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

Andro Alif Rakhman[1], Achmad Wahid Kurniawan[2]
[1,2]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131 - (024) 3517261
E-mail : androalif@rocketmail.com[1], wahid@dsn.dinus.ac.id[2]

Abstrak

Penggunaan informasi melalui media gambar atau citra mempunyai beberapa kelemahan, salah satunya adalah kemudahan melakukan manipulasi citra oleh pihak-pihak tertentu dengan bantuan teknologi yang berkembang sekarang ini. Upaya dalam peningkatan pengamanan pengiriman informasi melalui media gambar dan perlindungan atas hak cipta hasil karya media digital maka algoritma kriptografi dapat diterapkan untuk pengamanan citra tersebut.

Pada penelitian ini, menggunakan perpaduan algoritma Rivest Shamir Adleman (RSA) dan Vigenere Cipher untuk melakukan pengamanan citra. Citra yang akan digunakan yaitu file bitmap dengan kedalaman piksel 8 bit. Citra 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. Sedangkan untuk tahap pendekripsiannya dilakukan dengan menggunakan algoritma Vigenere Cipher terlebuh dahulu kemudian menggunakan algoritma kriptografi RSA. Selanjutnya dilakukan analisis pengaruh penerapan algoritma Rivest Shamir Adleman (RSA) dan Vigenere Cipher pada citra yang akan diamankan, meliputi analisis ruang kunci, analisis perubahan indeks warna, dan analisis waktu proses enkripsi dan deskripsi.Pengujian yang dilakukan untuk analisis tersebut, menggunakan citra berdimensi 3840 x 2160 piksel dan ukuran file 7,91 MB dan citra berdimensi 5012 x 2819 piksel dan ukuran file 13,4 MB. Analisis ruang kunci menunjukkan bahwa citra telah berhasil didekripsikan dan secara visual pola citra kembali ke bentuk semula tanpa mengalami cacat sedikitpun. Analisis perubahan indek warna, dilihat secara visual pada hasil palette warna membuktikan bahwa metode enkripsi yang dirancang telah berhasil digunakan untuk memperbaruhi nilai indeks warna citra asli. Sedangkan dari analisis waktu proses enkripsi dan deskripsi dapat disimpulkan Rata-rata lama waktu yang dibutuhkan untuk proses dekripsi lebih lama dibandingkan dengan lama waktu proses enkripsi.

Kata Kunci : *kriptografi, bitmap, rivest shamir adleman, vigenere cipher*

Abstract

Use of information through the images have several drawbacks, one of which is the ease of image manipulation by certain parties with the help of technology that is now developing. Efforts in increasing the security of the transmission of information through media images and the protection of copyright works, the digital media cryptographic algorithms can be implemented to safeguard the image. In this study, using a fusion algorithm of Rivest Shamir Adleman (RSA) and Vigenere Cipher to secure the image. The image that will be used is a bitmap file with 8-bit pixel depth. The image will be processed by encrypting the index value of RGB colors at each pixel using RSA cryptography algorithm first and then followed by using Vigenere Cipher algorithm. As for the description stage done using Vigenere Cipher then uses the RSA cryptography algorithm. Furthermore, the analysis of the effect of applying the algorithm Rivest Shamir Adleman (RSA) and Vigenere Cipher in the image that will be secured, includes analysis of key space, analysis of changes in the color index, and the analysis time and deskripsi. Encryption process testing is carried out for the analysis, using the image of dimension 3840 x 2160 pixels and a file size of 7.91 MB and the image dimensions 5012 x 2819 pixels and a file size of 13.4 MB. Analysis of key space indicates that the image has been

successfully described and visual pattern of the image back to its original shape without experiencing the slightest flaw. Analysis of changes in color index, seen visually on the results prove that the color palette designed encryption method has been successfully used to renew the original image color index value. While the analysis and description of the encryption processing time can be summed average length of time required for the decryption process longer than the length of time the encryption process.

Keywords : *cryptography, bitmap, rivest shamir adleman, vigenere cipher*

1. PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Salah satu usaha untuk mengamankan data 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. [1]

Penggunaan media informasi berupa gambar dari jaman dulu sudah sering digunakan. Bahkan dalam kehidupan sehari-hari pun erat kaitannya dengan media gambar. Akan tetapi, 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 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. Terlebih jika informasi berupa file gambar tersebut bersifat rahasia. Seperti data-data pribadi, dokumen kenegaraan, atau data medis rumah sakit [2].

Oleh karena itu penerapan teknologi kriptografi RSA dan *Vigenere Cipher* [3][4] ini diharapkan dapat membantu upaya dalam peningkatan pengamanan pengiriman informasi media gambar dan mempermudah perlindungan atas hak cipta hasil karya media digital.

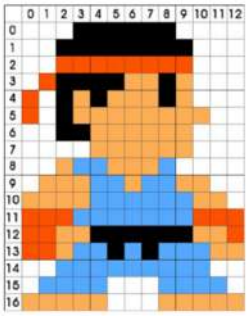
2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu mengkombinasikan algoritma kriptografi Rivest Shamir Adleman (RSA) dan *Vigenere Cipher* terhadap nilai indeks warna dari masing-masing piksel [5][6][7][8]. Enkripsi gambar dilakukan melalui perhitungan kriptografi RSA terlebih dahulu kemudian dilanjutkan dengan algoritma *Vigenere Cipher*. Sedangkan untuk tahap pendekripsiannya dilakukan dengan menggunakan algoritma *Vigenere Cipher* terlebuh dahulu kemudian menggunakan algoritma kriptografi RSA.

2.1 Tahap Pengenalan Citra

Karena 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 17. Representasi Bitmap 8 bit

Berdasarkan gambar 1, karena berbasis gambar 8 bit maka sistem warna yang digunakan adalah sistem *indexed color* yaitu sistem indeks pada warna. Sistem indeks warna adalah sebuah nilai numerik sederhana yang menentukan warna dari suatu obyek, sehingga tiap-tiap piksel yang diperoleh mewakili nilai indeks warna, seperti yang ditunjukkan pada gambar 2.

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 18. Nilai Indeks Warna Dari Bitmap Gambar 1.

2.2 Prosedur Enkripsi Gambar

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 1 dan Gambar 2. Nilai-nilai tersebut merupakan nilai indeks dari komponen warna merah (*Red*), hijau (*Green*), dan biru (*Blue*). Setelah diperoleh nilai indeks warna dari citra tersebut, kemudian menentukan sebuah kunci publik dan kunci privat dengan menggunakan algoritma RSA.

2.2.1 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 x 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 x 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)

2.2.2 Enkripsi RSA

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

Tabel 1 : Nilai indeks warna bitmap untuk proses enkripsi

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

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*) = (3233, 17) dengan rumus $y = a^e \bmod n$.

Tabel 2 : Nilai Hasil Enkripsi RSA

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

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*.

2.2.3 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 000-999. 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.

2.2.4 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 $s = (y + r_{1,2,3,4}) \bmod 1000$.

Tabel 3 : Nilai Hasil Enkripsi Vigenere Cipher

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

2.2.5 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.

Tabel 4 : Pembagian Nilai Enkripsi Menjadi Blok 8 Bit

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

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 berikut.

Tabel 5 : Nilai Indeks Warna Hasil Enkripsi

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

2.2.6 Prosedur Dekripsi 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.

2.2.7 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.

Tabel 6 : Gabungan 2 Nilai Suatu Piksel Menjadi 2 Byte

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	

2.2.8 Dekripsi *Vigenere Cipher*

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

Tabel 7 : Tabel dekripsi Vigenere Cipher

Dekripsi		
Nilai Enkripsi Vigenere (*s*)	$y = (s - r_{1,2,3,4})$ mod 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

2.2.9 Dekripsi Rivest Shamir Adleman (RSA)

Dalam proses dekripsi RSA digunakan kunci rahasia yang sudah ditentukan sejak awal perhitungan. Pasangan kunci rahasia $(n, d) = (3233, 2753)$ dengan rumus $a = y^d$ mod n. Untuk hasil lengkapnya ditunjukkan pada tabel berikut.

Table 8 : Tabel Dekripsi Nilai Indeks Warna

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

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

3. HASIL DAN PEMBAHASAN

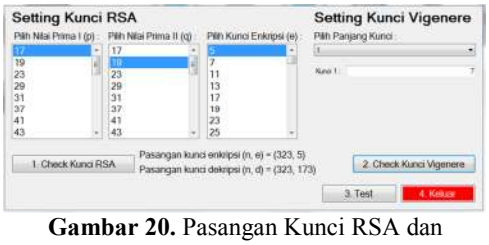
3.1 Kasus dan Hasil Pengujian

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 seperti yang ditunjukkan pada gambar di bawah ini.

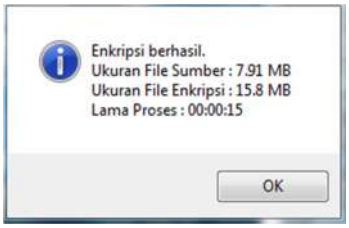
Gambar 19. Objek Pengujian Pertama

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

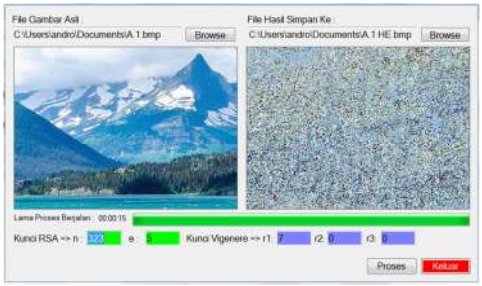


Gambar 20. Pasangan Kunci RSA dan *Vigenere Cipher* Pengujian Pertama

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



Gambar 21. Tampilan Proses Enkripsi Pengujian Pertama Berhasil



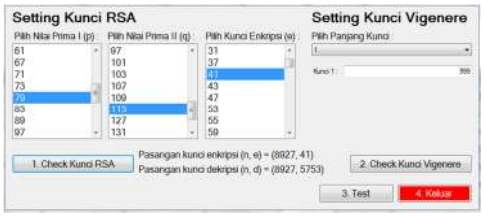
Gambar 22. Tampilan Form Enkripsi Pengujian Pertama

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

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

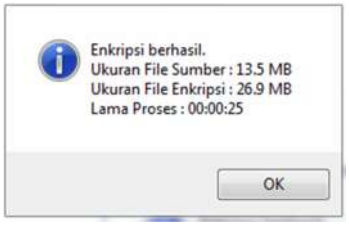
Gambar 23. Objek Pengujian Kedua

Pasangan kunci RSA dan Vigenere Cipher yang digunakan pada pengujian kedua dapat dilihat pada gambar berikut ini.

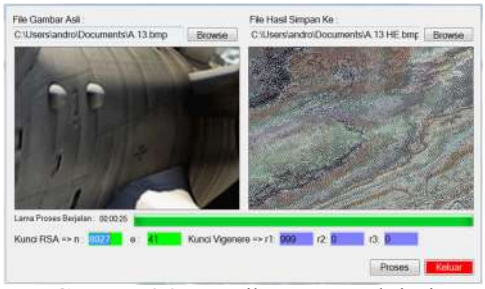


Gambar 24. Pasangan Kunci RSA dan Vigenere Cipher Pengujian Kedua

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

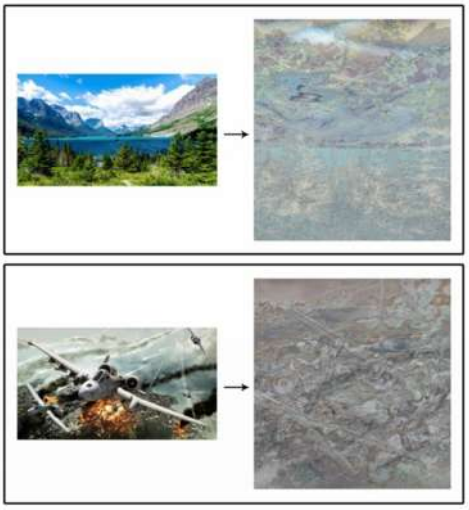


Gambar 25. Tampilan Proses Enkripsi Pengujian Kedua Berhasil



Gambar 26. Tampilan Form Enkripsi Pengujian Kedua

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



Gambar 27. Hasil perbandingan gambar sebelum dan sesudah dienkripsi.

Gambar di atas menunjukkan perbandingan gambar sebelum dan sesudah mengalami proses enkripsi.

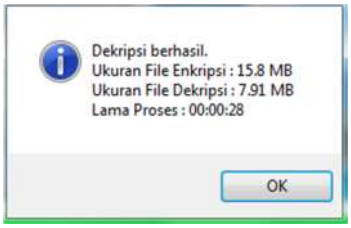
Pada pengujian pertama, citra asli memiliki dimensi file 3840 x 2160 piksel, setelah mengalami proses enkripsi dimensi citra berubah menjadi 3840 x 4320 piksel. Ukuran lebar gambar seteleh dienkripsi menjadi 2 kali lipat dari 2160 menjadi 4320.

Pada pengujian kedua, citra asli memiliki dimensi file 5012 x 2819 piksel, setelah mengalami proses enkripsi dimensi citra 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.

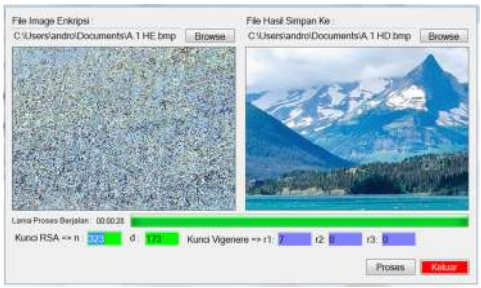
Untuk membuktikan kembali bahwa hasil enkripsi sudah benar, maka proses dekripsi dilakukan terhadap citra terenkripsi dan hasil percobaan yang didapat adalah citra terenkripsi akan kembali seperti semula. Dalam proses dekripsi citra, pasangan kunci rahasia harus sesuai dengan perhitungan saat membuat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

Mengacu pada pengujian enkripsi citra yang pertama, pasangan kunci RSA dan *Vigenere Cipher* yang telah terbentuk seperti pada gambar 4 menghasilkan nilai kunci rahasia RSA (323, 173) dan panjang kunci *Vigenere Cipher* yaitu 1 dengan nilai 7.



Gambar 28. Tampilan Proses Dekripsi Pengujian Pertama Berhasil

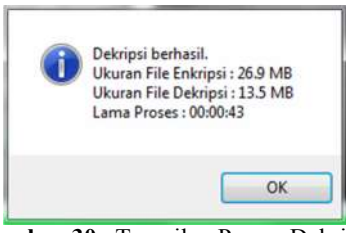
Dapat dilihat pada gambar di atas menunjukkan bahwa pengujian dekripsi citra pertama telah berhasil. Hasil yang diperoleh adalah ukuran file dekripsi citra telah kembali ke ukuran semula yaitu 7,91 MB dan lama waktu proses dekripsi yang dibutuhkan adalah 00:00:28.



Gambar 29. Tampilan Form Dekripsi Pengujian Pertama

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

Untuk pengujian kedua, pasangan kunci RSA dan *Vigenere Cipher* yang telah terbentuk seperti pada gambar 8 menghasilkan nilai kunci rahasia RSA (8927, 5753) dan panjang kunci *Vigenere Cipher* yaitu 1 dengan nilai 999.



Gambar 30 . Tampilan Proses Dekripsi Pengujian Kedua Berhasil

Dapat dilihat pada gambar 14 menunjukkan bahwa pengujian dekripsi citra kedua telah berhasil. Hasil yang diperoleh adalah ukuran file dekripsi citra telah kembali ke ukuran semula yaitu 13,5 MB dan lama waktu proses dekripsi yang dibutuhkan adalah 00:00:43

Gambar 31. Tampilan Form Dekripsi Pengujian Kedua

Gambar 15 menunjukkan perbandingan citra setelah mengalami proses enkripsi dan citra setelah mengalami proses dekripsi. Citra telah berhasil didekripsikan dan secara visual pola citra kembali ke bentuk semula tanpa mengalami cacat sedikitpun. Hal ini bisa dibuktikan dengan cara melihat dimensi citra yang kembali ke bentuk awal, yaitu 5012 x 2819 piksel dan ukuran file citra yaitu 13,4 MB.

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

3.2 Analisis Hasil Pengujian

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

3.2.1 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 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."

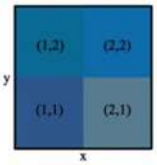
Analisa hasil pengujian dilihat dari perbandingan citra sebelum dan sesudah dilakukan proses enkripsi dan dekripsi dengan menggunakan metode algoritma kriptografi RSA dan *Vigenere Cipher*.

3.2.2 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 32. Objek pengujian pertama yang akan diteliti nilai indeks warnanya

Berdasarkan gambar 16, penulis mengambil beberapa *sample* nilai indeks sebanyak 2 x 2 piksel di dalam lingkaran berwarna kuning untuk mewakili citra secara keseluruhan yang akan dienkripsi.



Gambar 33. Sample Piksel 2x2

Untuk memudahkan pemberian koordinat piksel, maka penulis memberikan pengkodean nama piksel terhadap gambar 17 berdasarkan koordinat *x* dan *y*. Berikut adalah tabel nilai indeks warna potongan piksel di atas berdasarkan koordinat *x* dan *y* yang akan diteliti.

Tabel 9 : Nilai Indeks Warna Bitmap

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

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).

Tabel 10 : Nilai Hasil Enkripsi RSA

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

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.

Tabel 11 : Nilai Hasil Enkripsi Vigenere Cipher

Enkripsi		
Nilai Enkripsi RSA (*y*)	**$s = (y + r_{1,2,3,4}) \bmod 1000$**	**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

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.

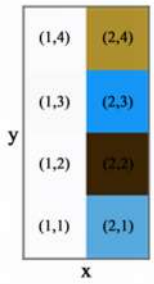
Table 12 : Pembagian nilai enkripsi menjadi blok 8 bit

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

Berikut ini adalah hasil perubahan nilai indeks warna dari masing-masing piksel setelah mengalami proses enkripsi.

Tabel 13 : Hasil Perubahan Nilai Indeks Warna Bitmap Setelah 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



Gambar 34 : Hasil Palette Warna Dari Nilai Indeks Warna Tabel 13

Secara visual, gambar 18 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, 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 pembahasan sebelumnya. Hasil lengkapnya ditunjukkan pada tabel berikut.

Tabel 14 : Gabungan 2 Nilai Piksel Menjadi 2 Byte

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	

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

Tabel 15 : Tabel Dekripsi Vigenere Cipher

Dekripsi		
Nilai Enkripsi Vigenere (*s*)	**$y = (s - r_{1,2,3,4}) \bmod 1000$**	**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

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.

Table 16 : Tabel Dekripsi Nilai Indeks Warna Semula

Dekripsi RSA		
Nilai Enkripsi RSA (*y*)	**$a = y^d \bmod n$**	**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

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

3.2.3 Analisis Waktu Proses Enkripsi dan Deskripsi

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 yang akan diproses, semakin lama waktu yang dibutuhkan untuk menyelesaikan proses tersebut. Sebaliknya, semakin kecil ukuran suatu file citra yang akan diproses, semakin singkat waktu yang dibutuhkan untuk menyelesaikan proses tersebut.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dalam jurnal ini telah dipaparkan hasil pengujian dan analisis penggunaan kombinasi algoritma RSA dan *Vigenere Cipher* dalam mengenkripsi dan mendekripsikan citra bitmap 8 bit. Hasil pengujian menunjukkan secara visual citra 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 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 asli. Semakin banyak variasi pola warna pada citra 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 bitmap 8 bit telah berhasil dengan baik. Sehingga konsep penggunaan algoritma kriptografi yang diusulkan layak digunakan untuk mengamankan data citra gambar.

4.2 Saran

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

1. Format citra yang digunakan dalam penelitian ini adalah bitmap 8 bit. Oleh karena itu, dalam pengembangan lebih lanjut bisa mengggunakan format citra 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 yang akan dienkripsi.
3. Citra hasil enkripsi pada penelitian ini menjadi lebih besar dari citra aslinya. Hal ini dikarenakan penambahan bit (*padding*). Oleh karena itu diperlukan suatu algoritma kompresi agar citra 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 dalam penelitian ini juga bisa dikombinasikan dengan algoritma steganografi atau watermarking. Sehingga citra yang dihasilkan nantinya bisa mencakup berbagai aspek keamanan.

DAFTAR PUSTAKA

[1] Zainal Arifin (2009), *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*, Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman.

[2] Chin-Chen Chang (2001), *A New Encryption Algorithm for Image Cryptosystems*, Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan.

[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] Didin Mukodim (2002), *Tinjauan Tentang Enkripsi Dan Dekripsi Suatu Teknik Pengamanan Data Dengan Penyandian RSA*, Universitas Gunadarma.

[6] Ivan Wibowo (2009), *Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle*, Teknik Informatika, Universitas Kristen Duta Wacana.

[7] 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.

[8] 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.