ARTIKEL

PENERAPAN ALGORITMA ELGAMAL DALAM STEGANOGRAFI

Oleh:

Alim Mutohidin

13.1.03.02.0209

Dibimbing oleh :

1. Resty Wulanningrum, M.Kom.

2. Ardi Sanjaya, M.Kom.

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2018

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2018

Yang bertanda tangan di bawah ini:

Nama Lengkap	: Alim Mutohidin
NPM	: 13.1.03.02.0209
Telepun/HP	: 085607726057
Alamat Surel (Email)	: alim.mutohidin@outlook.com
Judul Artikel	: Penerapan Algoritma Elgamal Dalam Steganografi
Fakultas – Program Studi	: Fakultas Teknik – Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jl. KH. Ahmad Dahlan No.76, Mojoroto, Kota Kediri, Jawa Timur 6411

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 7 Februari 2018
Pembimbing I Resty Wulanningrum, M.Kom. NIDN. 0719068702	Pembimbing II Ardi Sanjaya, M.Kom. NIDN. 0706118101	Penulis, Alim Mutohidin NPM. 13.1.03.02.0209

PENEAPAN ALGORITMA ELGAMAL DALAM STEGANOGRAFI

Alim Mutohidin
13.1.03.02.0209
Fakultas Teknik – Program Studi Teknik Infomatika
alim.mutohidin@outlook.com
Resty Wulanningrum, M.Kom. dan Ardi Sanjaya, M.Kom.
UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Perkembangan *teknologi* saat ini sangat pesat di segala bidang. Dampak positif dari perkembangan tersebut adalah semakin mudahnya melakukan proses *transfer* data dengan berbagai media yaitu *internet*, Seiring dengan kemudahan dalam melakukan *transfer* data, terdapat suatu resiko yang menyertai, yaitu keamanan data, *Steganografi* merupakan salah satu cara pengamanan data untuk menjamin kerahasiaan data, namun hal ini masih memungkinkan terjadinya pencurian data maupun akses aplikasi secara *ilegal* oleh pihak yang tidak bertanggung jawab. Oleh sebab itu, Penulis mencoba untuk memperkuat segi keamanan dalam proses pengeluaran (*extraction*) data rahasia dengan cara mengkombinasikan dengan teknik *kriptografi ElGamal*.

Tujuan yang hendak ingin dicapai adalah Bagaimana mengimplementasikan dan mengkombinasikan *steganografi* dan kriptografi metode *ElGamal* pada media citra digital dan apakah aplikasi pengamanan data menggunakan teknik *steganografi* dan kriptografi dapat menjaga pertukaran data lebih aman serta menjaga keamanan dan kerahasiaan data.

Teknik penelitian dalam penelitian ini adalah Penelitian Pengembangan atau Rekayasa Teknologi Informasi dengan subyek mahasiswa teknik inormatika UNP Kediri angkatan 2013. Sedangkan untuk pendekatan menggunakan pendekatan kuantitatif. Jenis pendekatan kuantitatif yang dipilih adalah noneksperimental berupa deskriptif.

Dari penelitian ini telah di hasilkan Aplikasi Steganografi & Enkripsi Elgamal dengan Windows *Opration System.* Aplikasi ini dapat membantu dalam menjaga pertukaran data lebih aman.
Berdasarkan hasil simpulan direkomendasikan : (1) Aplikasi Steganografi & Elgamal ini perlu menyembunyikan data lain seperti gambar ataupun file dokumen, sehingga data yang bisa kita simpan bukan hanya data teks saja. (2) Penyempurnaan fitur lain seperti menggunakan media penyisipan dengan format ekstensi lain, menambah kapasitas teks yang disisipkan serta fitur lain yang perlu ditambahkan untuk menambah kenyamanan pengguna.

KATA KUNCI : Algoritma Asimetris, Algoritma ElGamal, Pesan Rahasia Steganografi,

I. LATAR BELAKANG

Perkembangan *teknologi* saat ini sangat pesat di segala bidang. Dampak positif dari perkembangan tersebut adalah semakin mudahnya melakukan proses *transfer* data dengan berbagai media yaitu *internet*, media *portable*, atau dengan koneksi *nirkabel*. Dengan demikian proses pertukaran data dapat dilakukan dengan cepat dan *efisien*.

Seiring dengan kemudahan dalam melakukan *transfer* data, terdapat suatu resiko yang menyertai, yaitu keamanan data. Tidak semua data boleh diakses oleh umum, beberapa di antaranya bersifat rahasia yang berarti data tersebut tidak boleh diketahui oleh pihak yang tidak memiliki wewenang, sehingga kebutuhan tingkat keamanan terhadap suatu informasi maupun data rahasia sangat tinggi, agar data tersebut tidak diketahui oleh pihak yang tidak berwenang. *Steganografi* merupakan salah satu cara pengamanan data untuk menjamin kerahasiaan data. *Steganografi* merupakan suatu cara menyembunyikan informasi dan mencegah kemungkinan terjadinya pendeteksian pesan dengan menyamarkan keberadaan data yang telah disisipkan ke media penampungnya. Media penampung tersebut dapat berupa *audio, citra, video atau media* lainnya. Dalam hal ini media penampung masih terlihat seperti layaknya *file* normal tanpa mengalami perubahan secara kasat mata. Sehingga seolah - olah media penampung yang telah disisipi oleh data rahasia (*stego image*) tersebut tidak dicurigai oleh orang lain.

Meskipun pengamanan data telah dilakukan sedemikian rupa dengan mengunakan *steganografi*, namun hal ini masih memungkinkan terjadinya pencurian data maupun akses aplikasi secara *ilegal* oleh pihak yang tidak bertanggung jawab. Oleh sebab itu, Penulis mencoba untuk memperkuat segi keamanan dalam proses pengeluaran (*extraction*) data rahasia dengan cara mengkombinasikan dengan teknik *kriptografi ElGamal*.

Pada penelitian ini penulis menggunakan *citra digital* sebagai media penampung dalam *Steganografi* dengan perpaduan menggunakan *teknik kriptografi* dalam menjaga keamanan dan kerahasiaan. *Algoritma ElGamal* termasuk dalam *kriptografi modern* yang menggunakan *plainteks, cipherteks* dan kunci untuk melakukan proses *enkripsi* dan *dekripsi* dalam pengamanan data, Kelebihan dari *algoritma ElGamal* adalah terletak pada kesulitan penghitungan *alogaritma diskret*

pada bilangan *modulo prima* yang besar sehingga upaya untuk menyelesaikan masalah algoritma ini menjadi sangat sukar. *Algoritma ElGamal* terdiri dari tiga proses, yaitu proses pembentukan kunci, proses *enkripsi* dan proses *dekripsi*. Algoritma ini merupakan *cipher blok*, yaitu melakukan proses enkripsi pada blok-blok *plainteks* dan menghasilkan blok-blok *cipherteks* yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan (Ifanto, 2009).

Berdasarkan latar belakang di atas maka penulis berusaha untuk mengembangkan sebuah aplikasi yang sesuai dengan harapan tersebut dengan judul "PENERAPAN ALGORITMA ELGAMAL DALAM STEGANOGRAFI". Agar nantinya aplikasi ini diharapkan mampu menjaga kerahasiaan data serta memberikan keamanan data dari para penyadap maupun dari pihak-pihak yang tidak bertanggung jawab.

II. METODE

A. Steganografi

Steganografi adalah ilmu menyembunyikan teks pada *media* lain yang telah ada sedemikian rupa sehingga teks yang tersembunyi menyatu dengan *media* itu. *Media* tempat penyembunyian pesan tersembunyi dapat berupa *media teks, gambar, audio, atau video*. *Steganografi* yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat *diekstrasi* (Sadikin, 2012).

B. Algoritma Asimetris

Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan.

C. Algoritma Elgamal

Algoritma *ElGamal* merupakan algoritma dalam *kriptografi* yang termasuk dalam kategori algoritma *asimetris*. Keamanan algoritma *ElGamal* terletak pada kesulitan penghitungan logaritma *diskret* pada bilangan *modulo prima* yang besar sehingga upaya untuk menyelesaikan masalah

alogaritma ini menjadi sangat sukar.

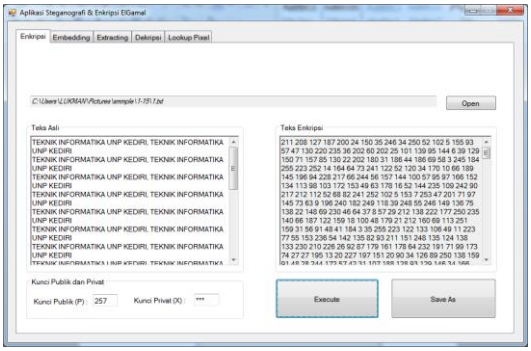
Algoritma *ElGamal* mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan. Algoritma ini mempunyai kerugian pada *cipherteksnya* yang mempunyai panjang dua kali lipat dari plainteksnya. Akan tetapi, algoritma ini mempunyai kelebihan pada *enkripsi.* Untuk *plainteks* yang sama, algoritma ini memberikan *cipherteks* yang berbeda (dengan kepastian yang dekat) setiap kali *plainteks* di *enkripsi.*

D. Citra

Citra merupakan istilah lain untuk gambar, yaitu sebagai salah satu komponen *multimedia* yang memegang peranan sangat penting sebagai bentuk *informasi visual*. Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi (Sutoyo, 2009).

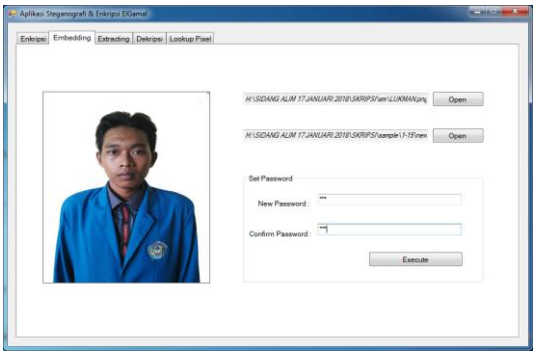
III. HASIL DAN KESIMPULAN

A. Hasil



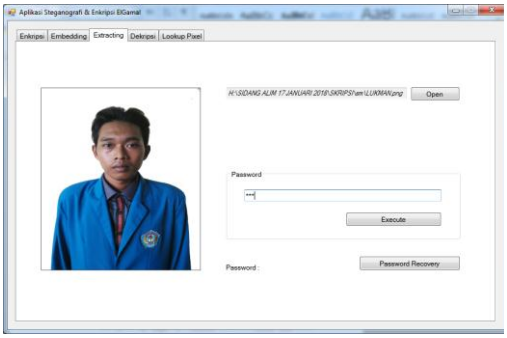
Gambar 1 Desain Antarmuka (Menu Enkripsi)

Pada Gambar 1 Menu *Enkripsi* ini terdiri atas berbagai fitur antara lain adalah *Input Massage*, kolom *Input Public Key* dan *Input Privat Key* serta *Button Execute* dan *Save As Massage.*



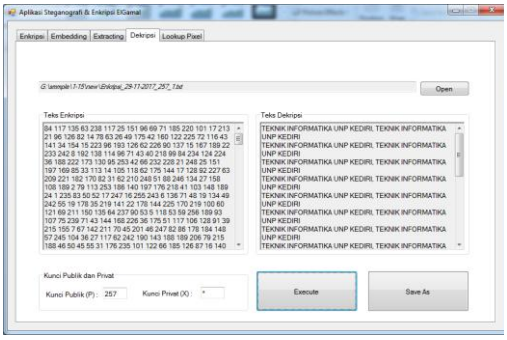
Gambar 2 Desain Antarmuka (Menu Embedding)

Pada Gambar 2 Menu *Embedding* ini terdiri atas berbagai fitur antara lain satu *Input Image* yakni *Input Stego Image* dan *Input Massage* berupa *file Txt*, *Input Password* dan *Button Execute Embedding*.



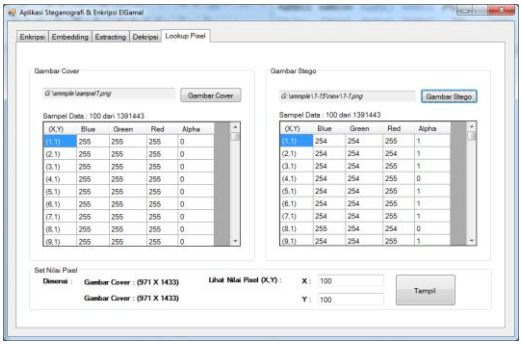
Gambar 3 Desain Antarmuka (Menu Extracting)

Gambar 3 Menu *Extracting* ini terdiri atas berbagai fitur antara lain satu *Input Image Stego, Input Passwrd* dan *Button Execute,* serta *button password recovery* untuk mengetahui password gambar.



Gambar 4 Desain Antarmuka (Menu Dekripsi)

Pada Gambar 4 Menu *Dekripsi* ini terdiri atas berbagai fitur antara lain adalah *Input Massage* yang di *Enkripsi* berupa file *Txt*, kolom *Input Public Key* dan *Input Privat Key* serta *Button Execute* dan *Save As Massage*.



Gambar 5 Desain Antarmuka (Menu *Lookup Pixel*)

Pada Gambar 5 Menu *Lookup Pixel* ini digunakan untuk membedakan niai pixel pada gambar sebelum di sisipi teks dan setelah di sisipi teks, terdiri atas berbagai fitur antara lain, *input Image Cover* yaitu berupa gambar sebelim di sisipi pesan, *input Image Stego* yaitu berupa gambar yang sudah di sisipi teks, dan akan menampilkan nilai dimensi dari gambar *Cover* dan *Stego* serta kolom untuk menentukan nilai x dan y berupa *pixel* gambar yang di pilih.

StegoElgamal akan dibagi menjadi menjadi tiga proses, yaitu proses enkripsi, poses embedding, dan proses dekripsi dengan menggunakan citra sebagai media penampung pesan/teks rahasia dan akan dilihat perbedaan ukuran pesan/teks sebelum dan sesudah terenkrisi serta perbedaan ukuran citra sebelum dan sesudah di sisipi

pesan/teks rahasia dengan tiga ukuran citra 100 kb, 500 kb, dan 1000 kb, berikut simulasi prosesnya.

1) Proses Enkripsi

Tabel 1 Perubahan Proses Enkrips

No	Uuran teks awal	Ukuran teks terenkripsi
1	1 KB	7 KB
2	2 KB	15 KB
3	3 KB	22 KB
4	4 KB	29 KB
5	5 KB	36 KB

Pada tabel 1 dapat dilihat perbedaan ukuran pesan/teks dengan ukuran pesan/teks yang sudah dalam bentuk enkripsi.

2) Proses Embedding

Tabel 2 Perbedaan Ukuran Citra

No	Ukuran citra wal	Uuran teks awal	Ukuran teks terenkripsi	Ukran citra yang sudah disisipi
1	100 kb	1 KB	7 KB	114 KB
2		2 KB	15 KB	120 KB
3		3 KB	22 KB	126 KB
4		4 KB	29 KB	135 KB
5		5 KB	36 KB	143 KB
6	500 kb	1 KB	7 KB	578 KB
7		2 KB	15 KB	588 KB
8		3 KB	22 KB	596 KB
9		4 KB	29 KB	605 KB
10		5 KB	36 KB	612 KB
11	1000 kb	1 KB	7 KB	114 KB
12		2 KB	15 KB	120 KB
13		3 KB	22 KB	126 KB
14		4 KB	29 KB	135 KB
15		5 KB	36 KB	143 KB

Pada gambar 2 dapat dilihat perbedaan antara citra ukuran awal dan ukuran citra setelah di sisipi pesan/teks rahasia.

3) Proses Dekripsi

Tabel 3 Proses Dekripsi

No	Ukuran citra wal	Uuran teks awal	Ukuran teks terenkripsi	Ukran citra yang sudah disisipi	Proses dekrpsi
1	100 kb	1 KB	7 KB	114 KB	Succes
2		2 KB	15 KB	120 KB	Succes
3		3 KB	22 KB	126 KB	Succes
4		4 KB	29 KB	135 KB	Succes
5		5 KB	36 KB	143 KB	Succes
6	500 kb	1 KB	7 KB	578 KB	Succes
7		2 KB	15 KB	588 KB	Succes
8		3 KB	22 KB	596 KB	Succes
9		4 KB	29 KB	605 KB	Succes
10		5 KB	36 KB	612 KB	Succes
11	1000 kb	1 KB	7 KB	114 KB	Succes
12		2 KB	15 KB	120 KB	Succes
13		3 KB	22 KB	126 KB	Succes
14		4 KB	29 KB	135 KB	Succes
15		5 KB	36 KB	143 KB	Succes

Dapat dilihat pada Tabel 3 bahwa proses dekrpsi pesan/teks succes eksekusi,

Dari tiga proses diatas dapat diketahui perbedaan ukuran pesan/teks sesudan dan sebelum terenkripsi dan perbedaan ukuran citra sebelum dan sesudah disisipi pesan/teks rahasia dengan berbagai ukuran citra yang telah digunakan.

Aplikasi stegoelgamal ini telah bisa mengkobinasikan antara teknik steganogafi menggunakan media citra digital dengan algoritma elgamal sehingga keamanan pada aplikasi ini lebih aman untuk melindungi pesan/teks rahasia dari orang-orang yang akan bertindak ilegal, karena dengan media citra yang digunakan tidak dapat membedakan apakah didalamnya terdapat data rahasianya yang sudah terenkripsi dengan kriptografi elgamal.

B. Kesimpulan

Setelah melalui beberapa tahapan dalam menyelesaikan Aplikasi Steganografi & Elgamal dengan berbasis desktop ini dihasilkan kesimpulan sebagai berikut :

1. Aplikasi ini dapat dikombinasikan dengan baik antara steganografi dan metode elgamal untuk menyembunyikan teks yang bersifat rahasia kedalam citra digital yang memudahkan penggunanya.
2. Data yang kita sembunyikan pada media citra yang dipadukan dengan kriptografi elgamal yang berfungsi untuk pertukaran data akan menjadi lebih aman.

IV. DAFTAR PUSTAKA

Ifanto, Muhammad. 2009. *"METODE ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN ALGORITMA ELGAMAL"*.

Sadikin, Rifki. 2012. *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Andi Offset.

Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, O.D. dan Wijanarko, M. T. 2009. *Teori Pengolahan Citra Digital*. Yogyakarta: Andi Offset.