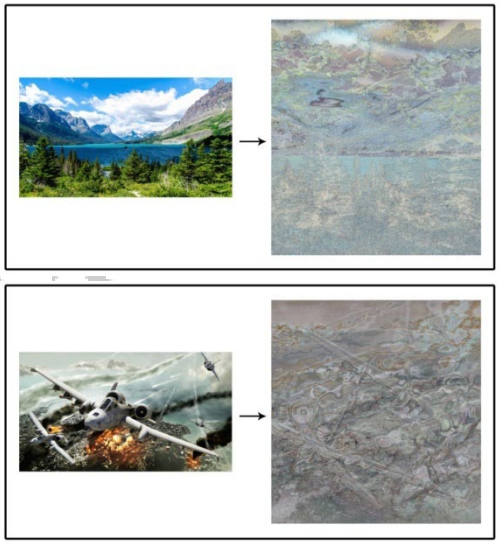


Gambar 11 : Tampilan Proses Enkripsi Pengujian Kedua Berhasil



Gambar 12 : Tampilan Form Enkripsi Pengujian Kedua

Dapat dilihat pada pengujian kedua, proses enkripsi citra gambar telah berhasil dan pola warna menjadi teracak.



Gambar 13 : Hasil perbandingan gambar sebelum dan sesudah dienkripsi.

Gambar 13 menunjukkan perbandingan citra gambar sebelum dan sesudah mengalami proses enkripsi.

Pada pengujian pertama, citra gambar asli memiliki dimensi file 3840 x 2160 piksel, setelah mengalami proses enkripsi dimensi citra gambar berubah menjadi 3840 x 4320 piksel. Ukuran lebar gambar seteleh dienkripsi menjadi 2 kali lipat dari 2160 menjadi 4320.

Pada pengujian kedua, citra gambar asli memiliki dimensi file 5012 x 2819 piksel, setelah mengalami proses enkripsi dimensi citra gambar berubah menjadi 5012 x 5638 piksel. Ukuran lebar gambar setelah dienkripsi menjadi 2 kali lipat dari 2819 menjadi 5638.

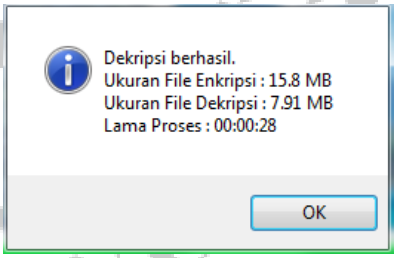
Hal ini sesuai dengan algoritma yang dirancang karena setiap byte yang dienkripsi akan menghasilkan nilai enkripsi yang dibagi menjadi blok 2 byte atau dengan kata lain menghasilkan 2 piksel. Hasil percobaan enkripsi citra gambar yang telah penulis lakukan dengan menggunakan variasi pasangan kunci RSA dan Vigenere Cipher dapat dilihat pada tabel 12.

No.	Kode File	(P)	(Q)	(E)	Nilai Enkripsi	Nilai Vigenere	Durasi Waktu	Dimensi File	Ukuran File
1	A.4.1	17	19	5	(323, 5)	1 (7)	00.00.37	3840 X 4320	15,8 MB
2	A.4.2	149	19	197	(2831, 197)	2 (768, 456)	00.00.03	1920 X 2160	3,95 MB
3	A.4.3	83	109	151	(9047, 151)	3 (768, 76, 5)	00.00.01	1366 X 1536	2,00 MB
4	A.4.4	37	41	383	(1517, 383)	1 (3)	00.00.06	2302 X 2878	6,32 MB
5	A.4.5	79	113	41	(8927, 41)	1 (999)	00.00.01	900 X 1126	991 KB
6	A.4.6	53	59	251	(3127, 251)	2 (65, 187)	00.00.26	5012 X 6266	80,0 MB
7	A.4.7	71	73	109	(5183, 109)	3 (345, 543, 567)	00.00.01	600 X 674	395 KB
8	A.4.8	23	29	113	(667, 113)	1 (472)	00.00.09	2893 X 3616	9,98 MB
9	A.4.9	61	67	7	(4087, 7)	2 (4, 6)	00.00.01	800 X 1000	782 KB
10	A.4.10	19	137	359	(2603, 359)	3 (4, 13, 7)	00.00.02	1280 X 1600	1,95 MB
11	A.4.11	73	103	329	(7519, 329)	1 (83)	00.00.01	1000 X 1250	1,19 MB
12	A.4.12	97	101	139	(9797, 139)	3 (13, 76, 4)	00.00.04	2100 X 2626	5,25 MB
13	A.4.13	79	113	41	(8927, 41)	1 (999)	00.00.25	5012 X 5638	26,9 MB
14	A.4.14	37	61	347	(2257, 347)	2 (999, 333)	00.00.01	900 X 1078	948 KB

Tabel 12 : Tabel Pengujian Enkripsi

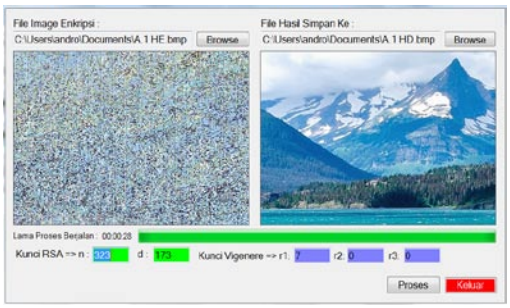
Untuk membuktikan kembali bahwa hasil enkripsi sudah benar, maka proses dekripsi dilakukan terhadap citra gambar terenkripsi dan hasil percobaan yang didapat adalah citra gambar terenkripsi akan kembali seperti semula. Dalam proses dekripsi citra gambar, pasangan kunci rahasia harus sesuai dengan perhitungan saat membuat pasangan kunci enkripsi. Apabila tidak sesuai, hal ini akan sangat berpengaruh terhadap proses pendeskripsian citra gambar, sehingga gambar yang dienkripsi tidak akan kembali seperti semula.

Mengacu pada pengujian enkripsi citra gambar yang pertama, pasangan kunci RSA dan Vigenere Cipher yang telah terbentuk seperti pada gambar 6 menghasilkan nilai kunci rahasia RSA (323, 173) dan panjang kunci Vigenere Cipher yaitu 1 dengan nilai 7.



Gambar 14 : Tampilan Proses Dekripsi Pengujian Pertama Berhasil

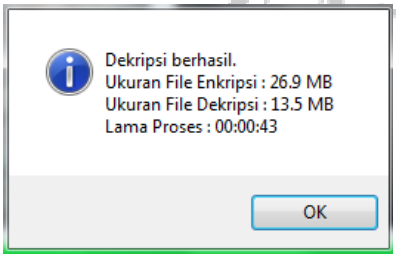
Dapat dilihat pada gambar 14 menunjukkan bahwa pengujian dekripsi citra gambar pertama telah berhasil. Hasil yang diperoleh adalah ukuran file dekripsi citra gambar telah kembali ke ukuran semula yaitu 7,91 MB dan lama waktu proses dekripsi yang dibutuhkan adalah 00:00:28.



Gambar 15 : Tampilan Form Dekripsi Pengujian Pertama

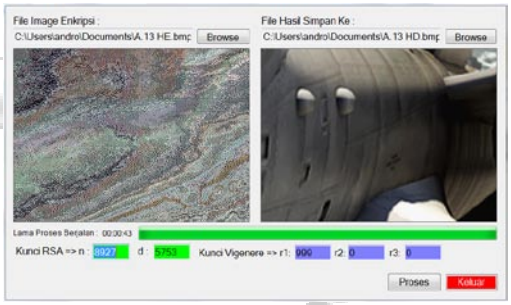
Gambar 15 menunjukkan perbandingan citra gambar setelah mengalami proses enkripsi dan citra gambar setelah mengalami proses dekripsi. Citra gambar telah berhasil didekripsikan dan secara visual pola citra gambar kembali ke bentuk semula tanpa mengalami cacat sedikitpun. Hal ini bisa dibuktikan dengan cara melihat dimensi citra gambar yang kembali ke bentuk awal, yaitu 3820 x 2160 piksel dan ukuran file citra yaitu 7,91 MB.

Untuk pengujian kedua, pasangan kunci RSA dan Vigenere Cipher yang telah terbentuk seperti pada gambar 10 menghasilkan nilai kunci rahasia RSA (8927, 5753) dan panjang kunci Vigenere Cipher yaitu 1 dengan nilai 999.



Gambar 16 : Tampilan Proses Dekripsi Pengujian Kedua Berhasil

Dapat dilihat pada gambar 16 menunjukkan bahwa pengujian dekripsi citra gambar kedua telah berhasil. Hasil yang diperoleh adalah ukuran file dekripsi citra gambar telah kembali ke ukuran semula yaitu 13,5 MB dan lama waktu proses dekripsi yang dibutuhkan adalah 00:00:43



Gambar 17 : Tampilan Form Dekripsi Pengujian Kedua

Gambar 17 menunjukkan perbandingan citra gambar setelah mengalami proses enkripsi dan citra gambar setelah mengalami proses dekripsi. Citra gambar telah berhasil didekripsikan dan secara visual pola citra gambar kembali ke bentuk semula tanpa mengalami cacat sedikitpun. Hal ini bisa dibuktikan dengan cara melihat dimensi citra gambar yang kembali ke bentuk awal, yaitu 5012 x 2819 piksel dan ukuran file citra yaitu 13,4 MB.

Hasil percobaan dekripsi citra gambar yang telah penulis lakukan dengan menggunakan variasi pasangan kunci RSA dan Vigenere Cipher dapat dilihat pada tabel 13.

No.	Kode File	Nilai Dekripsi	Nilai Vigenere	Durasi Waktu	Dimensi File	Ukuran File
1	A.4.1	(323, 173)	1 (7)	00.00.28	3840 X 2160	7,91 MB
2	A.4.2	(2831, 2069)	2 (768, 456)	00.00.06	1920 X 1080	1,98 MB
3	A.4.3	(9047, 3343)	3 (768, 76, 5)	00.00.03	1366 X 768	1,00 MB
4	A.4.4	(1515, 767)	1 (3)	00.00.10	2302 X 1439	3,16 MB
5	A.4.5	(8927, 5753)	1 (999)	00.00.02	900 X 563	495 KB
6	A.4.6	(3127, 2259)	2 (65, 187)	00.00.49	5012 X 3133	14,9 MB
7	A.4.7	(5183, 4069)	3 (345, 543, 567)	00.00.01	600 X 674	395 KB
8	A.4.8	(667, 169)	1 (472)	00.00.16	2893 X 1808	4,99 MB
9	A.4.9	(4087, 2263)	2 (4, 6)	00.00.02	800 X 500	391 KB
10	A.4.10	(2603, 791)	3 (4, 13, 7)	00.00.03	1280 X 800	0,97 MB
11	A.4.11	(7519, 2009)	1 (83)	00.00.02	1000 X 625	611 KB
12	A.4.12	(9797, 7459)	3 (13, 76, 4)	00.00.08	2100 X 1313	2,62 MB
13	A.4.13	(8927, 5753)	1 (999)	00.00.45	5012 X 2819	13,4 MB
14	A.4.14	(2257, 803)	2 (999, 333)	00.00.02	900 X 539	474 KB

Tabel 13 : Tabel Pengujian Dekripsi

Hal ini menunjukkan bahwa penerapan algoritma RSA dan *Vigenere Cipher* untuk enkripsi dan dekripsi citra gambar 8 bit telah berhasil.

4.3 Analisis Hasil Pengujian

Analisa hasil pengujian dilihat dari perbandingan citra gambar sebelum dan sesudah dilakukan proses enkripsi dan dekripsi dengan menggunakan metode algoritma kriptografi RSA dan Vigenere Cipher.

4.3.1 Hasil Analisis Ruang Kunci

Dapat dilihat pada proses enkripsi pengujian pertama dan pengujian kedua, penggunaan kombinasi ruang kunci algoritma RSA dan Vigenere Cipher dapat menghasilkan perubahan nilai indeks warna dari masing-masing piksel. Hal ini dibuktikan dengan perubahan pola warna citra gambar hasil enkripsi yang dapat diamati secara visual.

Untuk proses dekripsi, penggunaan pasangan ruang kunci harus sesuai dengan pasangan kunci saat proses enkripsi. Apabila pasangan kunci dekripsi tidak sesuai, maka pola gambar yang dihasilkan tidak akan kembali ke bentuk semula.

Akan tetapi seperti yang disebutkan Arifin Luthfi P (Program Studi Teknik Informatika, Institut Teknologi Bandung) dalam tesisnya yang berjudul Enkripsi Citra Bitmap Melalui Substitusi Warna Menggunakan Vigenere Cipher menyebutkan bahwa “Kunci yang panjang dan kompleks akan sangat sulit untuk diingat oleh manusia, hal ini nampak sia-sia karena jika kita memakai kata kunci yang panjang dan kompleks, kita harus meletakkannya pada suatu file khusus untuk kunci tersebut. Jika file yang berisi kunci tersebut bocor pada publik, maka enkripsi citra ini akan sia-sia karena dapat didekripsi dengan mudah [15].”

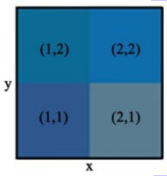
Analisa hasil pengujian dilihat dari perbandingan citra gambar sebelum dan sesudah dilakukan proses enkripsi dan dekripsi dengan menggunakan metode algoritma kriptografi RSA dan *Vigenere Cipher*.

4.3.2 Hasil Analisis Perubahan Nilai Indeks Warna

Untuk membuktikan nilai indeks warna dari masing-masing piksel mengalami perubahan, penulis mengambil contoh beberapa piksel untuk diteliti kembali perubahan nilai indeks warnanya sebelum dienkripsi dan sesudah dienkripsi pada objek pengujian pertama.

Gambar 18 : Objek pengujian pertama yang akan diteliti nilai indeks warnanya

Berdasarkan gambar 18, penulis mengambil beberapa *sample* nilai indeks sebanyak 2 x 2 piksel di dalam lingkaran berwarna kuning untuk mewakili citra gambar secara keseluruhan yang akan dienkripsi.



Gambar 19 : *Sample* piksel 2 x 2

Untuk memudahkan pemberian koordinat piksel, maka penulis memberikan pengkodean nama piksel terhadap gambar 19 berdasarkan koordinat *x* dan *y*. Berikut adalah tabel nilai indeks warna potongan piksel di atas berdasarkan koordinat *x* dan *y* yang akan diteliti.

No	(*x*, *y*)	Nilai Indeks Warna (*a*)	R	G	B
1.	1,1	56	210	62	48
2.	2,1	192	75	72	131
3.	1,2	73	133	252	24
4.	2,2	95	164	127	31

Tabel 14 : Nilai indeks warna bitmap

Dari tabel di atas, nilai indeks warna yang mewakili masing-masing warna RGB merupakan nilai plainteks yang akan dienkripsi. Untuk menjalankan proses enkripsi, digunakan kunci publik yang telah dibentuk sebelumnya, yaitu kunci publik (*n*, *e*) = (323, 5).

Enkripsi		
Nilai Indeks Warna (*a*)	**$y = a^e \bmod n$**	**Nilai Enkripsi RSA (*y*)**
56	$56^5 \bmod 323$	303
192	$192^5 \bmod 323$	184
73	$73^5 \bmod 323$	99
95	$95^5 \bmod 323$	57

Tabel 15 : Nilai hasil enkripsi RSA

Dari tabel di atas telah dihasilkan nilai enkripsi terhadap nilai indeks warna dengan perhitungan menggunakan algoritma kriptografi RSA. Langkah selanjutnya yaitu menghitung kembali nilai hasil enkripsi di atas menggunakan metode Vigenere Cipher yang sudah ditentukan panjang kuncinya adalah 1 dengan nilai 7.

Enkripsi		
Nilai Enkripsi RSA (*y*)	**$s = (y + r_{1,2,3}) \bmod 1000$**	**Nilai Enkripsi Vigenere (*s*)**
303	(303 + 7) mod 1000	310
184	(184 + 7) mod 1000	191
99	(99 + 7) mod 1000	106
57	(57 + 7) mod 1000	64

Tabel 16 : Nilai hasil enkripsi Vigenere Cipher

Nilai enkripsi sesuai tabel di atas kemudian dibagi menjadi 2 blok 1 *byte* yaitu *Most Significant Bit* (MSB) dan *Least Significant Bit* (LSB). Hasil lengkapnya ditunjukkan pada tabel berikut.

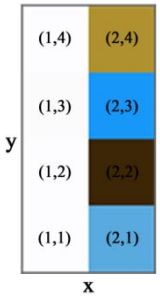
Nilai Enkripsi Vigenere (*s*)	Konversi Ke Biner		Nilai Enkripsi Indeks Warna Akhir (*m*)
310	MSB	00000001	1
	LSB	00110110	54
191	MSB	00000000	0
	LSB	10111111	191
106	MSB	00000000	14
	LSB	01101010	106
64	MSB	00000000	0
	LSB	01000000	64

Tabel 17 : Pembagian nilai enkripsi menjadi blok 8 bit

Seperti yang sudah dijelaskan pada bab III, berikut ini adalah hasil perubahan nilai indeks warna dari masing-masing piksel setelah mengalami proses enkripsi.

No.	Koordinat (*x*, *y*)	Nilai Indeks Warna (*m*)	R	G	B
1	1,1	1	252	252	254
2	2,1	54	88	170	223
3	1,2	0	252	252	254
4	2,2	191	60	33	8
5	1,3	14	251	251	251
6	2,3	106	24	162	248
7	1,4	0	252	252	254
8	2,4	64	175	145	48

Tabel 18 : Hasil perubahan nilai indeks warna bitmap setelah enkripsi



Gambar 20 : Hasil *palette* warna dari nilai indeks tabel 18

Secara visual, gambar 20 menunjukkan perubahan warna yang terjadi setelah mengalami proses enkripsi. Hal ini membuktikan bahwa metode enkripsi yang dirancang telah berhasil digunakan untuk memperbaruhi nilai indeks warna citra gambar asli.

Untuk melakukan dekripsi citra gambar, mula-mula nilai dari 2 bagian piksel yang masing-masing berukuran 1 *byte* disatukan menjadi nilai 2 *byte* atau 16 bit, seperti yang sudah dijelaskan pada bab III. Hasil lengkapnya ditunjukkan pada tabel berikut.

Nilai Indeks Warna Enkripsi (*m*)	Konversi Ke Biner		Nilai Enkripsi Vigenere (*s*)
1	MSB	00000001	310
54	LSB	00110110	
0	MSB	00000000	191
191	LSB	10111111	
14	MSB	00000000	106
106	LSB	01101010	
0	MSB	00000000	64
64	LSB	01000000	

Tabel 19 : Gabungan 2 nilai piksel menjadi 2 *byte*

Untuk tahap dekripsi Vigenere Cipher, prosesnya hampir sama dengan proses enkripsinya. Hasil lengkapnya ditunjukkan pada tabel berikut.

Dekripsi		
Nilai Enkripsi Vigenere (*s*)	**$y = (s - r_{1,2,3})$ mod 1000**	**Nilai Enkripsi RSA (*y*)**
310	(310 - 7) mod 1000	303
191	(191 - 7) mod 1000	184
106	(106 - 7) mod 1000	99
64	(64 - 7) mod 1000	57

Tabel 20 : Tabel dekripsi Vigenere Cipher

Dalam proses dekripsi RSA digunakan kunci rahasia yang sudah ditentukan sejak awal perhitungan. Pasangan kunci rahasia (*n*, *d*) = (323, 173). Untuk hasil lengkapnya ditunjukkan pada tabel berikut.

Dekripsi RSA		
Nilai Enkripsi RSA (*y*)	**$a = y^d$ mod *n***	**Nilai Indeks Warna (*a*)**
303	303^{173} mod 323	56
184	184^{173} mod 323	192
99	99^{173} mod 323	73
57	57^{173} mod 323	95

Tabel 21 : Tabel dekripsi nilai indeks warna semula

Selanjutnya dari hasil nilai dekripsi di atas maka dicocokkan dengan tabel warna atau *palette* untuk mendapatkan komponen warna sebenarnya.

4.3.3 Analisis Waktu Proses Enkripsi dan Dekripsi

Rata-rata lama waktu yang dibutuhkan untuk proses dekripsi lebih lama dibandingkan dengan lama waktu proses enkripsi. Hal ini dikarenakan saat melakukan proses dekripsi, nilai dari 2 bagian piksel yang masing-masing berukuran 1 byte mengalami proses penggabungan byte menjadi nilai 2 byte atau 16 bit. Semakin besar ukuran suatu file citra gambar yang akan diproses, semakin lama waktu yang dibutuhkan untuk menyelesaikan proses tersebut. Sebaliknya, semakin kecil ukuran suatu file citra gambar yang akan diproses, semakin singkat waktu yang dibutuhkan untuk menyelesaikan proses tersebut.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dalam buku tesis ini telah dipaparkan hasil pengujian dan analisis penggunaan kombinasi algoritma RSA dan Vigenere Cipher dalam mengenkripsi dan mendekripsikan citra gambar bitmap 8 bit. Hasil pengujian menunjukkan secara visual citra gambar hasil enkripsi sulit untuk dibaca atau dilihat. Hal ini disebabkan karena keteracakan pola warna dan perubahan intensitas nilai indeks warna yang dihasilkan setelah mengalami enkripsi.

Citra gambar yang didekripsikan tidak mengalami cacat sedikitpun dan berhasil kembali ke bentuk semula. Hal ini dibuktikan secara visual maupun dari hasil analisa perubahan nilai indeks warna.

Keteracakan pola warna hasil enkripsi juga dipengaruhi oleh pola warna citra gambar asli. Semakin banyak variasi pola warna pada citra gambar asli, semakin sulit dan acak pola warna enkripsi yang dihasilkan.

Dari beberapa parameter uji coba menunjukkan bahwa proses enkripsi menggunakan algoritma kriptografi RSA dan Vigenere Cipher pada citra

gambar bitmap 8 bit telah berhasil dengan baik. Sehingga konsep penggunaan algoritma kriptografi yang diusulkan layak digunakan untuk mengamankan data citra gambar.

5.2 Saran

Saran dari penulis untuk pengembangan lebih lanjut tentang penggunaan kombinasi algoritma kriptografi RSA dan Vigenere Cipher ini adalah :

1. Format citra gambar yang digunakan dalam penelitian ini adalah bitmap 8 bit. Oleh karena itu, dalam pengembangan lebih lanjut bisa mengggunakan format citra gambar lain, seperti JPG/JPEG (*Joint Photographic Experts Group*), GIF (*Graphics Interchange Format*), PNG (*Portabel Network Graphics*) dan lain-lain.
2. Tambahkan kombinasi algoritma kriptografi selain RSA dan Vigenere Cipher untuk memperkuat keamanan pada citra gambar yang akan dienkripsi.
3. Citra gambar hasil enkripsi pada penelitian ini menjadi lebih besar dari citra gambar aslinya. Hal ini dikarenakan penambahan bit (padding). Oleh karena itu diperlukan suatu algoritma kompresi agar citra gambar hasil enkripsi lebih kecil.
4. Penggunaan kombinasi algoritma kriptografi RSA dan Vigenere Cipher ini diharapkan dapat diterapkan di dalam citra digital lainnya, seperti file suara atau video.
5. Hasil enkripsi citra gambar dalam penelitian ini juga bisa dikombinasikan dengan algoritma steganografi atau watermarking. Sehingga citra gambar yang dihasilkan nantinya bisa mencakup berbagai aspek keamanan.

Daftar Pustaka

1. Chin-Chen Chang (2001), *A New Encryption Algorithm for Image Cryptosystems*, Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan.
2. Zainal Arifin (2009), *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*, Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman.
3. Prisyafandiafif Charifa (2013), *Penerapan Vigenere Cipher Untuk Aksara Arab*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.
4. Rini Wati Lumbangaol (2013), *Aplikasi Pengamanan Gambar Dengan Algoritma Rivest-Shamir Adleman (RSA)*, Jurusan Teknik Informatika, STMIK Budidarma Medan.
5. Muhammad Sholeh (2012), *Pengantar Kriptografi*, Teknik Informatika. Institut Sains & Teknologi. AKPRIND.
6. Munir, Rinaldi (2010). *Bahan Kuliah IF2153 Matematika Diskrit*. Departemen Teknik Informatika, Institut Teknologi Bandung.
7. Kent Ardy Sutjiadi (2014), *Kriptografi*, Universitas Binus Jakarta.
8. Didin Mukodim (2002), *Tinjauan Tentang Enkripsi Dan Dekripsi Suatu Teknik Pengamanan Data Dengan Penyandian RSA*, Universitas Gunadarma.
9. Ivan Wibowo (2009), *Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle*, Teknik Informatika, Universitas Kristen Duta Wacana.
10. M. Yuli Andri (2009), *Implementasi Algoritma Kriptografi DES, RSA, Dan Algoritma Kompresi LZW Pada Berkas Digital*, Program Studi Ilmu Komputer Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara.
11. Dyani Mustikarini (2012), *Implementasi Dan Analisa Pengiriman Data Menggunakan Algoritma Kriptografi RSA Pada Sistem Eucalyptus Private Cloud IAAS*, Fakultas Teknik Komputer, Departemen Teknik Elektro, Universitas Indonesia.
12. Gasendra (2010), *Program Aplikasi Kombinasi Dua Kriptografi Klasik Vigenere Cipher Dan Keyed Columnar transposition*, Jurusan Matematika, Universitas Pendidikan Indonesia.
13. T Sutoyo, Edy Mulyanto, Vincent Suharono, Oky Dwi Nurhayati, and Wijanarto, *Teori Pengolahan Citra Digital*. Semarang, Indonesia: Andi, 2009.
14. Rinaldi Munir (2012), *Algoritma Enkripsi Selektif Citra Digital dalam Ranah Frekuensi Berbasis Permutasi Chaos*, Sekolah Teknik

Elektro dan Informatika, Institut Teknologi Bandung (ITB).
15. Arifin Luthfi P (2011), *Enkripsi Citra Bitmap Melalui Substitusi Warna Menggunakan Vigenere Cipher*, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung (ITB).
16. Ahmad Sofian (2015), *Aplikasi Enkripsi dan Dekripsi Video Menggunakan Algoritma Rivest-Shamir-Adleman (RSA) Pada Divisi Film Programming Bioskop Blitzmegaplex*, Program Studi Teknik Informatika, Universitas Budi Luhur.