Perancangan Aplikasi Pengamanan Citra Bewarna Dengan Algoritma RSA

Pandi Barita Nauli Simangunsong[1], Komariah Fitri[2]
[1]AMIK STIEKOM Sumatera Utara, Medan - Indonesia
[2]STMIK Budidarma Medan, Medan - Indonesia
E-Mail : simangunsong.pandi@gmail.com

Abstrak

Kriptografi adalah teknik yang digunakan untuk pengamanan sebuah pesan (message) yang bersifat rahasia*. Implementasi Kriptografi banyak berkembang dalam pemanfaatannya dalam bidang komputer. Prisnsip kerja dari kriptografi adalah mengubah pesan yang bersifat asli yang disebut dengan (plainteks) menjadi pesan yang tidak dapat sama sekali dimengerti oleh pihak lain yang disebut dengan (cipherteks) yang artinya pesan cipherteks adalah pesan yang tidak dapat dipahami oleh pihak yang tidak berkepentingan . Proses kerja tersebut merupakan proses enkripsi dan proses deskripsi. Algoritma asimetri adalah teknik yang digunakan oleh algoritma RSA, proses enkripsi dan deskripsi memiliki kunci yang tidak sama, kunci untuk enkripsi tidak akan pernah sama dengan kunci yang digunakan untuk mendeskripsi. Kunci puplik akan berguna saat dilakukan enkripsi sedangkan untuk proses deskripsi yang digunakan adalah kunci privat. Algoritma RSA yang dikenal dengan model kunci public. Teknik pengerjaan algoritma RSA sering dikenal dengan teknik pembangkit kunci acak, enkripsi dan deskripsi.*

Kata Kunci : Kriptografi, Algoritma RSA.

Abstract

Cryptography is a technique used to secure messages that allow secrets. Cryptographic implementation has developed a lot in its use in the computer field. The work principle of cryptography is to change the original changed message called (plainteks) into a message that cannot be completely understood by another party called (ciphertext) that allows ciphertext messages to be messages that cannot be used by unauthorized parties. This work process is an encryption process and process description. An asymmetry algorithm is a technique used by the RSA algorithm, the encryption process and description have unequal keys, the key to encryption will never be the same as the key used to describe. The key will be useful when encryption is performed. While the description process used is the private key. The RSA algorithm is known as the public key model. RSA is known as random key processing techniques, encryption and description.

Keywords: Cryptography, RSA Algorithm.

1. PENDAHULUAN

Kriptografi adalah cara yang menggunakan perhitungan yang memiliki kaitan hubungan dengan sebuah keamanan dalam mendapatkan sebuah pesan seperti data ataupun yang lainnya, aslinya sebuah identitas dan aslinya sebuah data[1]. Kriptografi mempunyai berbagai teknik untuk menghasilkan gambar yang aman[2]. Penyandian gambar adanya media yang menggunakan elektronik pastilah membutuhkan proses yang bisa menjamin sebuah gambar yang aman gambar dan keutuhan dari gambar tersebut. Gambar yang akan diamankan haruslah bersifat rahasia dengan bertujuan untuk menjaga karahasiaannya terhadap akses untuk menghindari pihak yang tidak mempunyai akses yang bersifat tertentu.

Permasalahan dalam keaman yaitu pada suatu gambar adalah hal yang penting untuk pribadi maupun secara umum terlebih apabila gambar yang sifatnya rahasia terhubung ke jaringan sehingga membutuhkan keamanan yang kerahasiaan data tersebut haruslah tetap terjaga meskipun data tersebut tetap dalam wilayah yang sangat berbahaya seperti terkoneksi pada sebuah internet.

Tentu saja gambar rahasia tidak boleh diakses oleh sembarangan diakses oleh pihak-pihak yang tidak memiliki kepentingan pada gambar tersebut. Apabila pihak lain mendapatkan kerahasiaan dari gambar tersebut gambar akan rusak bahkan dapat hilang dan akan mengakibatkan kerugian pada pemilik gambar yang memiliki kerahasiaan[3].

RSA adalah metode enkripsi yang dikembangkan oleh Ron Rivest Adi Shamir dan Leonard Adleman yang diperkenalkan pada tahun 1977 dan dipatenkan oleh MIT. Keamanan Algoritma RSA memiliki kesulitanya pada faktor bilangan yang cukup besar untuk menjadikan kebentuk bilangan yang bersifat prima. Pemfaktoran bertujuan untuk menghasilkan sebuah kunci yang bersifat sangat private. Adapun kelebihan dari algoritma RSA saat dilakukan enkripsi sebuah pesan,maka dengan adanya algoritma ini sangat membantu dalam mengamankan sebuah gambar untuk menghasilkan gambar yang sangat rahasia yaitu dengan cara mengenkripsi gambar tersebut dengan adanya kunci private akan membantu dalam prose pengenkripsian gambar berdasarkan piksel yang dimiliki gambar tersebut dan langkah selanjutnya adalah mengembalikan gambar yang telah dienkripsi menjadi gambar yang dapat dilihat seperti aslinya yaitu dengan cara mengenkripsi gambar tersebut.

Berdasarkan latar belakang di atas, maka perumusan masalah yang akan di bahas dari penelitian adalah Bagaimana proses pengamanan gambar, Bagaimana menerapkan algoritma RSA dalam gambar dan agar penelitian ini lebih terfokus dan tepat sesuai dengan perumusan masalah yang ada, maka batasan masalah yang dibahas dalam penelitian ini seperti Hanya membahas tentang proses enkripsi dan dekripsi gambar dengan algoritma RSA, Gambar yang digunakan sebagai sampel dalam penelitian ini adalah gambar berwarna 24 bit dan berextensi bmp[3].

2. LANDASAN TEORI

2.1 Keamanan

Keamanan adalah sebuah teknik yang paling penting dalam menghasilkan sebuah system informasi. Keamanan sering tidak diperhatikan oleh para perancang saat mengolah sistem yang menghasilkan informasi yang penting. Keamanan merupakan bagian paling terakhir oleh para program saat membangun sistem yang menghasilkan informasi yang penting oleh seabab itu diharapkan keamanan pada sebuah sistem[4].

2.2 Kriptografi

Kriptografi merupakan ilmu yang memiliki seni dalam pengacakan sebuah data, membuat pihak lain sangat sulit untuk memahami arti pesan yang telah teracak. Oleh sebab itu meskipun data yang sudah teracak sedemikian rupa juga penting dapat dipahami oleh pihak yang memiliki akses tersebut kapanpun data tersebut dibutuhkan. Yunani sangat dikenal dengan teknik kriptografi, artinya crypto dan kata graphia. Crypto memiliki arti secret (rahasia) dan Graphia merupakan tulisan. Kriptografi adalah seni yang memiliki ilmu dalam mengamankan data tersebut menjadi data yang sangat rahasia[5]

Algoritma kriptografi adalah teknik yang dilakukan sesuai dengan langkah-langkah yang mempunyai aturan yang logis sesuai dengan kebutuhan [1].

Adapun kegunaan pada algoritma untuk kriptografi adalah sebagai berikut :

1. Enkripsi
   Enkripsi adalah data asli yang memiliki sebuah kerahasiaan yang sangat penting oleh karena itu data tersebut sering disebut dengan cipherteks. Kerahasiaan sebuah data dibuat kedalam bentuk kode-kode yang tidak dapat terbaca oleh pihak yang tidak penting.
2. Dekripsi
   Dekripsi adalah teknik pengembalian pesan kebentuk aslinya, pesan yang sudah tidak dapat lagi terbaca oleh karena itu pesan ini disebut dengan istilah cipherteks maka dengan itu diperlukan cara untuk mengembalikan data yang sudah dienkripsi menjadi pesan yang dapat terbaca.
3. Kunci
   Kunci adalah teknik yang dibutuhkan untuk melancarkan proses dalam pengenkripsian.

2.3 RSA (Rivest Shamir Adleman)

Algoritma RSA akan aman dengan nilai n yang sanga besar dan akan mempengaruhi tingkat keamanan. Hanya algoritma RSA yang mempunyai kunci public yang sangat baik sampai saat ini. Algoritma RSA diciptakan 3 orang yang memiliki latar belakang seorang peneliti dari institute yang yang cukup terkenal (Massachusetts Institute of Technology) dia tahun 1976, adapun nama dari RSA adalah Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman [6][7].

Kunci publik (asimetri) pada algoritma RSA merupakan bagan dari algoritma kriptografi yang memiliki alur berjumlah tiga proses yaitu adanya pembentukan kunci, enkripsi, maupun dekripsi. Adapun proses dari tiga alur tersebut yaitu sebagai berikut:

1. Proses Pembentukan Kunci

Algoritma RSA membutuhkan pembangkit kunci dengan cara membuat nilai kunci yang random agar dapat digunakan untuk mengenkripsi sebuah pesan agar keamanan lebih terjaga. Proses ini yang pertama kali dilakukan setelah adanya pembentukan kunci atau sering disebut dengan pembangkit kunci setelah adalanya pembangkit kunci maka langkas selanjutnya adalah proses enkripsi.

Adapun cara untuk menghasilkannya adalah sebagai berikut:

a. Membuat nilai p dan nilai q, dimana nilai variable tersebut bilangan prima akan tetapi nilai kedua bilangan tersebut tidak boleh sama, dimana nilai keduanya haruslah berbeda.
b. Membuat nilai untuk modulus untuk pasangan kunci public dan kunci rahasia. Nilai modulus adalah variable yang disimbolkan dengan n. Nilai n dihasilkan dari bilangan prima p dan q dimana nilai keduanya adalah hasil dari perkalian. Secara matematis, teknik yang digunakan dalam mencari nilai (RSA) modulus adalah sebagai berikut:
c. Menjumlahkan nilai Φ(n) maupun nilai totient/phi n
d. Cari nilai enciphering exponent disimbolkan dengan variabel e, akan digunakan untuk kunci public dan nilai modulus. Enciphering exponent (e) bilangan prima terhadap variabel Φ(n), e Φ(n) merupakan hasil pembagian yang bernilai harus 1.ketentuan $1< e < \Phi(n)$ dan e haruslah prima.
e. Selanjutnya adalah tentukan nilai deciphering exponent yang merupakan variabel d, nilai decipering exponent bertujuan pasangan pembangkit kunci dan modulus dalam algoritma RSA. variabel (n,d) adalah formula untuk menemukan nilai d didapatkan dengan persamaan: Variabel k adalah merupakan nilai yang bebas yang menghasilkan nilai d yang bersifat integer (bulat).
f. Nilai variabel d, p, dan q adalah nilai yang harus rahasi, nilai variabel n, e adalah nilai yang tidak perlu dirahasiakan (bebas), pasangan (n,e) merupakan kunci yang bersifat umum, pasangan (n,d) merupakan rahasia.

2. Proses Enkripsi

Enkripsi dilakukan dengan membutuhkan kunci publik (n,e) yang akan didapat dalam pembentukan sebuah kunci. Formula yang digunakan untuk enkripsi adalah sebagai berikut.

Dimana:
Y = Ciphertext (rahasia)
X = Plaintext (Pesan asli)
N = modulus
E = Enciphering Exponent.

3. Proses Dekripsi

Dekripsi suatu teknik untuk menghasilkan pesan yang telah dienkripsi, teknik ini diperlukan untuk mengembalikan kepesan semula dengan kunci rahasia (n,d), secara matematis dekripsi didappat kedalam persamaan sebagai berikut:

Dimana:
X = Plaintext (Pesan Asli)
Y = Ciphertext (Pesan Palsu)

D = Enciphering Exponent
N = m

3. PEMBAHASAN

Penerapan teknik kriptografi dalam melakukan penyandian gambar dengan merubah nilai warna elemen warna dalam setiap piksel, sehingga nilai-nilai elemen warna piksel gambar asli (citra plain) akan berubah dengan nilai-nilai yang baru. Proses manipulasi nilai-nilai elemen warna piksel dilakukan berdasarkan algoritma kriptografi yaitu algoritma RSA, dimana algoritma ini akan memanfaatkan nilai setiap elemen warna gambar pada setiap piksel dan nilai kunci yang ditetapkan oleh pelaku penyandian.

Nilai-nilai elemen warna untuk tiap piksel dilakukan dengan menggunakan aplikasi matlab 6.1 kemudian nilai-nilai tersebut akan dimanfaatkan sebagai nilai-nilai citra plain yang akan sandikan berdasarkan algoritma RSA. Nilai yang dihasilkan tersebut akan berbentuk matriks warna dari citra plain dimana setiap piksel terdiri dari tiga nilai elemen warna yaitu red, green dan blue.

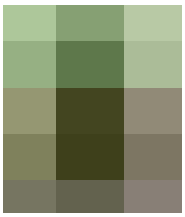
Proses manipulasi nilai-nilai dari setiap elemen warna piksel menyebabkan perubahan yang cukup signifikan pada citra plain sehigga citra plain tidak dapat dikenali lagi seperti gambar asli, dalam arti bahwa perubahan nilai-nilai elemen warna terebut menyebabkan gambar tersandi.

Penelitian ini menggunakan gambar sampel dengan ukuran 3 x 5 dan berjenis gambar berwarna yang merupakan hasil pengecilan dari gambar berukuran 1200 x 1800 dan berjenis gambar berwarna. Hal ini dilakukan untuk mempersingkat proses perhitungan manual yang dituangkan dalam penelitian ini. Namun, pada proses pengujian sistem dapan digunakan gambar yang berukuran lebih besar.

Gambar 1 Gambar Sampel ukuran

Adapun penerapan dalam mengenkripsi gambar adalah:

1. Ambil Citra Plain (Citra Asli)



Gambar 2 Citra Plain ukuran 3x5

2. Ambil nilai-nilai elemen warna setiap piksel citra plain

Tabel 1 Nilai-nilai Elemen Warna Setiap Piksel

Piksel	0			1			2		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	173	199	154	134	160	155	184	201	165
1	150	176	131	94	120	75	171	188	152
2	149	151	114	67	69	32	145	138	119
3	127	129	92	62	64	27	125	118	99
4	118	117	97	99	98	78	136	127	118

3.1. Pembentukan Kunci

Untuk proses pembenukan kunci pada pengujian ini dilakukan langkah-langkah berikut:

1. Menentukan 2 bilangan prima dengan nama variabel p dan variabel q.
   dimisalkan p = 1001 dan q = 151.
   a. Menghitung nilai modulus (n), dimana n = p*q maka:
      1001 * 151
      n = 15251
   b. Menghitung nilai totient n, dimana Φ(n) = (p-1)*(q-1) maka:
      Φ(n) = (101-1)*(151-1)
      Φ(n) = (101)*(150)
      Φ(n) = 15000
2. Mencari nilai e dengan ketentuan gcd (e, Φ(n)) = 1, e = bilangan yang prima, dan 1 < e < Φ(n) pada kasus ini, bilangan prima nilai e yang akan acak adalah 2,3,5 dan 7.
   Proses pencarian nilai e yang cocok sesuai syarat adalah sebagai berikut: Φ(n) = 15000 (didapat dari langkah sebelumnya).
3. Mencari nilai *decipherin_ exponent* (d) maka:
   d=(1+(k* Φ(n)) : e
   d=(1+(k*15000)) :7
   nilai k adalah nilai acak sampai dihasilkan satu bilangan bulat.
   k = 0
   d = (1+(0*15000)): 7, maka d=0.142 masih pecahan, lanjutkan
   k = 1 (1+(1*15000)) :7, hasilnya yang didapat d=2143 bukan pecahan, sthasil pencarian mendapatkan d=2143
4. Berdasarkan langkah diatas, nilai n, e dan d telah ditemukan sehingga pasangan kunci telah terbentuk.
   Pasangan kunci publik (n,e) = (15251,7)
   Pasangan kunci rahasia (n,d) = (15251,2143)

3.2 Enkripsi Gambar

Untuk menjalankan proses enkripsi, digunakan kunci publik yang telah dibentuk yaitu kunci publik (e,n) = (7,15251), dengan formula $C1 = m1^e$ mod n.

(0,0)
C1= 173^7 mod 15251= 4894
C2= 199^7 mod 15251= 6398
C3= 154^7 mod 15251= 73

(0,1)
C1= 134^7 mod 15251= 2015
C2= 160^7 mod 15251= 10916
C3= 155^7 mod 15251= 11854

(0,2)
C1= 184^7 mod 15251=9244
C2= 201^7 mod 15251=12624
C3= 165^7 mod 15251=2669

(0,3)
C1= 150^7 mod 15251= 8908
C2= 176^7 mod 15251= 13632
C3= 131^7 mod 15251= 7521

(1,0)
C1= 94^7 mod 15251= 3243
C2= 120^7 mod 15251= 2347
C3= 75^7 mod 15251= 14844

(1,1)
C1= 171^7 mod 15251=6069
C2= 188^7 mod 15251=3327
C3= 152^7 mod 15251=11024

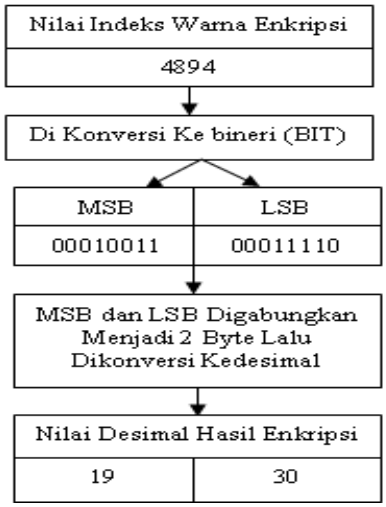
(1,2)

(1,3)

C1= 149^7 mod 15251=13764
C2= 151^7 mod 15251= 4530
C3= 114^7 mod 15251= 146
(2,0)
C1= 145^7 mod 15251=11041
C1= 138^7 mod 15251=8744
C1= 119^7 mod 15251=6310
(3,0)
C1= 62^7 mod 15251= 4302
C1= 64^7 mod 15251= 8022
C1= 27^7 mod 15251= 12574
(4,0)
C1= 118^7 mod 15251=1024
C2= 117^7 mod 15251=9978
C3= 97^7 mod 15251= 2604
(5,0)
C1= 136^7 mod 15251=3165
C2= 127^7 mod 15251=1821
C3= 118^7 mod 15251=1024

C1= 67^7 mod 15251= 14671
C2= 69^7 mod 15251= 8647
C3= 32^7 mod 15251= 13169
(2,1)
C1= 127^7 mod 15251=1821
C1= 129^7 mod 15251=8545
C1= 92^7 mod 15251= 1502
(3,1)
C1= 125^7 mod 15251=1228
C1= 118^7 mod 15251= 1024
C1= 99^7 mod 15251= 6033
(4,1)
C1= 99^7 mod 15251=6033
C2= 98^7 mod 15251=237
C3= 78^7 mod 15251=1107

Nilai enkripsi di atas tidak dapat langsung digunakan menjadi nilai indeks warna unuk enkripsi. Karena nilai diatas memiliki panjang 2 byte, sedangkan maksimal nilai indeks warna adalah 1 byte (0-255). Most significant byte dan least significant byte akan dibagi menjadi dua blok tiap blok memiliki nilai 1 byte yaitu 1 byte untuk most significant byte dan 1 byte atau 1 blok untuk least significant byte. Penjelasannya dapat dilihat pada bentuk gambar berikut:



Gambar 3 Representasi pembagian nilai enkripsi menjadi blok 8 bit / 1 byte

Hasil selengkapnya ditunjukan pada gambar 3 dengan cara yang sama.

3. Hasil enkripsi gambar (representasi dalam nilai desimal setiap piksel)

LSB

Piksel	0			1			2		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	30	254	73	223	132	78	36	80	139
1	204	64	97	171	43	252	181	255	16
2	164	178	0	79	199	113	33	40	166
3	29	97	222	174	86	30	172	0	145
4	0	250	44	145	237	83	93	29	0

MSB

Piksel	0			1			2		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	19	24	73	7	42	46	28	49	10
1	34	53	29	12	9	57	23	12	43
2	53	17	146	57	33	51	43	34	24
3	7	33	5	16	31	47	4	4	23
4	4	38	10	23	237	4	12	7	4

4. Simpan gambar terenkripsi ke media penyimpanan

3.3 Dekripsi Gambar

Gabungan nilai pixel LSB dan MSB, hasil penggabungan nya adalah sebagai berikut:

Piksel (0,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
30	19	254	24	73	73
4894		6389		73	

Piksel (0,1)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
223	7	132	42	78	46
2015		10916		11854	

Piksel (0,2)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
36	28	80	49	139	10
9244		12624		2669	

Piksel (0,3)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
204	34	64	53	97	29
8908		13632		7521	

Piksel (1,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
171	12	43	9	252	57
3243		2347		14844	

Piksel (1,1)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
181	23	255	12	16	43
6069		3327		11024	

Piksel (1,2)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
164	53	178	17	0	146
13764		146		14671	

Piksel (1,3)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
79	57	199	33	113	51
4530		8647		13169	

Piksel (2,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
33	43	40	34	166	24
11041		8744		6310	

Piksel (2,1)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB

29	7	97	33	222	5
1821		8545		1502	

Piksel (3,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
174	16	86	31	30	47
4302		8022		12574	

Piksel (3,1)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
172	4	0	4	145	23
11041		8744		6310	

Piksel (4,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
0	4	250	38	44	10
1024		9978		2604	

Piksel (4,1)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
145	23	237	237	83	4
6033		237		1107	

Piksel (5,0)

RED		GREEN		BLUE	
LSB	MSB	LSB	MSB	LSB	MSB
93	12	29	7	0	4
3165		1821		1024	

Untuk membuktikan apakah proses enkripsi sudah benar, maka proses dekripsi sesuai algoritma RSA haruslah menghasilkan nilai yang benar, dengan formula C1$= m1^{d}$ mod n.

(0,0)

C1= 4894^{2143} mod 15251= 173
C2= 6389^{2143} mod 15251= 199
C3= 73^{2143} mod 15251= 154

(0,1)

C1= 2015^{2143} mod 15251= 134
C2=10916^{2143} mod 15251=160
C3= 11854^{2143} mod 15251=155

(0,2)

C1= 9244^{2143} mod 15251=184
C2= 12624^{2143} mod 15251=201
C3= 2669^{2143} mod 15251=165

(0,3)

C1= 8908^{2143} mod 15251= 150
C2= 13632^{2143} mod 15251= 176
C3= 7521^{2143} mod 15251= 131

(1,0)

C1= 3243^{2143} mod 15251= 94
C2= 2347^{2143} mod 15251= 120
C3= 14844^{2143} mod 15251= 75

(1,1)

C1= 6069^{2143} mod 15251=171
C2= 3327^{2143} mod 15251=188
C3= 11024^{2143} mod 15251=152

(1,2)

C1= 13764^{2143} mod 15251=149
C2= 146^{2143} mod 15251= 151
C3= 14671^{2143} mod 15251= 114

(1,3)

C1= 4530^{2143} mod 15251=67
C2= 8647^{72143} mod 15251= 69
C3= 13169^{2143} mod 15251= 32

(2,0)

C1= 11041^{2143} mod 15251=145
C1= 8744^{2143} mod 15251=138
C1= 6310^{2143} mod 15251=119

(2,1)

C1= 1821^{2143} mod 15251=127
C1= 8545^{2143} mod 15251=129
C1= 1502^{2143} mod 15251= 92

(3,0)

C1= 4302^{2143} mod 15251= 62
C1= 8022^{2143} mod 15251= 64
C1= 12574^{2143} mod 15251= 27

(3,1)

C1= 1228^{2143} mod 15251=125
C1= 1024^{2143} mod 15251= 118
C1= 6033^{2143} mod 15251= 99

(4,0)

C1= 1024^{214a} mod 15251=118

C2= 9978^{214a} mod 15251=117

C3= 2604^{214a} mod 15251= 97

(4,1)

C1= 6033^{214a} mod 15251= 99

C2= 237^{214a} mod 15251= 98

C3= 1107^{214a} mod 15251=78

(5,0)

C1= 3165^{214a} mod 15251=136

C2= 1821^{214a} mod 15251=127

C3= 1024^{214a} mod 15251=118

4 Hasil Dekripsi Gambar

Piksel	0			1			2		
	RED	GREEN	BLUE	RED	GREEN	BLUE	RED	GREEN	BLUE
0	173	199	154	134	160	155	184	201	165
1	150	176	131	94	120	75	171	188	152
2	149	151	114	67	69	32	145	138	119
3	127	129	92	62	64	27	125	118	99
4	118	117	97	99	98	78	136	127	118

5. KESIMPULAN

Adapun kesimpulan yang didapat berdasarkan penelitian saat dilakukan pada pembahasan sebelumnya sebagai berikut:

1. Proses pengamanan citra bewarna menggunakan Algoritma RSA dalam membantu penulis agar dapat mengamankan data-data yang tidak perlu diketahui pihak-pihak lain. Dimana setiap citra dienkripsikan sebanyak dua kali (secara ganda) sehingga menghasilkan simbol yang berbeda dengan citra aslinya, dan akan kembali lagi kebentuk semula saat pengguna memasukkan kata kunci yang telah diterapkan.
2. Penerapan algoritma RSA pada citra bewarna 8 bit memang telah berhasil mengamankan gambar dari penelitian yang penulis lakukan.

DAFTAR PUSTAKA

[1] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.

[2] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab," *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017.

[3] M. A. I. Pakereng, Y. R. Beeh, and S. Endrawan, "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) Antara Waktu Proses dan Ukuran File Gambar."

[4] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[5] R. Sadikin, "Kriptografi untuk keamanan jaringan," *Penerbit Andi, Yogyakarta*, 2012.

[6] D. Email, A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk," vol. 3, no. 2, pp. 253–258, 2015.

[7] R. Sahara, H. Prastiawan, and A. Rohman, "Implementasi Keamanan SMS Dengan Algoritma RSA Pada Smartphone Android," *J. Ilm. FIFO*, vol. 9, no. 2, pp. 118–122, 2017.