IMPLEMENTASI KRIPTOGRAFI GAMBAR MENGGUNAKAN KOMBINASI ALGORITMA ELGAMAL DAN MODE OPERASI ECB (ELECTRONIC CODE BOOK)

Delva Rizal[1], T. Sutojo[2], Yuniarsi Rahayu[3]
[1,2,3]Jurusan Teknik Informatika, Fakultas Ilmu Komputer Universitas Dian Nuswatoro, Semarang
E-mail: delvarizal@gmail.com[1], tsutojo@gmail.com[2], yuniarsi.rahayu@dsn.dinus.ac.id[3]

Abstrak

Studio foto Aura photography merupakan suatu usaha yang bergerak di berbagai bidang seperti studio foto, fotocopy dan warnet. Studio ini memiliki satu komputer server dan delapan komputer client (warnet), dimana komputer server digunakan untuk menyimpan berbagai file penting, khususnya file gambar berekstensi .jpg dan .jpeg. Namun penggunaan komputer server tidak hanya karyawan saja, sehingga dalam pengaksesan data penting yang disimpan mudah diakses oleh orang lain yang tidak memiliki hak atas data tersebut. Oleh karena itu, untuk mengamankan file tersebut dibutuhkan pemanfaatan kriptografi dengan mengkombinasikan algoritma Elgamal dan mode operasi ECB dalam melakukan enkripsi dan dekripsi. Penelitian ini memilih kedua algoritma tersebut karena Elgamal merupakan algoritma asimetris serta menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit sedangkan ECB adalah mode operasi yang digunakan dengan kemampuan dekripsi dan enkripsi yang tepat. Sehingga dalam menggunakan kedua algoritma ini dapat memperkuat pengamanan file gambar dan menyulitkan kriptanalis dalam memecahkan file yang terenkripsi. Namun untuk file gambar yang sudah diserang seperti penambahan Brightness atau contrass, noise, blurring dan cropping tidak dapat di dekripsi karena intesitas nilai piksel pada chipertext berubah. Hasil pengujian dari gambar sebelum enkripsi dan sesudah enkripsi dekripsi yaitu MSE 0 dan PSNR inf.

Kata kunci: *Kriptografi, Elgamal, ECB, File Gambar.*

Abstract

Aura photo studio photography is a business engaged in various fields such as photo studio, photocopy and Internet cafe. The studio has a computer server and eight computer client (cafe), wherein the computer server used to store various important files, particularly image file extension .jpg and .jpeg. However, the use of a computer server not only employees only, so in accessing critical data stored easily accessed by others who do not have rights to the data. Therefore, to secure the files necessary to combine the use of cryptographic algorithms and modes of operation ECB ElGamal in encryption and decryption. This study chose the latter because ElGamal algorithm is asymmetric algorithms and key strength focuses on solving the discrete logarithm problem while the ECB is a mode of operation that is used by the decryption and encryption capability right. So that in using two algorithms can strengthen the security of image files and complicate cryptanalyst in solving the encrypted files. But for the images file that has been attacked like Brightness or contrass addition, noise, blurring and cropping can not be decrypted because the intensity of the pixel values of the ciphertext changed. The results from the image before encryption and after decryption encryption that MSE PSNR 0 and inf.

Keywords: *Cryptography, Elgamal, ECB, Images File*

1. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi dan komunikasi, banyak pekerjaan yang dapat diselesaikan dengan cepat dan efisien salah satunya adalah dengan menggunakan koneksi internet. Namun tidak semua dengan kecanggihan yang dimiliki oleh teknologi sekarang ini memberikan dampak yang positif bagi kalangan pengguna. Dampak negatif yang bisa terjadi adalah penyadapan data atau pencurian data. Informasi ada yang bersifat umum dan ada yang bersifat rahasia. Bentuk informasipun sangat banyak seperti teks, gambar, suara, video, dan lain sebagainya. Dengan kemajuan teknologi sekarang ini, diperlukan suatu usaha keamanan yang ketat supaya data atau informasi digital tidak dapat dibaca dan dipergunakan oleh orang yang tidak bertanggung jawab. Teknik pengamanan data tersebut dikenal dengan istilah kriptografi.

Algoritma kriptografi secara umum ada dua tipe berdasarkan kuncinya yaitu algoritma simetris dan algoritma asimetris. Algoritma yang memiliki kunci enkripsi dan dekripsi yang sama disebut dengan algoritma simetris. Sedangkan algoritma asimetris mempunyai dua buah kunci yaitu kunci publik dan kunci pribadi dimana kunci publik digunakan untuk melakukan enkripsi sedangkan kunci pribadi untuk proses dekripsi. Dalam algoritma kunci asimetris ini, kunci publik adalah kunci yang didistribusikan yang tidak diperlukan kerahasiannya sedangkan kunci pribadi adalah kunci yang disimpan atau tidak didistribusikan. Setiap orang yang mempunyai kunci publik dapat melakukan proses enkripsi tetapi hasil dari enkripsi hanya bisa dibuka atau dibaca oleh orang yang memiliki kunci pribadi [1].

Dalam kriptografi, banyak terdapat ekstensi file yang akan diproses. Salah satu jenis file adalah gambar. kriptografi gambar merupakan suatu teknik yang umum yang digunakan dalam melindungi citra dari suatu pengaksesan yang dilakukan secara ilegal. Enkripsi citra adalah suatu proses untuk mengubah citra kedalam bentuk lain yang tidak dapat dibaca secara visual dengan menggunakan suatu kunci. Dengan kunci yang sama, citra yang sudah terenkripsi dapat dikembalikan lagi atau didekripsi menjadi bentuk semula [2].

Terdapat banyak algoritma dalam kriptografi yang digunakan untuk memproses file gambar. Dalam penelitian ini algoritma yang dipakai adalah Elgamal dan ECB (*Electronic Code Book*). Penelitian terdahulu menggunakan algoritma elgamal [3], mengenai aplikasi kriptografi elgamal untuk pengamanan file citra yang menjelaskan bahwa salah satu algoritma kriptografi kunci asimetris yang menggunakan sepasang kunci yang berbeda, satu kunci enkripsi dan satu kunci dekripsi. Hasil dari aplikasi ini mampu mengenkripsi file citra tipe bitmap dengan format piksel 24 bit. Citra yang dihasilkan berekstensi "Este".

Penelitian teori *chaos* pada kriptografi yang menggunakan algoritma stream cipher dan ECB [4], mengenai aplikasi keamanan teks yang menjelaskan bahwa Teori *Chaos* dengan *Logistic Map* mampu membangkitkan kunci secara acak dan panjang. Kemudian kunci tersebut diterapkan pada algoritma *Stream Cipher* dan ECB. Dengan teori *Chaos* tersebut akan dihasilkan kunci

yang acak dan panjang kunci sama dengan panjang plainteks pada *Stream Cipher*. Sedangkan pada ECB akan menambah jumlah panjang kunci yang acak sehingga dapat menutup kelemahan. Hasil dari penelitian ini dapat mempermudah dalam mengingat kunci yang acak dan segaligus panjang.

Dalam penelitian ini penulis mencoba untuk mengkombinasikan algoritma Elgamal dengan mode operasi ECB. Pengimplementasian algoritma Elgamal dan mode operasi ECB ini ditujukan pada Studio Foto Aura P*hotography*. Studio Foto Aura *photography* adalah suatu usaha yang bergerak diberbagai dalam bidang seperti studio foto, fotocopy dan warnet. Studio ini memiliki satu komputer *server* dan delapan komputer *client* (warnet) dimana komputer server tersebut juga dijadikan sebagai komputer yang menyimpan berbagai file penting, khusunya di file gambar atau foto. Dalam kegiatannya sehari – hari komputer ini sering digunakan oleh seorang karyawan yang menjaga warnet atau fotocopy sehingga dalam pengaksesan data penting yang disimpan mudah diakses oleh karyawan atau orang lain yang tidak memiliki hak atas data – data tersebut. Sebelumnya pada studio foto ini pernah terjadi kasus perubahan data dan penghapusan data gambar yang dilakukan oleh karyawan dan orang lain (teman) yang menggunakan komputer di studio foto ini. Untuk meminimalisir terjadinya kesalahan yang akan datang seperti perubahan data, penghapusan data, atau pencurian data, maka perlunya suatu program aplikasi yang dapat melindungi file gambar atau foto tersebut mengingat komputer yang bersifat multiuser ini tetap terjaga integritas datanya dari pihak yang tidak bertanggung jawab atau yang tidak berhak atas data – data yang ada dikomputer tersebut.

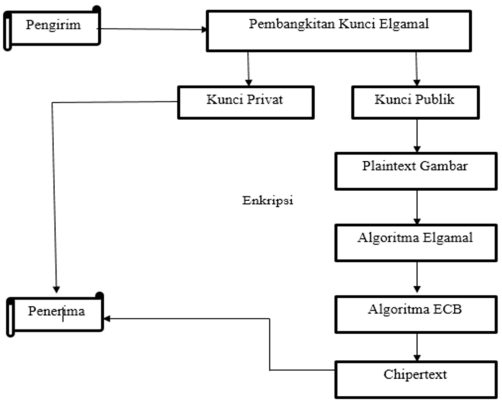
Berdasarkan uraian yang telah dijelaskan diatas, penulis tertarik untuk menggunakan dua teknik tersebut untuk proses dalam pengamanan file gambar. Oleh karena itu penulis mengambil judul "Implementasi kriptografi gambar menggunakan kombinasi algoritma Elgamal dan Mode Operasi Elektronik Code Book (ECB)".

2. METODE PENELITIAN

2.1 Metode yang Diusulkan

Metode yang diusulkan dalam penelitian ini adalah proses enkripsi dan dekripsi pada data file gambar dengan menggunakan teknik algoritma kriptografi yaitu algoritma Elgamal yang dikombinasikan dengan mode operasi ECB *(Electronik Code Book).*

a. Proses Enkripsi



Gambar 1. Proses Enkripsi

Berikut penjelasan proses enkripsi pada Gambar 1. :

1. Pengguna menjalankan sistem, dan melakukan pembangkitan kunci.
   - Proses pada pembangkitan kunci menggunakan bilangan Prima = 251, kemudian pilih dua buah bilangan acak g dan x, dengan syarat $g < p$ dan $1 \leq x \leq p - 2$. Untuk inputan g dan x berupa

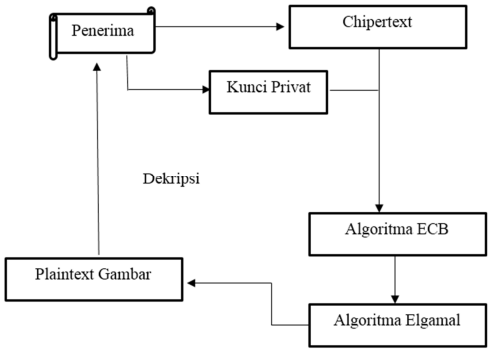
karakter huruf maksimal 9 digit kemudian karakter tersebut dijumlahkan atau dikonversi menjadi angka pada saat pembangkitan kunci yang mana A – Z = 1 – 26. Selanjutnya yaitu menghitung nilai g dan x dengan menggunakan persamaan rumus sebagai berikut :

- $y = g^x \ mod \ p$
- Hasil dari pembangkitan kunci ini diperoleh :
  Kunci Publik : Tripel (y, g, p)
  Kunci Privat : Pasangan (x, p)

2. Pengguna menggunakan kunci publik untuk proses enkripsi file gambar, dimana kunci publik ini adalah kunci yang tidak dirahasiakan.
3. Pengguna mencari dan memasukkan plainteks gambar yang akan di enkripsi.
4. Setelah itu proses enkripsi akan diproses menggunakan algoritma elgamal, dimana setiap m (nilai piksel) akan diproses menggunakan rumus *:*
   - $a = g^k \ mod \ p$
   - $b = y^k \ mod \ p$

   Untuk nilai pangkat k, dipilih secara acak dimana $1 \leq k \leq p - 2$. Hasil dari algoritma ini akan menghasilkan dua chipertext yaitu a dan b.
5. Selanjutnya melakukan proses ECB pada chipertext a dan b dengan cara operasi XOR.
   - $a = a \oplus x$
   - $b = b \oplus a.$
6. Setelah itu geser atau wrap 1 bit kekiri pada chipertext a dan b.
7. Hasil enkripsi atau chipertext yang dihasilkan adalah variable a dan b.

b. Proses Dekripsi



Gambar 2. Proses Dekripsi

Berikut penjelasan proses dekripsi pada Gambar 2. :

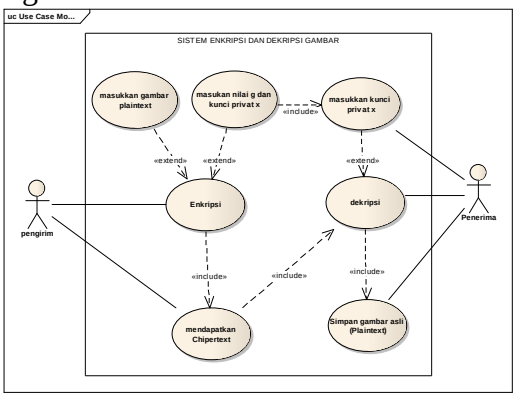
1. Pengguna menggunakan kunci privat x untuk proses dekripsi file gambar, dimana nilai
   x diperoleh dari hasil penjumlahan pada karakter huruf A – Z = 1 – 26 kemudian dikonversi
   menjadi angka. X merupakan kunci privat yang di inputkan pada saat pembangkitan kunci.
2. Pengguna memasukkan chipertext dari pengirim.
3. Kunci privat dan chipertext akan diproses menggunakan algoritma ECB. Geser atau wrap
   satu bit kekanan pada kedua chipertext a dan b. Kemudian lakukan operasi XOR pada :
   - $b = b \oplus a$
   - $a = a \oplus x$
4. Lakukan perhitungan menggunakan rumus Dekripsi Elgamal.
   - $ax^{-1} = a^{p-1-x} \ mod \ p$
   - $m = b * ax^{-1} \ mod \ p$
5. Hasil dekripsi dari plaintext awal akan ditampilkan.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Perancangan Sistem

Perancangan sistem menggunakan diagram use case, dimana dalam diagram use case ini menggambarkan

siapa saja yang terlibat dalam sistem dan menggambarkan proses apa saja yang terlibat dalam sistem, berikut diagram Use case pada kriptografi elgamal dan ECB :



Gambar 3. Use Case Sistem Enkripsi dan Dekripsi Gambar

Dari diagram use case diatas pengirim dapat melakukan enkripsi, dimana dalam proses enkripsi tersebut terdapat bagian yang harus dipenuhi seperti masukkan plaintext gambar, dan masukkan kunci publik g dan kunci privat x. Setelah itu proses enkripsi akan diproses di sistem, untuk bilangan prima ditetapkan secara langsung dari sistem yaitu 251, sedangkan kunci publik y dan nilai awal k didapat langsung dari proses pembangkitan kunci ketika proses enkripsi di eksekusi di sistem. Setelah proses enkripsi selesai maka pengirim akan mendapatkan chipertext dimana chipertext ini didapatkan dari bagian proses enkripsi.

Selanjutnya penerima dapat melakukan proses dekripsi gambar dari kunci privat x dan chipertext gambar yang didapatkan dari pengirim. Untuk melakukan proses dekripsi penerima memasukkan kunci privat gambar terlebih dahulu dimana kunci privat x ini adalah bagian yang didapatkan dari proses dekripsi dan kunci privat x ini didapatkan dari bagian proses enkripsi. Selanjutnya proses dekripsi akan di eksekusi oleh sistem yang telah dibuat dan kemudian penerima akan mendapatkan gambar plaintext dimana gambar plaintext ini didapatkan dari proses dekripsi.

3.2 Implementasi Program

Pada bagian ini penulis akan menjelaskan proses enkripsi dan dekripsi pada file gambar. Proses enkripsi dimulai dari algoritma elgamal kemudian dioperasikan sama mode operasi ECB dan menghasilkan chiperteks gambar, dan proses dekripsi dimulai dari mode operasi ECB kemudian algoritma elgamal dan akan menghasilkan plainteks gambar sesuai dengan metode yang diusulkan. Pengimplementasian algoritma elgamal dan mode operasi ECB ini digunakan untuk meningkatkan keamanan pada file gambar berekstensi jpg dan jpeg. Berikut proses enkripsi dan dekripsi

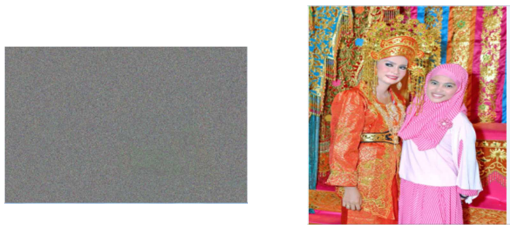
Gambar 4. Enkripsi File Gambar

pada program :

a. Proses Enkripsi

Pada Gambar 4 Untuk melakukan enkripsi, *user* harus memasukkan kunci *publik* g dan kunci *privat* x, dimana kunci *publik* g dan kunci *privat* x yang digunakan yaitu g=studio dan x=aurafoto. Setelah inputan plainteks, dan kunci g dan x sudah dituliskan pada program maka selanjutnya *user* dapat menekan tombol enkripsi yang terdapat

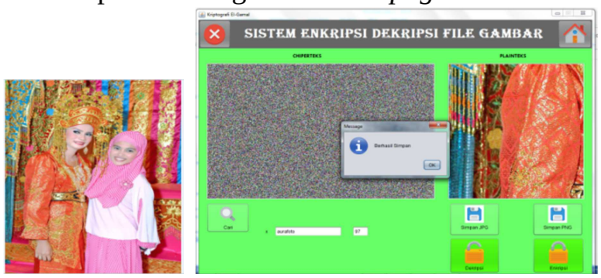
pada program dan menunggu hasil *eksekusi* program tersebut selesai. Setelah proses enkripsi pada program selesai, *user* dapat menyimpan file chiperteks gambar tersebut. Dalam analis eksperimen ini penulis menyimpan file chiperteks dengan nama *foto_1Enkrip*. Berikut perbandingan antara plainteks *gambar foto_1.jpg* dengan file gambar atau chiperteks yang sudah di enkripsi :



(a) (b)

Gambar 5. Plainteks Foto_1.jpg (a) dan Chiperteks foto_1Enkrip.png(b)

Pada gambar (b) merupakan chiperteks dari plainteks gambar foto_1.jpg (a). Setelah gambar foto_1.jpg melalui proses enkripsi, pola gambar tidak kelihatan sama sekali, dan gambar tidak dapat dikenali secara visual karena gambar sudah menjadi acak – acakan sehingga pola gambar susah ditebak dan dikenali. Hasil gambar plainteks sebelumnya *berekstensi .jpg*, namun setelah melalui proses enkripsi yang diproses diprogram akan menghasilkan gambar chiperteks dengan ekstensi *.png*.



Gambar 6. Dekripsi File Gambar

b. Proses Dekripsi

Untuk proses dekripsi pada Gambar 6. *user* harus memasukkan kunci *privat* yang digunakan pada saat proses *eksperimen* enkripsi. kunci privat yang digunakan untuk dekripsi *foto_1Enkrip* yaitu x = aurafoto. Setelah *file* chiperteks dan kunci *privat* x di inputkan, selanjutnya *user* dapat menunggu hasil *eksekusi* program pada dekripsi *file foto_1Enkrip*.

(a) (b)

Gambar 7. Chiperteks foto_1Enkrip.png (a) dan plainteks Foto_Dekrip1.jpg (b)

Setelah hasil *eksperimen* dekripsi program selesai maka *user* dapat menyimpan file gambar tersebut dengan *ekstensi .JPG, .JPEG* maupun *ekstensi PNG*. Penulis menyimpan file *ekstensi .jpg* dengan nama *foto_Dekrip1* dan *ekstensi .png* dengan nama *foto_Dekrip2*.

3.3 Eksperimen

Gambar 8. Hasil foto_dekrip1.jpg

Berdasarkan hasil eksperimen yang telah dilakukan diatas, Gambar 8. adalah hasil gambar foto_dekrip1.jpg (a) dan Hasil foto_dekrip2.png (b) merupakan hasil dari proses enkripsi dan dekripsi. Pada Gambar 8. diatas, secara visual gambar (a) dan (b) dapat dilihat secara langsung dan tidak ada perupahan antara gambar (a) dan (b)

terhadap gambar plainteks foto_1.jpg (a) pada Gambar 5. Namun jika dilihat pada intesitas piksel dari gambar plainteks foto_1.jpg dengan hasil gambar setelah enkripsi dan dekripsi pada foto_dekrip1.jpg terdapat perbedaan dikarenakan penyimpanan pada proses enkripsi dan dekripsi pada ekstensi jpg dan jpeg bervariasi sehingga nilai piksel ada yang berubah dan ada yang sama tetapi untuk gambar secara visual masih bisa dilihat tanpa adanya perbedaan. Sedangkan intesitas nilai piksel pada gambar plainteks foto_1.jpg dan hasil gambar setelah enkripsi dan dekripsi pada foto_dekrip2.png hasilnya sama baik dari segi piksel maupun secara visual tidak ada perubahan. Berikut perbedaan dari nilai - nilai piksel pada plainteks foto_1.jpg dan nilai piksel pada proses enkripsi dan dekripsi pada foto_dekrip1.jpg dan foto_dekrip2.png :

Tabel 1: plainteks Nilai RGB foto_1.jpg (a)

i / j	1			2			3			4			.....			1181		
RGB	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
1	106	191	108	129	213	128	163	215	141	145	199	123	...	..	..	234	74	162
...	...	...	...	...	...	...	...	...	...	...	...	...	...	..	..	..	..	...
1772	160	102	39	159	101	38	151	93	30	140	82	19	...	..	..	251	133	95

Tabel 2: plainteks Nilai RGB foto_dekrip1.jpg (a)

i / j	1			2			3			4			.....			1181		
RGB	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
1	107	192	109	133	210	130	157	218	141	136	203	123	...	..	..	233	75	162
...	...	...	...	...	...	...	...	...	...	...	...	...	...	..	..	..	..	...
1772	160	102	39	159	101	38	151	93	30	140	82	19	...	..	..	251	133	95

Tabel 3: plainteks Nilai RGB foto_dekrip2.png (b)

i / j	1			2			3			4			…….			1181		
RGB	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
1	106	191	108	129	213	128	163	215	141	145	199	123	...	..	..	234	74	162
...	...	...	...	...	...	...	...	...	...	...	...	...	...	..	..	..	..	...
1772	160	102	39	159	101	38	151	93	30	140	82	19	...	..	..	251	133	95

3.4 Hasil Pengujian

Pada bagian ini peneliti akan menganalisis beberapa eksperimen enkripsi dan dekripsi yang telah dilakukan serta perbandingan dari citra plainteks maupun citra setelah melalui proses enkripsi dan dekripsi. Analisis hasil ini meliputi pada Perubahan ukuran citra asli (lebar dan tinggi) dengan citra enkripsi dan citra dekripsi *jpg / jpeg* dan *png*. Analisis hasil ini meliputi pada :

1. Perubahan ukuran citra asli (lebar dan tinggi) dengan citra enkripsi dan citra dekripsi *jpg / jpeg* dan *png*.
2. Perbedaan kapasitas citra asli dengan citra enkripsi dan citra dekripsi *.jpg / jpeg* dan *.png*.
3. Rata – rata *MSE* citra asli dengan citra dekripsi *.jpg / .jpeg* dan *.png*.
4. Rata – rata *PSNR* citra asli dengan citra dekripsi *.jpg / jpeg* dan *.png*.

Tabel 4: Hasil pengujian

No	Ukuran Citra Asli	Besar Citra Asli	Ukuran Citra Enkripsi	Besar Citra Enkripsi	Ukuran Citra Dekripsi JPG dan .PNG	Besar Citra Dekripsi JPG dan .PNG	MSE Dekripsi .JPG dan .PNG	PSNR Dekripsi .JPG dan .PNG
1	Foto_1.jpg 1181x1772	1.83MB	2362x1772	9.61MB	1181x1772.jpg 1181x1772.png	.JPG 1.46MB .PNG 5.32MB	.JPG 3.7572 .PNG 0	.JPG 36.6335 .PNG Inf
2	Foto_2.jpg 1181x1772	412 KB	2362X1772	9.74MB	1181x1772.jpg 1181x1772.png	.JPG 1.53 MB .PNG 5.47MB	.JPG 2.4647 .PNG 0	.JPG 40.2957 .PNG Inf
3	Foto_3.jpg 1181x1772	424 KB	2362X1772	9.60MB	1181x1772.jpg 1181x1772.png	.JPG 1.59MB .PNG 5.41MB	.JPG 2.3732 .PNG 0	.JPG 40.6240 ,PNG Inf
4	Foto_4.jpg 1181x1772	322 KB	2362X1772	9.55MB	1181x1772.jpg 1181x1772.png	.JPG 1.19 MB .PNG 4.74 MB	.JPG 1.6447 .png 0	.JPG 43.8093 .png Inf

5	Foto_5.jpg 1500x2100	408 KB	3000x2100	14.5MB	1500x2100.jpg 1500x2100.png	.JPG 1.15 MB .PNG 3.94 MB	.JPG 1.4835 .png 0	.JPG 44.7052 .png Inf
6	Foto_6.jpg 400 x 600	61.9 KB	800 x 600	1.02MB	400 x 600.jpg 400 x 600.png	.JPG 107 KB .PNG 348 KB	.JPG 3615 .PNG 0	.JPG 45.4506 .PNG Inf
7	Foto_7.jpg 1063 x 709	497 KB	2126 x 709	3.59MB	1063 x 709.jpg 1063 x 709.png	.JPG 444 KB .PNG 1.47 MB	.JPG 1.3322 .PNG 0	.JPG 45.6392 .PNG Inf
8	Foto_8.jpg 472 x 709	57.5 KB	944 x 709	1.22MB	472 x 709.jpg 472 x 709.png	.JPG 97.5 KB .PNG 264 KB	.JPG 2.2159 .PNG 0	.JPG 41.2197 .PNG Inf
9	Foto_9.jpg 354 x 472	103 KB	708 x 472	748 KB	354 x 472.jpg 354 x 472.png	.JPG 82.1 KB .PNG 196 KB	.JPG 1.9127 .PNG 0	.JPG 42.4977 .PNG Inf
10	Foto_10.jpg 1500x1051	677 KB	3000x1051	7.48MB	1500x1051.jpg 1500x1051.png	.JPG 1.24 MB .PNG 3.46 MB	.JPG 2.9247 .PNG 0	.JPG 38.8092 .PNG Inf

4. KESIMPULAN

Dari hasil perancangan dan pembuatan program aplikasi dengan menggunakan dua algoritma yaitu elgamal dan mode operasi ECB, maka dapat diambil kesimpulan sebagai berikut:

1. Penulis berhasil mengimplementasikan algoritma Elgamal dan Mode Operasi ECB dalam mengamankan gambar yang berekstensi *.jpg* dan *.jpeg* dan menyimpan gambar yang telah dienkripsi ke dalam file berekstensi *.png*.
2. Penulis berhasil mendekripsikan gambar yang telah dienkripsi dan mengembalikan seperti semula ke dalam file berekstensi *.jpg, .jpeg* maupun *.png.*
3. Penulis berhasil mengamankan data gambar sehingga tidak dapat dilihat secara visual.
4. Untuk Chipertext gambar tidak tahan terhadap serangan seperti *brightness dan kontras, noise, blurring,* dan *cropping.*

5. SARAN

Adapun saran-saran yang berguna untuk penelitian selanjutnya agar output yang dihasilkan lebih baik lagi adalah sebagai berikut :

1. Diperlukan pengembangan dalam pengamanan file yang tidak hanya mencakup .jpg dan .jpeg.
2. Diperlukan pengembangan aplikasi untuk dapat mengenkripsi lebar citra yang lebih dari 3000 px.
3. Untuk penelitian selanjutnya, diperlukan pengembangan aplikasi agar lebih cepat dan efisien untuk gambar yang berukuran lebih besar.

DAFTAR PUSTAKA

[1] H. Kurniadi, "Implementasi Algoritma Kriptografi Elgamal Untuk File Citra 2 Dimensi," pp. 1-6, 2015.

[2] Munir, Rinaldi, "Algoritma enkripsi citra dengan pseudo one- time pad yang menggunakan sistem chaos," *konferensi nasional informatika,* pp. 12-16, 2011.

[3] M. T. Tamam, W. Dwiono and T. Hartanto, "Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra," *EECCIS,* vol. IV, pp. 8-11, 2010.

[4] E. Y. I. Kurniawan, "Penerapan teori chaos pada kriptografi menggunakan algoritma stream cipher dan elektronik code book (ECB) untuk keamanan pesan teks," 2014.