

ANALISIS HASIL ENKRIPSI DAN DEKRIPSI CITRA RGB 24 BIT MENGUNAKAN ALGORITMA *ELGAMAL* BERDASARKAN UKURAN, DAN WARNA CITRA ASLI

ANALYSIS OF THE RESULT OF ENCRYPTION AND DECRYPTION OF 24-BIT RGB IMAGE USING ELGAMAL ALGORITHM BASED ON ORIGINAL IMAGE SIZE AND COLOR

Hendrawaty¹ Desita RiaYusian TB²Munawir³

¹Politeknik Negeri Lhokseumawe

²Universitas Ubudiyah Indonesia

³Universitas Samudra

Jln. B.Aceh Medan Km.280 Buketrata, Lhokseumawe 24301

Koresponding Penulis: hendrawaty@pnl.ac.id

Abstrak— Internet dan perkembangan teknologi informasi yang pesat, membawa pengaruh yang besar dalam kehidupan manusia dewasa ini, baik di rumah, di kantor-kantor maupun di sekolah-sekolah. Pengiriman data lewat internet sudah menjadi hal yang dibutuhkan dan penting. Oleh karena itu pengamanan pada data yang dikirim menjadi suatu hal yang tidak dapat disepelekan. Selain teks, gambar termasuk salah satu jenis data yang banyak dikirimkan melalui internet. Gambar yang dikirim lewat internet bisa saja di curi, dimodifikasi, dan dimanfaatkan oleh pihak-pihak yang tidak diinginkan, sehingga dapat merugikan pemiliknya. Dewasa ini terdapat beberapa aplikasi kriptografi yang dibangun untuk mengamankan data gambar. Aplikasi kriptografi tersebut menerapkan algoritma-algoritma kriptografi untuk pengamanan datanya. ElGamal merupakan salah satu algoritma kriptografi yang digunakan pada aplikasi kriptografi. Penelitian ini membahas tentang analisis hasil enkripsi dan dekripsi citra RGB 24 bit yang dihasilkan oleh suatu aplikasi kriptografi yang menerapkan algoritma ElGamal untuk proses enkripsi dan dekripsinya. Hasil penelitian menunjukkan bahwa ukuran citra yang dienkripsi berpengaruh kepada proses dan hasil enkripsi, dimana citra yang memiliki ukuran lebih besar membutuhkan waktu enkripsi lebih lama dibandingkan dengan citra yang berukuran lebih kecil. Dan citra hasil enkripsi (*cipherimage*) yang dihasilkan memiliki ukuran lebih besar dua kali lipat dari citra aslinya. Warna dan isi objek dalam citra juga memiliki pengaruh terhadap hasil enkripsi, dimana Untuk citra dengan warna dan objek tertentu hasil enkripsinya tidak teracak secara sempurna. Pengiriman citra hasil enkripsi (*Cipherimage*) lewat internet dalam hal ini melalui email, tidak berpengaruh pada hasil dekripsinya, dimana *cipherimage* tersebut tetap dapat di dekripsi dengan hasil yang sempurna sesuai dengan citra aslinya.

Kata kunci: Hasil enkripsi, Hasil dekripsi, Algoritma ElGamal

Abstract— The internet and the rapid development of information technology have a great influence on human life today, both at home, in offices and in schools. Sending data via the internet has become a necessary and important thing. Therefore, the security of the data sent is something that cannot be underestimated. In addition to text, images are one of the types of data that are sent via the internet. Images sent via the internet can be stolen, modified, and used by unwanted parties, so that it can harm the owner. Today there are several cryptographic applications that are built to secure image data. The cryptography application applies cryptographic algorithms for data security. ElGamal is one of the cryptographic algorithms used in cryptography applications. This study discusses the analysis of the results of encryption and decryption of 24-bit images generated by a cryptographic application that applies the ElGamal algorithm for the encryption and decryption process. The results showed that the size of the encrypted image had an effect on the encryption process and results, where the larger size image required a longer encryption time than the smaller image. And the resulting encrypted image (*cipherimage*) has a size twice as large as the original image. The color and content of objects in the image also have an influence on the results of encryption, where for images with certain colors and objects the encryption results are not perfectly randomized. Sending the encrypted image (*Cipherimage*) via the internet, in this case via email, has no effect on the decryption result, where the *cipherimage* can still be decrypted with perfect results according to the original image.

Keywords: Encryption results, Decryption results, ElGamal algorithm

I. PENDAHULUAN

Internet dan perkembangan teknologi informasi yang pesat, membawa pengaruh yang besar dalam kehidupan manusia dewasa ini, baik di rumah, di kantor-kantor maupun di sekolah-sekolah. Pengiriman data lewat internet sudah menjadi hal yang dibutuhkan dan penting. Setiap harinya banyak data yang dikirimkan lewat internet. Selain data teks, data gambar juga termasuk data yang banyak dikirimkan lewat internet. Pengiriman data gambar lewat internet mempunyai resiko keamanan tersendiri.

Gambar atau Citra yang dikirim lewat internet bisa saja dicuri, dimodifikasi, dan dimanfaatkan dan disalah gunakan oleh pihak-pihak yang tidak berhak, sehingga dapat merugikan pemiliknya. Oleh karena itu pengamanan data gambar yang dikirim melalui internet menjadi suatu hal yang tidak dapat disepelekan. Dewasa ini terdapat beberapa aplikasi kriptografi yang dibangun untuk mengamankan data gambar. Aplikasi kriptografi tersebut menerapkan algoritma-algoritma kriptografi untuk pengamanan datanya. ElGamal merupakan salah satu algoritma kriptografi yang digunakan pada aplikasi kriptografi tersebut. penelitian ini membahas tentang analisis hasil enkripsi dan dekripsi Citra RGB 24 bit yang dihasilkan oleh suatu aplikasi kriptografi berbasis dekstop yang menerapkan algoritma ElGamal untuk proses enkripsi dan dekripsinya. Penelitian ini dilakukan untuk mengetahui seberapa baik hasil enkripsi dan dekripsi yang dihasilkan oleh aplikasi kriptografi ElGamal dalam mengamankan Citra RGB 24 bit dengan format JPG/JPEG.

II. STUDI PUSTAKA

A. Algoritma Kriptografi ElGamal

Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*)[4]. Algoritma ElGamal dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada mulanya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi. Algoritma *ElGamal* merupakan jenis algoritma asimetris karena menggunakan kunci yang berbeda untuk proses enkripsi dan proses dekripsi.

Sistem kriptografi ElGamal dibangun berdasarkan masalah logaritma diskrit. Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Besaran-besaran yang digunakan dalam algoritma ElGamal yaitu:

- 1. p bilangan prima (tidak rahasia)
- 2. Bilangan acak, g ($g < p$) (tidak rahasia)
- 3. Bilangan acak, x ($x < p$) (kunci privat) (rahasia)
- 4. $y = g^x \text{ mod } p$ (kunci publik) (tidak rahasia)
- 5. m (*plainteks*) (rahasia)
- 6. a dan b (*chipherteks*) (tidak rahasia)

B. Proses Pembangkitan Kunci

Algoritma *ElGamal* memerlukan sepasang kunci yang dibangkitkan dengan memilih bagian prima p dan dua bilangan acak (*random*) g dan x , dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan 1.

$$y = g^x \text{ mod } p \tag{1}$$

Dari persamaan tersebut nilai y , g dan p merupakan pasangan kunci privat.

C. Proses Enkripsi

Proses enkripsi dilakukan dengan memilih bilangan acak k yang berada dalam himpunan $1 \leq k \leq p-2$. Setiap blok *plaintext* m dengan persamaan:

$$a = g^k \text{ mod } p \tag{2}$$

$$b = y^k m \text{ mod } p \tag{3}$$

D. Proses Dekripsi

Proses dekripsi menggunakan kunci privat x dan p untuk mendekripsikan a dan b menjadi *plaintext* m dengan persamaan:

$$(ax)^{-1} = p^{p-x-1} \text{ mod } p \tag{4}$$

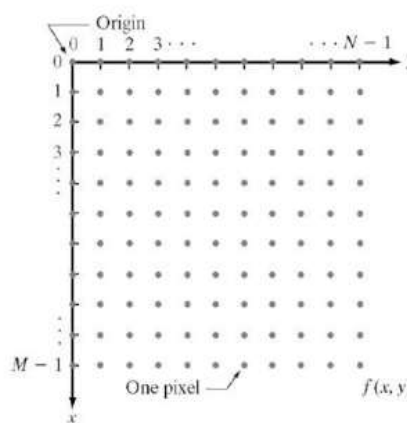
$$m = b * a^x \text{ mod } p \tag{5}$$

sehingga *plaintext* dapat ditemukan kembali dari pasangan *chiphertext* a dan b .

E. Citra Digital

Menurut Darma Putra [8], Secara umum pengolahan citra digital menunjuk pada pemrosesan gambar 2 dimensi menggunakan komputer. Citra digital merupakan sebuah larik (*array*) yang berisi nilai-nilai real maupun kompleks yang direpresentasikan dengan deretan bit tertentu.

Sebuah citra didefinisikan sebagai fungsi $f(x,y)$ berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial dan amplitudo f di titik koordinat(x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut. Pada Gambar 1 berikut menunjukkan posisi koordinat pada citra digital.



Gambar 1. Koordinat citra digital (sumber: buku pengolahan citra digital,2010)

F. Resolusi Pixel

Menurut Darma Putra [8], Resolusi piksel merupakan perhitungan jumlah piksel dalam sebuah citra digital. Sebuah citra memiliki resolusi $M \times N$ yang mana M sebagai lebar dan N sebagai tinggi. Dalam pengertian lainnya yaitu hasil perkalian jumlah piksel lebar dan tingginya dan kemudian dibagi dengan 1 juta. Jenis resolusi ini sering dijumpai pada kamera digital. Sebagai contoh sebuah citra memiliki lebar 1024 dan tinggi yaitu 768 maka akan memiliki total piksel sebesar $2048 \times 1536 = 3.145.728$, maka apabila dibagi dengan 1 juta maka akan menghasilkan 3,1 dan satuannya yaitu mega pixel.

Ada perhitungan lainnya yang menyatakan dalam satuan piksel per inci. Satuan ini menyatakan banyaknya piksel yang berada pada panjang 1 inci baris pada citra.

G. Citra 24-Bit

Ada total 16.777.216 variasi warna berasal dari setiap citra warna 24 bit yang mana variasi ini sudah cukup untuk memvisualisasikan seluruh warna yang dapat dilihat pada penglihatan manusia yang mana manusia hanya dapat membedakan 10 juta warna saja. Setiap 1 *byte* dari informasi *pixel* yang mana 1 *byte* mewakili 8 bit mewakili 3 warna yaitu Merah, Hijau dan Biru (RGB) yang mana 8 bit pertama menyimpan warna biru, kemudian diikuti dengan warna hijau dan 8 bit terakhir menyimpan warna merah.

H. Format File Citra JPEG/JPG

Format file citra digunakan dalam menyimpan file gambar dan setiap format memiliki jenis dan karakteristik masing-masing. JPEG/JPG (*Joint Photographic Experts Group*) adalah format yang umum digunakan saat ini khususnya pada kamera digital. Format ini digunakan untuk menyimpan citra hasil kompresi yang mana bersifat *lossy compression* yang dapat menyebabkan kualitas gambar menurun dan dapat menghilangkan data. Meskipun dapat menurunkan kualitas gambar, penurunan tersebut hampir tidak dapat terlihat secara kasat mata. File JPG cocok digunakan untuk gambar yang memiliki banyak warna, misalnya foto wajah dan pemandangan.

III. METODE

A. Rancangan Pengujian Citra pada Proses Enkripsi

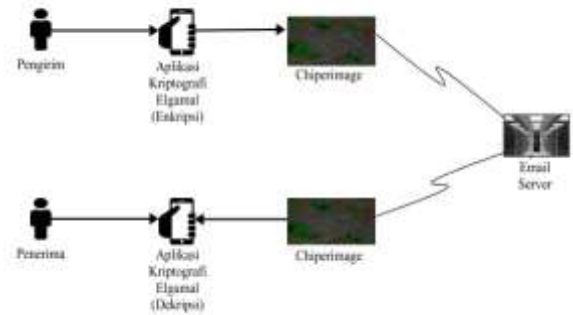
Perancangan Pengujian Enkripsi Citra RGB 24 bit (dengan format JPG/JPEG) menggunakan aplikasi kriptografi ElGamal pada penelitian ini terdiri dari:

1. Pengujian Enkripsi citra RGB 24 bit berdasarkan Ukuran Citra asli. Pada pengujian ini dilakukan enkripsi beberapa citra RGB 24 bit dengan ukuran yang bervariasi. Ukuran citra asli yang bervariasi tersebut dimaksudkan untuk melihat pengaruh ukuran citra yang di-enkripsi terhadap hasil enkripsi
2. Pengujian Enkripsi citra berdasarkan warna dan isi objek dalam citra. Pada pengujian ini dilakukan enkripsi beberapa citra RGB 24 bit dengan warna dan isi objek dalam citra yang bervariasi. Warna dan isi objek yang bervariasi pada citra asli tersebut dimaksudkan untuk melihat pengaruhnya pada hasil enkripsi.

B. Perancangan Pengujian Citra Pada Proses Dekripsi

Perancangan Pengujian Dekripsi *Cipherimage* menggunakan aplikasi kriptografi ElGamal pada penelitian ini terdiri dari:

1. Pengujian Dekripsi *cipherimage* berdasarkan Ukuran *cipherimage*. Pada pengujian ini dilakukan dekripsi terhadap beberapa *cipherimage* yang dihasilkan oleh proses pengujian enkripsi sebelumnya. Pengujian ini bertujuan untuk melihat keberhasilan dan perubahan citra pada hasil dekripsi,
2. Pengujian Dekripsi beberapa *cipherimage* yang dikirimkan melalui email. Pengujian ini dimaksudkan untuk melihat pengaruh *cipherimage* yang dikirimkan lewat internet terhadap hasil dekripsi. Gambar 2 memperlihatkan ilustrasi pengujian dekripsi *cipherimage* yang dikirim lewat email.









Gambar 2. Ilustrasi pengujian *cipherimage* yang dikirim lewat email



IV. HASIL DAN PEMBAHASAN

A. Hasil Pengujian Enkripsi Berdasarkan Ukuran Citra Asli.

Hasil Pengujian Enkripsi citra RGB 24 bit (dengan format JPG/JPEG), menggunakan aplikasi kriptografi ElGamal berdasarkan ukuran citra asli diperlihatkan pada Tabel 1.

Tabel 1. Hasil enkripsi berdasarkan ukuran citra asli

No.	Citra Asli (Plainimage)	Hasil Enkripsi (cipherimage)	Waktu Enkripsi (Menit)
1.	 1024x768 pixel 297 Kb	 2048x1536 pixel 3,26 Mb	09:15
2.	 024x768 pixel 297 Kb	 1640x1230 pixel 2,19 Mb	04:27
3.	 615x461 pixel 131 Kb	 1230x922 pixel 1,24 Mb	02:18

4.			01:28
	512x384 pixel 103 Kb	1024x768 pixel 880 Kb	








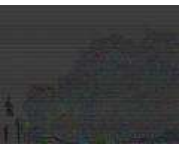
Dari tabel 1 diatas dianalisis bahwa ukuran citra sangat berpengaruh dalam proses enkripsi. Suatu citra yang memiliki ukuran yang besar (1024x768 piksel atau 27x20 cm) membutuhkan waktu yang lebih lama untuk enkripsi yaitu 09:15 menit, dibandingkan dengan citra yang memiliki ukuran yang lebih kecil (512x384 piksel atau 14x10 cm) dengan waktu enkripsi 01:28. Hal tersebut dikarenakan cara kerja algoritma ElGamal yaitu memproses citra per blok pikselnya. Citra yang ukurannya besar memiliki lebih banyak blok-blok piksel, sehingga semakin banyak blok-blok yang diproses maka semakin lama sistem untuk melakukan proses enkripsi.





Dari hasil pada Tabel 1 juga dapat dilihat bahwa ukuran citra asli 1024x768 pixel berubah menjadi 2048x1536 pixel setelah dienkripsi. Ukuran citra hasil enkripsi (*cipherimage*) menjadi dua kali lipat dibandingkan dengan ukuran citra aslinya (*plainimage*). Hal ini dikarenakan citra yang telah dienkripsi menggunakan algoritma ElGamal akan menghasilkan piksel baru yang dihasilkan dari perhitungan antara nilai piksel dengan nilai kunci.

B. Hasil pengujian Enkripsi Citra Berdasarkan Warna dan Isi Objek dalam Citra.

Tabel 2 memperlihatkan hasil pengujian enkripsi dari beberapa citra.

Tabel 2. Hasil enkripsi berdasarkan warna dan isi objek

No	Citra Asli (<i>Plainimage</i>)	Hasil Enkripsi (<i>cipherimage</i>)
1.		
2.		
3.		
4.		








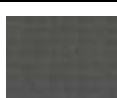




5.		
6.		

Dari tabel 2 dapat dianalisis bahwa warna citra dan objek pada citra juga dapat mempengaruhi hasil enkripsi, hal ini dapat dilihat pada hasil enkripsi (*cipherimage*) nomor 3, 4, 5, dan 6. Hasil enkripsi dari citra nomor 3 dan 4, yang memiliki warna abu-abu dan putih masih sedikit terlihat motif dari citra aslinya. Kemudian Hasil enkripsi dari gambar nomor 5 dan 6, yang memiliki warna orange dan merah terlihat lebih jelas motif citra aslinya.

C. Hasil Pengujian Dekripsi Berdasarkan Ukuran Citra.

Hasil Pengujian dekripsi dilakukan terhadap beberapa *chiperimage*. *Cipherimage* yang didekripsi memiliki ukuran yang bervariasi. Hasil Pengujian dilakukan dengan menggunakan aplikasi kriptografi ElGamal. Hasil pengujian diperlihatkan pada Tabel 3.

Tabel 3. Hasil Dekripsi Berdasarkan Ukuran Gambar

No.	Citra Asli	Hasil Enkripsi	Hasil Dekripsi	Waktu Dekripsi (Menit)
1.	 1024x768 297 Kb	 2048x1536 3,26 Mb	 1024x768 1,96 Mb	08:40
2.	 820x615 200 Kb	 1640x1230 2,19 Mb	 820x615 1,27 Mb	03:19
3.	 615x461 131 Kb	 1230x922 1,24 Mb	 615x461 745 Kb	02:10
4.	 512x384 103 Kb	 1024x768 880 Kb	 512x384 525 Kb	01:16

Dari tabel 3 dianalisis bahwa ukuran *cipherimage* berpengaruh dalam proses dekripsi. Suatu *cipherimage* yang memiliki ukuran yang besar membutuhkan waktu yang lebih lama untuk dekripsi dibandingkan dengan *cipherimage* yang memiliki ukuran yang lebih kecil. Hal tersebut dikarenakan cara kerja algoritma ElGamal yaitu memproses citra per blok pikselnya. *chipherimage* yang ukurannya besar memiliki lebih banyak blok-blok pikselnya, sehingga semakin banyak blok-blok yang diproses maka semakin lama sistem untuk melakukan proses dekripsi.











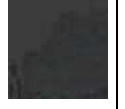

Selain hal itu, dapat dilihat bahwa ukuran citra hasil dekripsi menjadi lebih kecil dibandingkan dengan ukuran *cipherimage*. Hal ini dikarenakan pada proses dekripsi menggunakan algoritma ElGamal terjadi pengurangan piksel pada *cipherimage*.

Dapat dilihat juga bahwa warna dan isi objek pada citra hasil dekripsi sama dengan citra aslinya, dan ukuran citra hasil dekripsi hampir sama dengan ukuran citra aslinya.

D. Hasil Pengujian Dekripsi Cipherimage yang dikirim Lewat email

Hasil Pengujian dekripsi dilakukan terhadap beberapa *chipherimage* yang telah mengalami pengiriman lewat internet dalam hal ini email. Pengujian dilakukan dengan menggunakan aplikasi kriptografi ElGamal. Tabel 1. memperlihatkan hasil dekripsi *cipherimage* dari email.

Tabel 4. Hasil Dekripsi cipherimage dari email

No	Citra Asli	<i>cipherimage</i>	Citra Ouput	Keterangan
1				Gambar berhasil didekripsi
2				Gambar berhasil didekripsi
3				Gambar berhasil didekripsi
4				Gambar berhasil didekripsi

Dari tabel 4 dapat dilihat bahwa *cipherimage* awalnya

dikirim ke email seperti yang tampak pada ilustrasi perancangan Gambar 2. Kemudian *cipherimage* tersebut diunduh dan didekripsi dengan menggunakan aplikasi kriptografi ElGamal. Hasil dekripsi menunjukkan bahwa semua *cipherimage* yang telah mengalami proses pengiriman melalui email, tetap dapat dikembalikan seperti citra aslinya. Dengan demikian dapat dikatakan bahwa pengiriman *cipherimage* melalui email tidak mempengaruhi hasil dekripsi dari *cipherimage* tersebut.

V. KESIMPULAN

Berdasarkan hasil seluruh tahapan penelitian yang dilakukan pada analisis hasil enkripsi dan dekripsi citra menggunakan algoritma ElGamal dapat disimpulkan sebagai berikut:

1. Ukuran citra yang dienkripsi memiliki pengaruh yang berarti pada proses enkripsi, dimana semakin besar ukuran citra yang dienkripsi maka akan semakin lama waktu yang dibutuhkan untuk proses enkripsinya. Demikian juga halnya dengan proses dekripsi.
2. Ukuran citra hasil enkripsi (*cipherimage*) lebih besar dua kali dibandingkan dengan citra aslinya.
3. Warna dan isi objek pada gambar memiliki pengaruh yang berarti pada hasil enkripsi (*cipherimage*), dimana pada beberapa hasil enkripsi masih dapat terlihat bayangan dari citra aslinya (tidak teracak secara sempurna)
4. Pengiriman *cipherimage* melalui internet (email) tidak mempengaruhi hasil dekripsi. *cipherimage* tetap dapat dikembalikan seperti tampilan citra aslinya.

REFERENSI

- [1] D. Ariyus, *Pengantar Ilmu Kriptografi*, Penerbit Andi Jogjakarta, Indonesia, 2008.
- [2] S. Dharwiyanti, "Pengantar Unified Modeling Language (UML)". Ilmu Komputer, 2013.
- [3] A. Ihsan, "Implementasi Kombinasi Rivest Shamir Adleman (RSA) dan ElGamal dalam Penyandian Citra Bitmap," (*Tugas Akhir Mahasiswa Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara*), 2015.
- [4] R.A. Mollin, *An Introduction to Cryptography, Second Edition*. Taylor & Francis group, LLC : Boca Raton, USA, 2007.
- [5] R. Munir, *Kriptografi*, Bandung: Informatika, 2006.
- [6] S. Lubis, "Kriptografi Kunci Publik Algoritma ElGamal dengan Metode The Sieve Of Eratosthenes untuk Pembangkitan Bilangan Prima," (*Tugas Akhir Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara.*), 2012.
- [7] R. D. Purba, "Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm," *Medan : STMIK MIKROSKIL*.
- [8] D. Putra, *Pengolahan Citra Digital*. Yogyakarta: Andi, 2010.
- [9] E. Setyaningsih, "Penyandian Citra Menggunakan Metode Playfair Cipher," *Yogyakarta : Institut Sains & Teknologi AKPRIND Yogyakarta*.
- [10] T. Sutoyo. *Teori Pengolahan Citra Digital*, Yogyakarta: Andi, 2009.