ANALISIS DAN IMPLEMENTASI GABUNGAN KRIPTOGRAFI ELGAMAL DAN STEGANOGRAFI FRAME DENGAN MENGGUNAKAN KUNCI CITRA DIGITAL

I Komang Rinartha Yasa Negara [1], Evi Triandini[2]
STMIK STIKOM Bali
Jalan Raya Puputan No 86 Renon Denpasar Bali
[1)]katak_negara@yahoo.com, [2)] evi@stikom-bali.ac.id

Abstrak

Kriptografi digunakan dalam kehidupan sehari-hari, apalagi pada saat ini komunikasi yang sering digunakan adalah komunikasi melalui internet. Dalam penggunaanya, tidak menutup kemungkinan terdapat informasi-informasi rahasia yang tidak diperuntukkan kepada masyarakat umum, sehingga dibutuhkan suatu pengamanan informasi agar informasi yang bersifat rahasia dan penting dapat terjamin keamanannya dan utuh diterima oleh orang-orang yang menggunakannya. Salah satu cara yang dapat digunakan dalam mengamankan pengiriman informasi, yaitu dengan menyandikan informasi menjadi kode-kode yang tidak dengan mudah dimengerti oleh orang-orang yang tidak berkepentingan. Selain kriptografi, terdapat pula sebuah metode untuk menyembunyikan informasi pada informasi yang lain yang disebut dengan steganografi yaitu sebuah metode untuk menyembunyikan informasi ke dalam suatu media. Pada penelitian ini dikembangkan sebuah algoritma kriptografi dan steganografi yang merupakan gabungan dari kriptografi ElGamal dan steganografi Frame. Analisa terhadap penggabungan kedua buah metode tersebut dilakukan dengan menggunakan analisa matematis dan analisa program. Kemudian dilakukan pengujian terhadap data yang dikirimkan dengan data yang diterima. Setelah dilakukan analisa dan implementasi terhadap penggabungan kedua metode tersebut, didapat bahwa kriptografi ElGamal dapat digabungkan dengan steganografi frame untuk mengamankan data berupa teks. Setelah dilakukan pengujian didapat bahwa, data yang diterima setelah proses dekripsi menghasilkan data yang sama dengan data yang dikirimkan sebelum proses enkripsi dengan tingkat akurasi 100%. Data yang digunakan untuk menyimpan hasil enkripsi maupun kunci publik harus disimpan dalam bentuk citra bitmap yang tidak mengalami kompresi.

Kata kunci : keamanan data, kriptografi ElGamal, steganografi frame, file teks

Abstract

Cryptography is used in everyday life , especially at this time of communication that is often used is the communication via the internet . In use, it is possible there is secret information that is not intended for the general public , so it takes a security information so that the information is confidential and important to guarantee its security and received intact by the people who use them . One way that can be used to secure the transmission of information , ie the information is encoded into a code that is not easily understood by people who are not interested . In addition to cryptography , there is also a method for hiding information in other information called steganography is a method for hiding information into a medium . In this study developed a cryptography and steganography algorithm which is a combination of the ElGamal cryptography and steganography Frame . Analysis of a merger of the two pieces is done by using the methods of mathematical analysis and program analysis . Then be tested against the data transmitted by the data received . After analysis and implementation of the merger of these two methods , found that the ElGamal cryptography steganography can be combined with the frame to secure the data in the form of text . After testing found that , the received data after decryption process produces the same data with the data submitted before the encryption process with 100 % accuracy rate . The data used to store the results of a public key encryption and should be stored in the form of a bitmap image is not compressed .

***Keywords** : data security , ElGamal cryptography , steganography frames , text files*

1. Pendahuluan

Kriptografi merupakan metode yang digunakan dalam menyandikan informasi. Kriptografi dibutuhkan ketika menjaga kerahasian dari komunikasi pada jalur umum atau untuk membuktikan keaslian dari sebuah pesan (Joux, 2009). Kriptografi dan steganografi digunakan dalam kehidupan sehari-hari, apalagi pada saat ini komunikasi yang sering digunakan adalah komunikasi melalui internet. Dalam dunia bisnis, perbankan, perdagangan, industri, pemerintahan dan juga dunia pendidikan, internet dapat digunakan secara bebas, terlebih lagi penggunaan teknologi awan yang sedang marak dikembangkan di berbagai bidang. Dalam penggunaan teknologi awan (cloud computing), tidak menutup kemungkinan terdapat informasi-informasi rahasia yang tidak diperuntukkan kepada masyarakat umum, sehingga dibutuhkan suatu pengamanan informasi agar informasi yang bersifat rahasia dan penting dapat terjamin keamanannya dan utuh diterima oleh orang-orang yang menggunakannya. Salah satu cara yang dapat digunakan dalam mengamankan pengiriman informasi, yaitu dengan menyembunyikan informasi pada media lain maupun dengan menyandikan informasi menjadi kode-kode yang tidak dengan mudah dimengerti oleh orang-orang yang tidak berkepentingan.

Kriptografi dan steganografi yang dikembangkan adalah kriptografi ElGamal dan steganografi frame (tepi gambar). Hoffstein, Pipher dan Silverman pada tahun 2008 menjelaskan bahwa kriptografi kunci publik ElGamal diuraikan oleh Taher ElGamal pada tahun 1985. Kriptografi ElGamal merupakan kriptografi kunci publik yang menggunakan kunci yang berbeda dalam melakukan proses enkripsi dan dekripsi. Pada penggunaanya kriptografi ElGamal menggunakan kunci private untuk dekripsi dan kunci publik untuk enkripsi. Steganografi frame (tepi gambar) merupakan pengembangan dari steganografi End Of File. (Setyobudi, 2011) Steganografi End Of File menggunakan proses penyisipan pesan pada akhir dari sebuah file. Ukuran file yang dihasilkan dari proses steganografi End Of File akan memiliki ukuran yang sama dengan file media ditambah dengan ukuran file yang akan disisipkan. (Sukrisno, Utami. 2007)

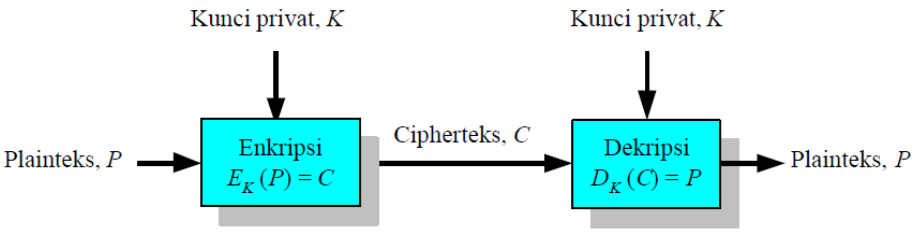
Citra digital digunakan sebagai kunci dalam kriptografi dikarenakan citra digital memiliki jangkauan nilai dari 0 hingga 255 yang merupakan intensitas warna yang terdapat di dalam citra digital. Citra digital yang umumnya digunakan oleh manusia memiliki dimensi piksel yang besar, sehingga citra digital lebih baik digunakan sebagai kunci dibandingkan dengan huruf maupun angka. Ketika kunci citra digunakan, maka ratusan angka yang tidak terlihat manusia dapat menjadi sebuah kunci. Apabila menggunakan huruf maupun angka, maka diperlukan masukan huruf dan angka yang berjumlah besar untuk menjadi kunci yang aman.

2. Tinjauan Pustaka

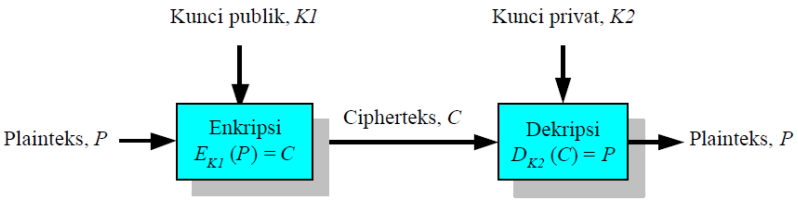
2. 1. Kriptografi

Terdapat beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu karena kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudiation* (Annonymous, 2010).

Proses yang dilakukan dalam kriptografi yang umum dikenal adalah proses enkripsi dan dekripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti (*plaintext*) menjadi sebuah kode yang tidak bisa dimengerti (*ciphertext*). Dekripsi merupakan kebalikan dari enkripsi, yaitu sebuah proses yang melakukan perubahan sebuah kode hasil proses enkripsi yang tidak bisa dimengerti (*ciphertext*) menjadi sebuah kode yang bisa dimengerti (*plaintext*) yang merupakan kode sebenarnya.



Gambar 1. Proses kriptografi kunci simetris



Gambar 2. Proses kriptografi kunci asimetris

2. 2. Kriptografi ElGamal

Algoritma ElGamal, ditemukan oleh ilmuwan Mesir Taher ElGamal pada tahun 1984, merupakan algoritma kriptografi kunci publik. Algoritma kunci publik menggunakan kunci yang berbeda untuk proses transformasinya. Untuk proses enkripsi menggunakan kunci publik, sedangkan proses dekripsi menggunakan kunci private. Algoritma ElGamal mendasarkan kekuatannya pada fakta matematis kesulitan menghitung logaritma diskrit (Afif, 2009).

Dalam kriptografi ElGamal terdapat 3 proses yang digunakan, antara lain proses public key creation (pembuatan kunci publik) oleh penerima, encryption (enkripsi) oleh pengirim, dan decryption (dekripsi) oleh penerima. (Rinartha, 2011)

a. Untuk proses public key creation yang akan dilakukan oleh pengguna yang akan menerima pesan yang kemudian akan diberikan kepada pihak yang akan mengirim pesan, memerlukan tiga buah masukan yang diolah sehingga menghasilkan sebuah keluaran dan dituliskan dalam bentuk matematis sebagai berikut :

$$A = g^a \ (mod\, p)$$

Dengan masukan pertama adalah bilangan p, masukan ke dua adalah bilangan g dan masukan ketiga adalah bilangan a yang diolah sehingga menghasilkan keluaran berupa bilangan A. Jadi kunci publik yang dapat diberikan kepada umum untuk melakukan enkripsi pesan adalah bilangan (p,g,A) dengan kunci *private* yang harus dirahasiakan adalah (a).

b. Untuk proses enkripsi yang dilakukan oleh pihak yang akan melakukan pengiriman pesan dengan kunci publik yang diberikan oleh pihak yang akan menerima pesan, memerlukan tiga buah masukan yang kemudian diolah sehingga dihasilkan dua buah keluaran yang dituliskan dalam bentuk matematis sebagai berikut :

$$C_1 = g^k \ (mod\, p) \text{ dan } C_2 = m.A^k \ (mod\, p)$$

Dengan masukan pertama merupakan plaintext pesan m, kemudian masukan kedua merupakan bilangan k yang merupakan bilangan acak sementara, masukan ketiga yaitu bilangan-bilangan (A, p, g) yang merupakan kunci publik yang diolah sehingga menghasilkan keluaran berupa bilangan C_1 , dan bilangan C_2. Jadi secara umum, hasil ciphertext yang dihasilkan adalah (C_1, C_2).

c. Untuk proses dekripsi yang akan dilakukan oleh penerima, memerlukan tiga buah masukan yang kemudian diolah menjadi sebuah keluaran dan dituliskan dalam bentuk matematis sebagai berikut :

$$pesan = (C_1^{\ a})^{-1} C_2 \ (mod\, p)$$

Dengan masukan pertama adalah bilangan C_1, masukan kedua adalah bilangan C_2 dan masukan ketiga adalah bilangan-bilangan (a, p) yang diolah sehingga dihasilkan keluaran plaintext pesan.

2. 3. Steganografi

Istilah steganografi termasuk penyembunyian data digital dalam file-file komputer. Contohnya, si pengirim mulai dengan file gambar biasa, lalu mengatur warna setiap *pixel* ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benarbenar memperhatikannya).

Yogie Aditya dkk pada tahun 2010 menyatakan bahwa Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (*teks* atau gambar) di dalam file-file lain yang mengandung *teks, image,* bahkan *audio* tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Metode ini termasuk tinta yang tidak tampak, *microdots,* pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau

sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.
Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya. (Setyobudi, 2011)

Saat ini dalam dunia digital, teknik steganografi banyak digunakan untuk menyembunyikan informasi rahasia dengan berbagai maksud. Salah satu tujuan dari steganografi adalah mengirimkan informasi rahasia melalui jaringan tanpa menimbulkan kecurigaan. Disamping itu steganografi juga dapat digunakan untuk melakukan autentikasi terhadap suatu hasil karya sebagaimana pemanfaatan watermarking. Steganografi memerlukan setidaknya dua properti. Properti pertama adalah wadah penampung (cover) dan yang kedua adalah data atau pesan yang disembunyikan. Untuk meningkatkan tingkat keamanan data yang disimpan, dapat dilakukan dengan menambahkan properti kunci (key) rahasia. properti kunci ini dapat berupa kunci simetris maupun kunci public atau privat. Berkas hasil dari proses steganografi sering disebut sebagai berkas stego (stego file) atau stego objek.

2. 4. Steganografi End Of File

Teknik ini tidak jauh beda dengan teknik LSB (*Least Significant Bit*). Jika LSB menambahakan data file pada akhir bit-nya, maka EOF langsung menambahkan data diakhir file image. Untuk teknik ini dapat menambahkan data atau file yang akan disembunyikan lebih dari ukuran file image. Data yang disembunyikan tersebut akan disisipkan pada akhir file sehingga file image akan terlihat sedikit berbeda dengan aslinya. Ada penanda khusus yang terlihat dari file image di paling bawah seperti garis-garis.

3. Analisis dan Implementasi

3. 1. Analisa steganografi frame

Analisa awal penelitian ini adalah melakukan analisa dan memodifikasi steganografi end of file untuk meningkatkan keamanan data. Teknik end of file merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Teknik inilah yang akan digunakan dalam penelitian ini. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut. Steganografi yang digunakan akan dimodifikasi sedemikian rupa agar berbentuk bingkai atau frame. Jadi data teks yang disisipkan ada di dalam frame tersebut. Sehingga dapat kita sebut sebagai steganografi tepi gambar.

Proses encode steganografi :

Gambar 3. Proses encode steganografi tepi gambar

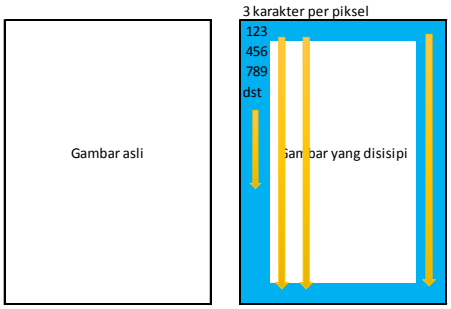
Proses decode steganografi :

Gambar 4. Proses decode steganografi tepi gambar

Proses penyisipan pesan dilakukan dengan cara :

Jika memiliki pesan “selamat pagi”, disisipkan ke dalam sebuah gambar dengan ukuran 295x200 piksel. Panjang pesan yang akan disisipkan sebanyak 12 huruf, sehingga dimasukkan ke dalam tepi

gambar dengan tempat yang akan disisipkan adalah sebanyak 3 karakter (huruf) setiap pikselnya dalam komponen RGB masing-masing piksel.



Gambar 5. Proses penyisipan pesan

Dari proses yang ditunjukkan pada Gambar 5, didapatkan penyisipan pesan yang menyerupai bingkai atau frame. Sehinga disebut sebagai steganografi tepi gambar. (Setyobudi, 2011)

3. 2. Kriptografi ElGamal

Pada kriptografi ElGamal dikenal tiga proses yaitu; pembuatan kunci publik, enkripsi dan dekripsi. Keseluruhan proses tersebut akan menggunakan citra dijital sebagai variabel-variabel masukan. Proses-proses dalam kriptografi ElGamal ditunjukkan dalam Tabel 1.(Rinartha, 2011)

Tabel 1. Proses-proses yang terjadi dalam kriptografi ElGamal

Penerima	Pengirim
Pembuatan kunci publik	
Sebelum pihak pengirim mengirimkan pesan, pihak penerima harus membuat kunci publik yang akan digunakan untuk melakukan enkripsi pesan. Pihak penerima memilih kunci pribadi (a), kunci publik tambahan (g) yang akan digunakan untuk membuat kunci publik, kemudian pihak penerima membuat kunci publik (A) dengan bentuk matematis $A = ((g + 1)^{(a+1)} \pmod{257}) - 1)$, kemudian pihak penerima mempublikasikan kunci publik A dan kunci publik tambahan g.	
Enkripsi	
	Pengirim memilih pesan (m) yang akan dikirimkan yang kemudian diolah dengan menggunakan kunci publik (A, g) pengirim dan bilangan acak (k) dengan bentuk matematis $C_1 = ((g + 1)^k \pmod{257}) - 1)$ $C_2 = ((m + 1)(A + 1)^k \pmod{257}) - 1)$ kemudian hasil enkripsi C_1 dan C_2 dikirimkan kepada pihak penerima.
Dekripsi	
Pihak penerima akan menerima hasil enkripsi C_1 dan C_2 dan akan mengolah hasil enkripsi tersebut	

sehingga pesan dapat terbaca sesuai dengan pesan aslinya, dengan bentuk matematis Pesan = $(((C_1 + 1)^{(a+1)})^{-1} \cdot (C_2 + 1) \pmod{257} - 1)$.	

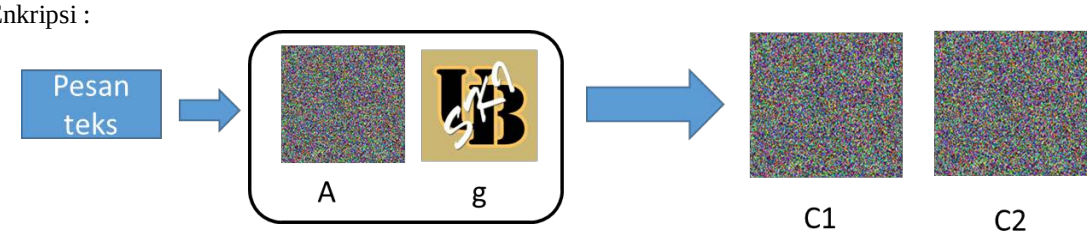
3. 3. Analisa Gabungan Kriptografi ElGamal dan Steganografi Frame

Kriptografi ElGamal dan steganografi frame digabungkan dengan melakukan proses secara berurutan steganografi terlebih dahulu dan kemudian dilanjutkan dengan proses kriptografi. Algoritma gabungan memiliki proses yang cenderung lebih mirip dengan kriptografi yaitu; pembuatan kunci publik, enkripsi dan dekripsi yang ditunjukkan pada gambar berikut:

Pembuatan kunci publik :

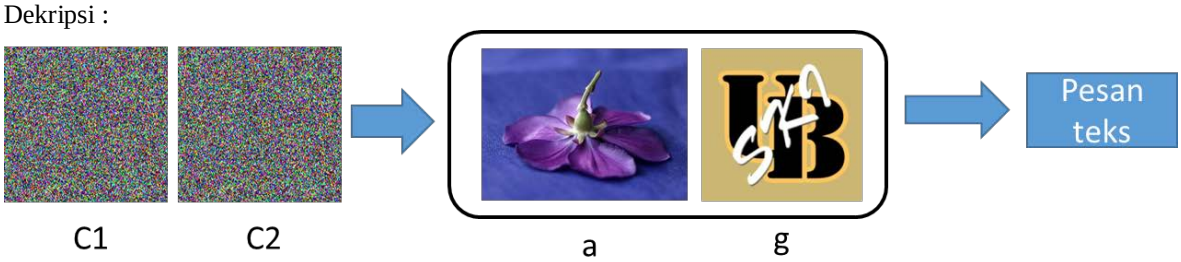
Gambar 6. Proses pembuatan kunci publik algoritma gabungan

Enkripsi :



Gambar 7. Proses enkripsi algoritma gabungan

Dekripsi :



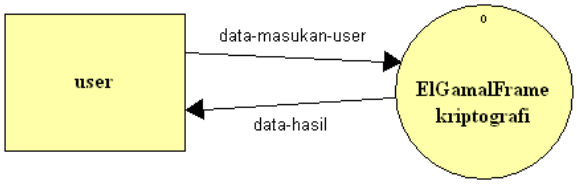
Gambar 8. Proses dekripsi gabungan

3. 4. Implementasi

Perancangan perangkat lunak aplikasi dimulai dari pembuatan *data context diagram* (diagram konteks), yang kemudian dilanjutkan dengan pembuatan *data flow diagram* (DFD) dengan menggunakan aturan Yourdon/DeMarco. Setelah merancang DFD, maka dilanjutkan dengan pembuatan program aplikasi.

a. Diagram Konteks

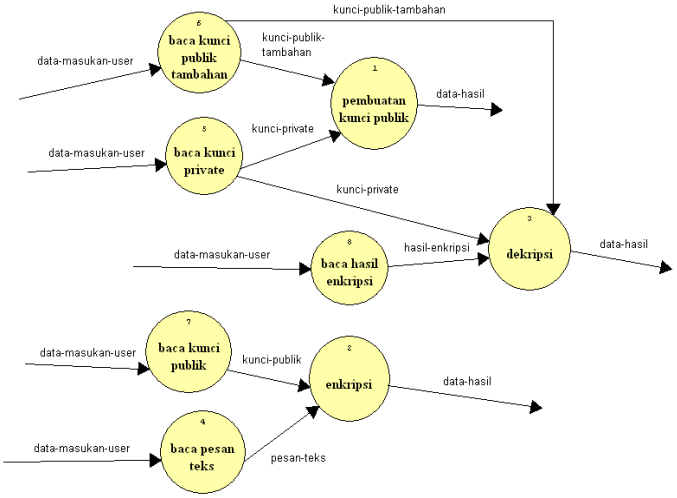
Diagram konteks menggambarkan proses yang terjadi secara umum yang juga disebut dengan *data flow diagram level* 0. Dalam program aplikasi kriptografi ini, terdapat komponen user yang terkait dengan program aplikasi. Diagram konteks ditunjukkan sebagai berikut :



Gambar 9. Diagram konteks

b. *Data Flow Diagram Level* 1

Data flow diagram level 1 merupakan penjabaran pertama dari program aplikasi dan akan dijabarkan secara lebih detail pada data flow diagram level berikutnya. Pada level 1 ini dijelaskan tentang proses-proses utama yang dimiliki oleh program aplikasi untuk melakukan fungsinya. *Data flow diagram level* 1 program aplikasi kriptografi ditunjukkan pada gambar berikut :



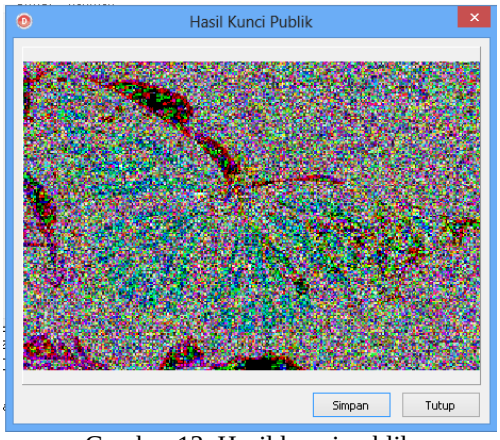
Gambar 10. Data flow diagram level 1

c. Implementasi program

Pada proses pembuatan kunci publik, diperlukan sebuah kunci private dan sebuah kunci publik tambahan yang harus dimasukkan oleh user. Adapun tampilan untuk pengambilan kunci private ditunjukkan pada Gambar 11. Selain itu pengambilan kunci public tambahan ditunjukkan pada Gambar 12. Setelah pengambilan kunci private dan kunci publik tambahan, dihasilkan hasil sebuah kunci publik yang ditunjukkan pada Gambar 13.

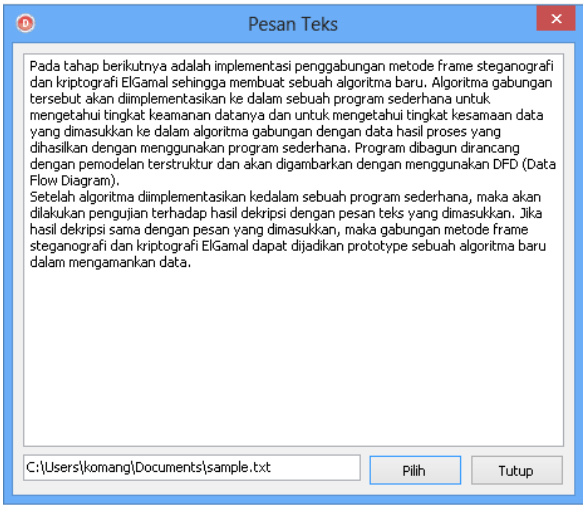
Gambar 11. Pengambilan kunci private

Gambar 12. Pengambilan kunci publik tambahan

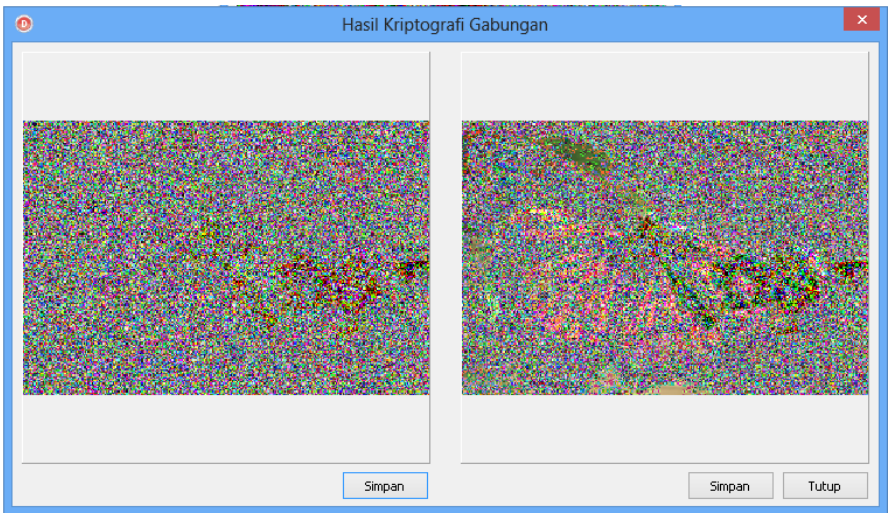


Gambar 13. Hasil kunci publik

Pada proses enkripsi yang diperlukan adalah sebuah kunci publik yang telah ditunjukkan pada Gambar 13, sebuah pesan yang dibuat dalam bentuk file teks dan juga kunci publik tambahan yang telah ditunjukkan pada Gambar 12. Proses pengambilan file teks ditunjukkan pada Gambar 14. Kemudian hasil dari proses enkripsi ditujukkan pada Gambar 15.

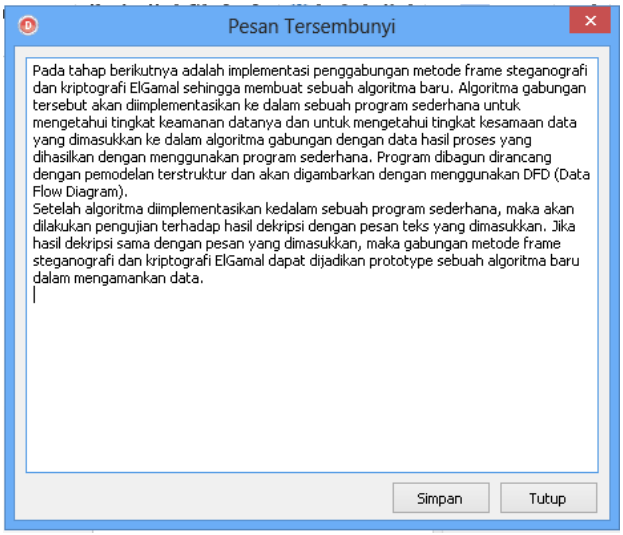


Gambar 14. Pengambilan pesan teks



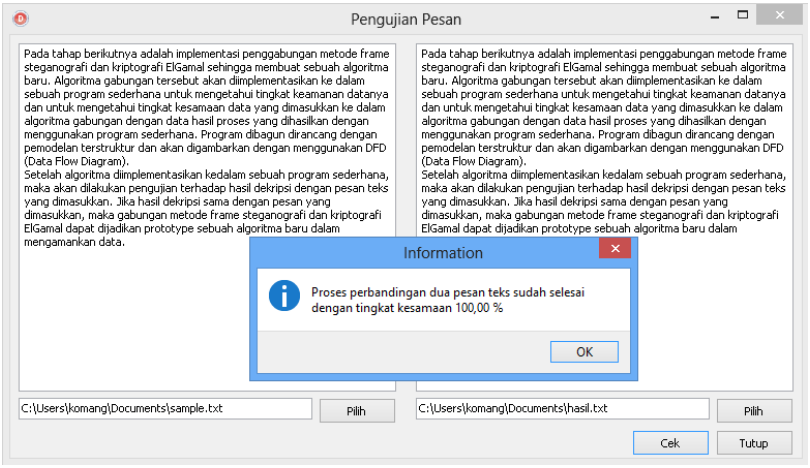
Gambar 15. Hasil enkripsi

Proses dekripsi algoritma gabungan menggunakan beberapa buah data antara lain; sebuah kunci private, sebuah kunci publik tambahan dan gambar hasil dekripsi yang telah ditunjukkan pada Gambar 15. Pengambilan kunci private ditunjukkan pada Gambar 11. Pengambilan kunci publik tambahan ditunjukkan pada Gambar 12. Hasil dari proses dekripsi ditunjukkan pada Gambar 16.



Gambar 16. Hasil dekripsi

Setelah melalui semua proses algoritma gabungan, maka pesan hasil dekripsi diuji tingkat kesamaan dengan pesan asli yang belum mengalami proses enkripsi. Pengujian kesamaan pesan teks ditunjukkan pada Gambar 17.



Gambar 17. Hasil pengujian kesamaan pesan teks

4. Kesimpulan

Dari perancangan, implementasi dan pengujian yang telah dilaksanakan di STMIK STIKOM Bali menunjukkan bahwa

a. Frame steganografi dapat digunakan untuk mengamankan pesan teks dalam sebuah citra digital yang diimplementasikan ke dalam sebuah program sederhana. Hasil proses decode frame steganografi menghasilkan sebuah pesan teks yang sama dengan pesan teks yang diamankan.
b. Gambar yang digunakan sebagai image cover dalam frame steganografi dapat berupa gambar yang memiliki ekstensi *.bmp maupun *.jpg namun untuk gambar yang telah disisipi pesan harus disimpan dalam bentuk bitmap untuk menghindari terjadinya kompresi data.
c. Kriptografi ElGamal dapat digunakan untuk mengamankan sebuah pesan gambar dengan menggunakan gambar sebagai kunci public maupun sebagai kunci private.

d. Gabungan frame steganografi dan kriptografi ElGamal dapat digunakan untuk mengamankan pesan teks dengan menggunakan kunci berupa citra digital.
e. Hasil pengujian kesamaan pesan teks dengan pesan hasil dekripsi menunjukkan tingkat kesamaan 100%.

Daftar Pustaka

[1.] Aditya, Yogie., Pratama, Andhika., dan Nurlifa, Alfian. 2010. Studi Pustaka Untuk Steganografi Dengan Beberapa Metode. Prosiding Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010). http://journal.uii.ac.id/index.php/Snati/ article/viewFile/1955/1730, diakses pada tanggal 1 Maret 2013.
[2.] Afif, S. 2009. *Kriptografi*. http://javanusco.files.wordpress.com/2009/01/ kriptografi7.doc, diakses pada 27 Oktober 2010.
[3.] Annonymous. 2010. *Pengantar Kriptografi*. http://www.informatika.org/~rinaldi/ Buku/Kriptografi/Bab-1_Pengantar%20Kriptografi.pdf, diakses pada tanggal 1 Maret 2013.
[4.] Cox, Ingemar J., Miller, Matthew L. dan Bloom, Jeffrey A. 2002. *Digital Watermarking*. Harcourt Place, 32 Jamestown Road, London, NW1 7BY, United Kingdom : Academic Press.
[5.] Defls, H dan Knebl, H. 2007. *Introduction to Cryptography - Principles and Applications*. Springer-Verlag Berlin Heidelberg.
[6.] Guiliang, Weiping, Xiaoqiang dan Mengmeng. 2010. *Digital image encryption algorithm based on pixels.* Intelligent Computing and Intelligent Systems (ICIS), IEEE International Conference on. ISBN**:** 978-1-4244-6582-8. Page 769 – 772. Xiamen, China.
[7.] Hassan, M dan Hamdan, T. 2005. *Alternatives to visual cryptography for colored images*. Electronics, Circuits and Systems. ICECS. 12th IEEE International Conference on. ISBN: 978-9972-61-100-1. Page 1 – 4. Gammarth.
[8.] Hoffstein, J., Pipher, J dan Silverman. 2008. *An Introduction to Mathematical Cryptography.* 233 Spring Street, New York : Springer Science+Business Media, LLC.
[9.] Oppliger, R. 2005. *Contemporary Cryptography*. 685 Canton Street, Norwood : Artech House, Inc.
[10.] Jeyamala, C., GopiGanesh, S dan Raman, G.S. 2010. *An image encryption scheme based on one time pads — A chaotic approach.* Computing Communication and Networking Technologies (ICCCNT), International Conference on, ISBN : 978-1-4244-6591-0. Page 1 – 6. Karur.
[11.] Joux, A. 2009. *Algorithmic Cryptanalysis*. 6000 Broken Sound Parkway NW, Suite 300 : Taylor and Francis Group, LLC.
[12.] Mollin, R. 2007. *An Introduction to Cryptography Second Edition*. 6000 Broken Sound Parkway NW, Suite 300 : Taylor & Francis Group, LLC.
[13.] Rinartha, K. 2010. *Pengamanan Citra Digital Dengan Menggunakan Pengembangan Kriptografi Kunci Public Elgamal*. Prosiding Seminar Nasional Teknologi Informasi dan Aplikasinya Volume 2, Malang : Politeknik Negeri Malang.
[14.] Rinartha, K. 2011. Analisis dan Implementasi Kriptografi Gabungan *Triple Vigenere Cipher* Dan Kriptografi *Elgamal* Menggunakan Citra Digital Sebagai Kunci. Tesis Program Magister dan Doktor Universitas Brawijaya. Malang : Universitas Brawijaya.
[15.] Setyobudi, Ranu. 2011. Steganografi Tepi Gambar dan Kriptografi Multiple Vigenere Untuk Menyembunyikan Data Text Pada Suatu Citra Dijital. Tesis Program Magister dan Doktor Universitas Brawijaya. Malang : Universitas Brawijaya.
[16.] Sukrisno, Utami E. 2007. Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungsi Hash Md5. Prosiding Seminar Nasional Teknologi 2007. http://p3m.amikom.ac.id/p3m/33%20-%20IMPLEMENTASI%20 STEGANOGRAFI%20TEKNIK%20EOF.pdf, diakses pada tanggal 1 Maret 2013
[17.] Wahana Komputer, Tim Penelitian dan Pengembangan. 2003. Konsep Jaringan Komputer dan Pengembangannya. Jakarta : Salemba Infotek.