Jurnal Sarjana Teknik Informatika
Volume 2 Nomor 3, Oktober 2014
e-ISSN: 2338-5197

IMPLEMENTASI KEAMANAN DATA MENGGUNAKAN ALGORITMA BLOWFISH DAN LSB PADA CITRA

[1]Khairul Putra Siregar, [2]Eko Aribowo (0006027001)

[1,2]Program Studi Teknik Infromatika
Universitas Ahmad Dahlan
Prof.Dr.Soepomo,S.H.,Janturan,Umbulharjo,Yogyakarta 55164
[1]Email: sir_egar7@yahoo.co.id
[2]Email: ekoab@tif.uad.ac.id

ABSTRAK

Keamanana informasi merupakan salah satu hal penting namun sering di abaikan di dalam pengelolaan dan pengembangan sistem informasi. Namun sebenarnya ada banyak cara yang di lakukan untuk meningkatkan keamanan informasi yang kita miliki salah satunya menggunakan kriptografi, kriiptografi adalah pengacakan atau pengubahan data pesan menjadi data yang sulit untuk dipahamai. Namun bentuk acak atau tidak wajar dari pesan tersebut terkadang menimbulkan kecurigaan atau rasa penasaran untuk memahami arti dari pesan acak tersebut, maka agar kecurigaan terhadap pesan aca tersebut hilang, pesan tersebut dapat di sisipkan kedalam bentuk data lain seperti citra, audio, video dan lain sebagainya.oleh karena itu dibuat lah penelitian tentang penggabungan kriptografi dengan metode Blowfish dan steganografi dengan metode least Significant Bit (LSB).

Subjek dalam penelitian ini adalah bagaimana mengimplementasikan kriptografi dengan algoritma Blowfish untuk mengubah pesan menjadi kode-kode yang tak bisa dikenali dan kemudian hasilnya disembunyikan dalam sebuah file gambar berformat Bitmap dengan steganografi metode LSB. Pengembangan aplikasi ini meliputi analisis kebutuhan sistem, perancangan DFD dan Flowchart enkripsi dan deskripsi Blowfish dan LSB, perancangan antarmuka dan implementasi program serta pengujian sistem.

Hasil dari penelitian ini adalah suatu Implementasi Keamanan Data Menggunakan Algoritma Blowfish dan LSB pada Citra. Aplikasi ini mampu mengenkripsi pesan dan meyembunyikannya ke dalam sebuah file citra dengan ekstensi BMP. Berdasarkan pengujian program dapat disimpulkan bahwa aplikasi ini bermanfaat dan berguna untuk menjaga keamanan dokumen.

Kata kunci : *Blowfish, Kriptografi, Least Significant Bit (LSB), Steganografi*

A. PENDAHULUAN

Masalah keamanan informasi kurang mendapatkan perhatian bagi perancang dan pengelola sistem informasi serta berada pada urutan setelah tampilan, atau bahkan diurutan terahir dalam daftar hal-hal yang dianggap penting. Apabila

 e-ISSN: 2338-5197

mengganggu performa sistem, sering kali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

Seiring perkembangan dalam teknologi informasi tersebut, saat ini sedang dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam *interruption, interception, modifikasi,* dan *fabrication,* data yang dikirimkan. Masyarakat pengguna jaringan komputer semakin sadar akan perlunya melindungi *privacy* dan se*crecy* informasi dari ancaman penyadapan maupun penyerangan, baik serangan yang berasal dari pihak luar maupun yang berasal dari pihak yang sedang berkomunikasi.

Keamanan suatu informasi pada jaman global ini semakin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan, terutama bagi suatu perusahaan, instansi atau organisasi. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Di mana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya. Sebagian besar informasi tersebut disimpan dalam bentuk teks agar mempermudah penyimpanan, pembacaan, serta mudah dimengerti.

Kemajuan sistem informasi banyak sekali memberikan keuntungan dalam dunia bisnis, selain itu ada juga aspek-aspek dari sisi negatif dari kemajuan sistem informasi tersebut. Sebagai pengguna komputer hampir semua aspek masyarakat menggunakan sistem informasi berbasis komputer, apalagi informasi-informasi mudah didapat dengan adanya jaringan komputer sperti dan internet memungkinkan meyediakan informasi secara cepat dan akurat.

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Dahulu, jumlah komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya *classified* baru dilakukan di sekitar tahun 1950-an.

Security attack, serangan terhadap keamanan sistem komputer, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Salah satu serangan terhadap keamanan adalah *Interception* yaitu Pihak yang tidak berwenang berhasil mengakses data atau informasi, yang mana serangan ini bisa terjadi seperti pada jaringan LAN (*Local Area Network*) atau bahkan pada komputer yang tidak terhubung jaringan sekalipun.

Beberapa cara telah dikembangkan untuk menangani masalah keamanan ini, salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini semakin banyak jumlahnya, sejalan dengan berkembangannya ilmu yang mempelajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data, untuk menjaga kerahasiaan suatu data salah satunya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *ciphertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan biasa (yang mudah dibaca)

 e-ISSN: 2338-5197

disebut dekripsi. Pesan biasa atau pesan asli disebut *plaintext* sedangkan pesan yang telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan *cpihertext*.

Sebuah algoritma kriptografi dikatakan aman (*computationally secure*) bila memenuhi tiga kriteria berikut :

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.
2. Biaya untuk memecahkan *chipertext* melampaui nilai informasi yang terkandung di dalam *chipertext* tersebut.
3. Waktu yang diperlukan untuk memecahkan *chipertext* melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

Serangan terhadap kriptografi pada dasarnya adalah memecahkan (membongkar keamanan) algoritma kriptografi, yang selanjutnya digunakan untuk usaha mengupas data tersandi tanpa mengetahui/menggunakan kunci. Kegiatan ini (memecahkan Algoritma kriptografi) adalah bagian dari kriptoanalisis, yaitu ilmu/seni memecahkan data tersandi. Kriptoanalisis dan kriptografi merupakan sebuah cabang ilmu pengetahuan yang disebut kriptologi.

Kriptoanalisis dapat pula diartikan sebagai seni atau ilmu untuk memecahkan cipherteks menjadi plainteks dengan memanfaatkan celah-celah keamanan sebuah sistem kriptografi. Hal inilah yang menjadikan kriptoanalisis dicap sebagai cara ilegal untuk menterjemahkan cipherteks.

Algoritma kriptografi yang di pakai untuk penelitian ini adalah algoritma blowfish. Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem* , metoda enkripsinya mirip dengan *DES* diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan *cache* data yang besar).

Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 *clock cycle per byte*, kompak dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variabel dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, *Multiple* 8 bit, *default* 128 bit).Blowfish dioptimasikan untuk berbagai aplikasi dimana kunci tidak sering berubah, seperti pada jaringan komunikasi atau enkripsi file secara otomatis. Dalam pengimplementasiannya dalam komputer bermicroprosesor 32-bit dengan *cache* data yang besar (Pentium dan Power PC) Blowfish terbukti jauh lebih cepat dari DES. Tetapi Blowfish tidak cocok dengan aplikasi dengan perubahan kunci yang sering. Blowfish pun tidak dapat digunakan pada aplikasi kartu pintar (*smart card*) karena memerlukan memori yang besar.

Selain kriptografi, cara yang bisa dipakai dalam pengamanan data adalah steganografi. Penggunaan steganografi antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang disandikan (*chiper text*) tetap tersedia, maka dengan steganografi chiperteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya.

 e-ISSN: 2338-5197

Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Steganografi dapat digolongkan sebagai salah satu bagian dari ilmu komunikasi. Kata steganografi berasal dari bahasa Yunani yang berarti "tulisan tersembunyi". Pada era informasi digital, steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan

Sedangkan dalam penelitian ini metode yang digunakan dalam penyembunyian pesan adalah metode LSB (*Least Significant Bit*). Metode ini merupakan metode yang sangat sederhana dan yang paling banyak digunakan dalam peyembunyian data. Dan metode ini paling terkenal diantara metode steganografi lainny, seperti metode spasi terbuka, metode *masking* dan *filtering* serta metode *Bit Plane Complexity Steganography* (BPCS)

Penggabungan dua teknik keamanan data yakni kriptografi dengan menggunakan metode blowfish dan steganografi dengan menggunakan metode LSB diharapkan mampu mengamanankan data, di mana kritpografi berfungsi untuk mengkodekan data sedangkan steganografi berfungsi untuk menyisipkan pesan, sehingga pesan yang sudah dienkripsi kemudian disembunyikan sehingga keberadaan pesan sulit untuk diketahui.

B. METODE PENELITIAN

Metode penelitian merupakan suatu cara yang ilmiah y ang digunakan dalam memperoleh suatu masalah dengan tujuan tertentu. Cara ilmiah berarti kegiatan penelitian ini dilandasi oleh metode keilmuan. Metode penelitan ini berisi panduan tentang urut-urutan bagaimana penelitian itu dilakukan. Desain penelitian harus sesuai dengan metode penelitian yang dipilih, prosedur, serta alat penelitian juga harus cocok. Sedangkan langkah-langkahnya adalah mengumpulkan data, analisis data, desain sistem, pengkodean sistem, dan meguji sistem.

C. SUBYEK PENELITIAN

Subyek dalam penelitian ini adalah bagaimana mengubah teks menjadi kode-kode yang tidak bisa dikenali lagi dengan menggunakan algoritma Blowfish kemudian hasil dari kode-kode tersebut ditempelkan atau disembunyikan pada sebuah gambar atau citra yang memiliki ekstensi *.bmp dengan menggunakan metode LSB. Kemudian mengambil kode-kode yang telah ditempelkan kemudian mengembalikannya dalam bentuk teks aslinya. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi menggunakan bahasa pemrograman *Borland Delphi* 7. Beberapa bahan penelitian yang akan digunakan dalam penelitian ini antara lain:

1. Teks yang akan diubah menjadi kode-kode.
   Teks ini yang nantinya akan dikodekan terlebih dahulu sebelum disembunyikan.
2. Citra atau gambar untuk menyembunyikan pesan.
   Citra atau gambar yang digunakan untuk menyembunyikan hasil dari kode-kode tersebut adalah citra atau gambar yang memiliki format *.bmp.
3. Algoritma kriptografi.

 e-ISSN: 2338-5197

Algoritma kriptografi yang digunakan adalah algoritma kriptograpi simetris yang menggunakan kunci enkripsi sama dengan kunci dekripsi. Algoritma ini berjenis simetris *block cipher*.

4. Algoritma steganografi.
   Algoritma steganografi yang digunakan adalah algoritma steganografi yang berjenis *spatial domain* atau ranah spasial.
5. Metode dalam algoritma pemrograman
   Metode yang digunakan adalah algoritma kriptograpi simetris Blowfish sedangkan untuk steganografi menggunakan metode LSB.

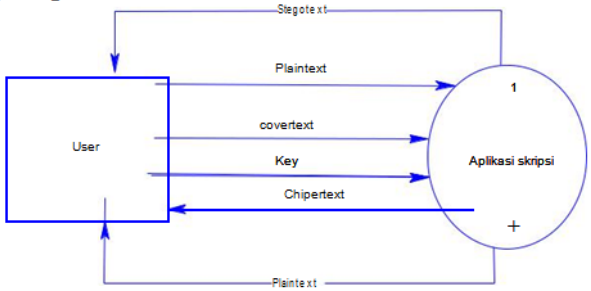
D. ANALISIS KEBUTUHAN SISTEM

Mencermati segala keperluan pengguna untuk mencapai tujuan dari sistem yang dibuat. Dimana pada tahap ini yaitu tahap analisis kebutuhan adalah tahap yang paling penting karena kesalahan pada tahap ini akan menyebabkan kesalahan pada tahap selanjutnya. Adapun langkah pertama dari proses analisis sistem menyangkut analisis kebutuhan sistem adalah memahami dan menentukan tujuan yang ingin dicapai.

E. PERANCANGAN SISTEM

Dalam tahap perancangan sistem ini, digunakan beberapa tahapan pemodelan sistem, sehingga dapat menghasilkan sebuah penelitian yang sesuai dengan apa yang diharapkan. Perancangan sistem ini meliputi:

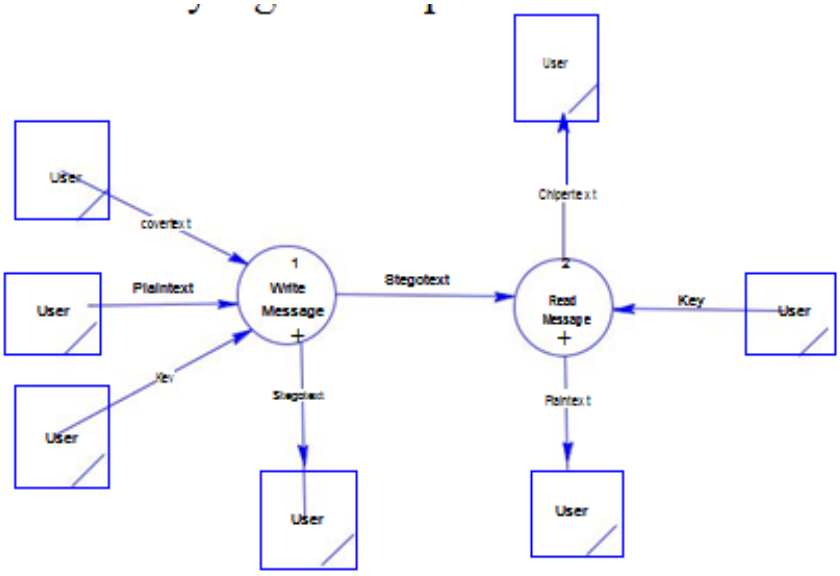
1. Perancangan Diagram Konteks.
   Tahapan ini digunakan untuk menggambarkan seluruh sistem yang akan dibuat, yang nantinya akan diimplementasikan dalam sebuah program aplikasi. Dari proses pertama sampai dengan proses terahir.



Gambar 1: diagram korteks

2. Perancangan DFD (*Data Flow Diagram*)
   Untuk lebih memperjelas sistem yang telah digambarkan dalam Diagram konteks, maka perlu dibuat sebuah DFD. DFD ini mencakup DFD enkripsi dan DFD deskripsi sebagai pemodelan alur data yang akan diproses di dalam sistem.

 e-ISSN: 2338-5197

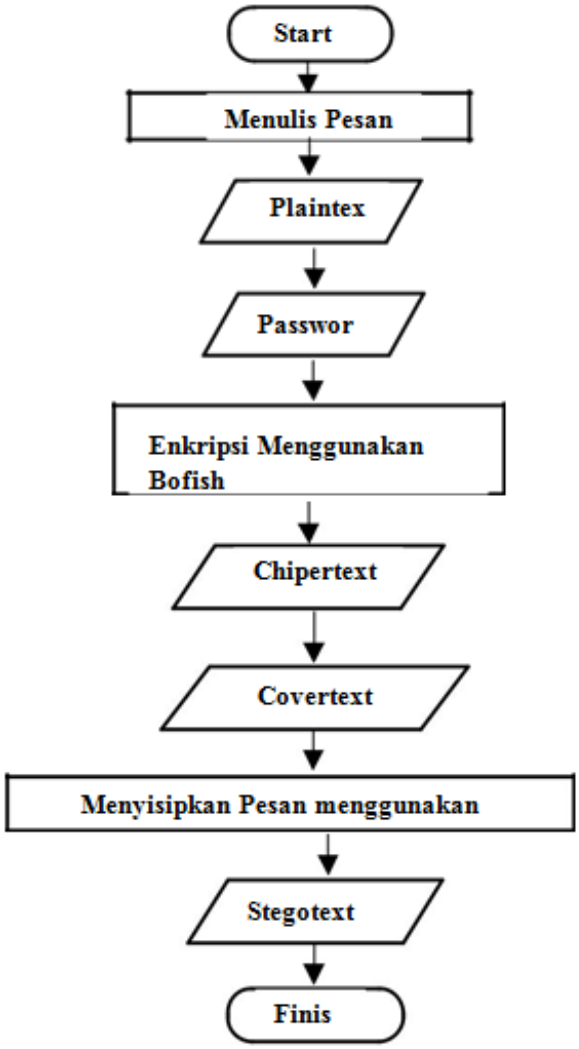


Gambar 2: DFD

3. Perancangan *Flowchart*

   Perancangan *flowchart* ditujukan untuk mempermudah pembuatan program. Dalam ini *Flowchart* dirancang untuk menjelaskan langkah-langkah apa saja yang harus dilakukan oleh *programmer* agar sistem yang dibuat dapat menghasilkan *output* yang sesuai dengan harapan dari *input*-an yang dimasukkan oleh *user*. Dalam penelitian ini *flowchart* dibuat proses dari *plaintext* yang dienkripsi mengunakan metode Blowfish yang menghasilkan *chipertext*, yang kemudian di masukan kedalam citra bertipe *bitmap* menggunakan metode LSB yang menghasilkan *stegotext*. Kemudian data yang berupa stegotext tersebut dikeluarkan dari mediumnya yng berupa cira kembali menjadi *chipertext,* dan dideskripsi menggunakan metode Blowfish untuk mendapatkan pesan asli atau *plaintext.*

 e-ISSN: 2338-5197



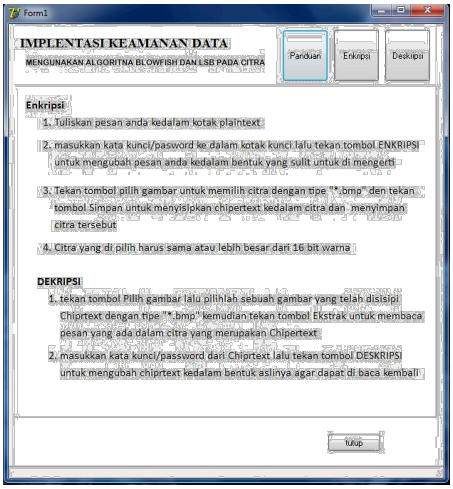
Gambar 3: flowcart

F. IMPLEMENTASI PROGRAM

Tahap ini merupakan pengimplementasian algoritma kriptografi Blowfish dan steganografi metode LSB untuk kemananan data dalam bentuk teks. Program yang digunakan untuk proses pengkodean dalam pembuatan program aplikasi keamanan data dengan menggunakan Borland Delphi 7.

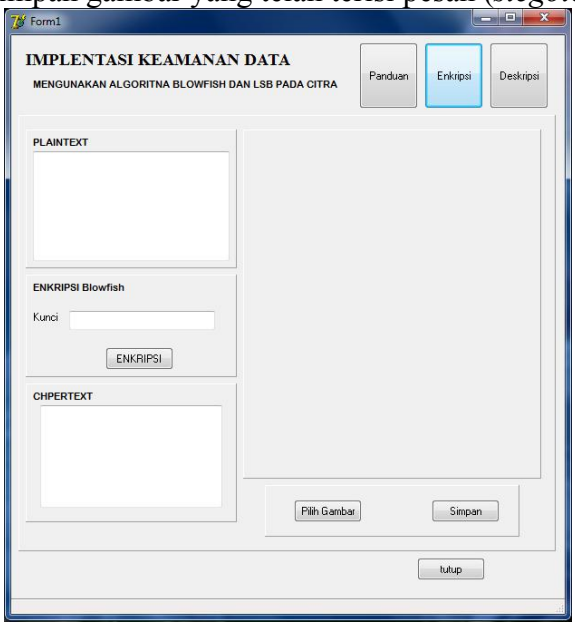
Pada gambar 4.15 merupakan form Panduan (Utama), pada form ini terdapat empat tombol yang berfungsi sebagai menu untuk menghubungkan antara form yang satu dengan form yang lainnya. tombol Enkripsi berfungsi untuk memanggil *form* Enkripsi, tombol Deskripsi berfungsi untuk memanggil *form* Deskripsi, dan tombol panduan berfungsi sebagai *form* panduan, yang mana *form* panduan juga merupakan *form* utama program ini, di form ini tuntunan atau panduan bagai mana cara menggunakan aplikasi ini.

 e-ISSN: 2338-5197



Gambar 4: *Form* Utama

Pada gambar 5 merupakan *form Enkripsi,* di mana pada *form* ini merupakan tempat enkripsi serta menyisipkannya, tombol Enkripsi digunakan untuk mengenkripi pesan dengan kata kunci yang telah diisi sehingga pesan tersebut menjadi *chipertext*, tombol Pilih Gambar digunakan untuk mencari atau memilih citra yang akan digunakan untuk menyisipkan pesandan harus berekstensi BMP, tombol Simpan digunakan untuk menyispkan hasil enkripsi (*chipertext*) ke dalam gambar dan langsung menyimpan gambar yang telah terisi pesan (*stegotext*)didalamnya.

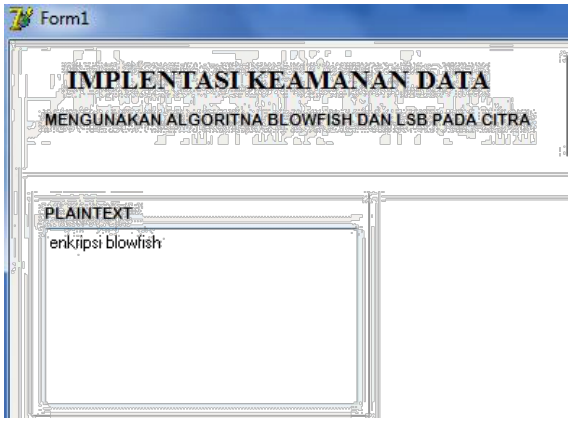


Gambar 5: *Form Enkripsi*

Untuk proses Enkripsi langkah-langkahnya adalah sebagai berikut:

1. Langkah pertama adalah memasukan pesan yang akan dienkripsi kedalam kotak plalintext, sebagai contoh kita masukkan kata “enkripsi blowfish”.

 e-ISSN: 2338-5197

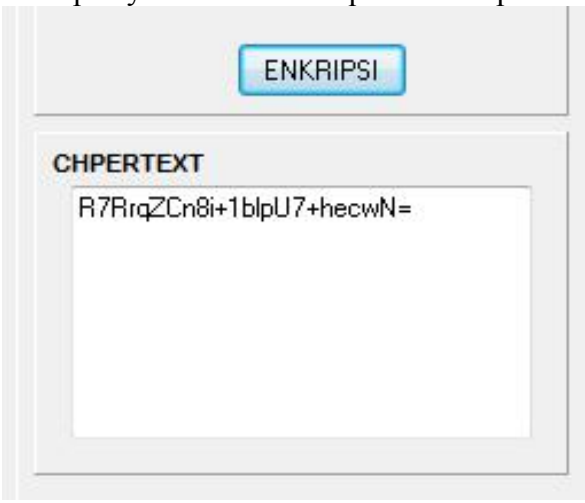


Gambar 6: contoh pengisian plaintext

2. kemudian masukan password, agar pesan tersebut menjadi aman keberadaannya,dan untuk password kita beri contoh “123”.

Gambar 7: contoh pengisian password

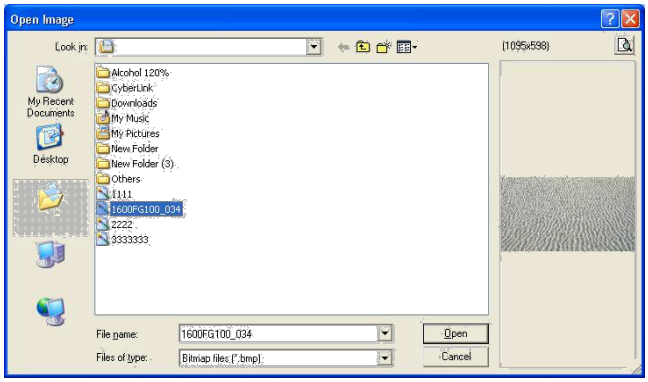
3. setelah itu pilih tombol Enkripsi, agar terjadi pesan yang sudah ada (Plaintext) diproses menjadi pesan yang terenkripsi (chipertext), berdasarkan contoh sebelumnya hasil enkripsinya adalah “R7RrqZCn8i+1blpU7+hecwN=”.



Gambar 8: contoh hasil enkripsi

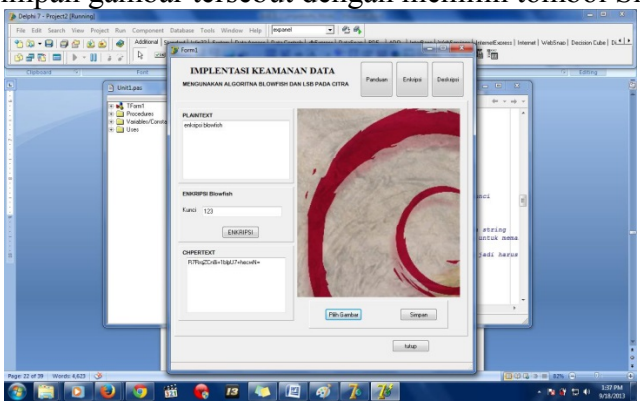
4. Lalu gambar yang akan di gunakan untuk menyisipkan pesan (covertext) dengan meilih tombol Pilih Gambar, maka akan muncuk open picture dialog seperti berikut ini.

 e-ISSN: 2338-5197



Gambar 9: Proses Ambil Gambar

5. Kemudian lakukan penyisipan hasil enkripsi (chipertext) ke dalam gambar dan langsung menyimpan gambar tersebut dengan memilih tombol Simpan.



Gambar 10: contoh gambar yang akan di sisipkan

G. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan beberapa hal sebagai berikut :

1. Telah dihasilkan suatu aplikasi steganografi yang menggunakan algoritma kriptografi untuk keamanan data bertipe plaintext menggunakan bahasa pemprograman *Borland Delphi 7.0*.
2. Proses pengujian aplikasi keamanan data dengan metode *black box test* dan *alpha test*. Aplikasi diujikan kepada beberapa responden, hasilnya adalah aplikasi ini sangat bermanfaat untuk mengamankan dokumen agar isinya tidak diketahui oleh orang lain.
3. Implementasi program ini menghasilkan suatu aplikasi yang dapat mengubah isi suatu dokumen (*plaintext*) yang berupa teks, menjadi kode-kode yang tidak dikenal (*ciphertext*). Kemudian menysisipkannya pada *file* citra sehingga tidak diketahui keberadaannya. Setelah itu *chipertext* dirubah menjadi dokumen aslinya (*plaintext*).
4. Aplikasi dapat menghasilkan *file stegotext* yang sama ekstensinya dengan *stegomedium* yang digunakan untuk menyisipkan pesan pada proses enkripsi.
5. Aplikasi ini juga dapat mampu mengembalikan *stegotext* ke dalam bentuk chipertext pada proses Deskripsi
6. Aplikasi keamanan data ini diimplementasikan dengan menggabungkan dua metode algoritma yaitu algoritma kriptografi *BLOWFIST* dan steganografi *LSB*.

 e-ISSN: 2338-5197

H. SARAN

Beberapa saran yang dapat diberikan untuk pengembangan aplikasi ini adalah sebagai berikut :

1. Aplikasi ini hanya untuk keamanan *file* yang dibatasi pada *file* .txt. untuk pengembangan selanjutnya diharapkan dapat dibuat aplikasi yang mampu mengamankan semua jenis *file*.
2. Aplikasi ini hanya menggunakan *file* citra sebagai *stegomedium*, sehingga dalam pengembangannya diharapkan bisa menggunakan semua bentuk *file* sebagai *stegomedium*.
3. Aplikasi ini hanya untuk keamanan dokumen sistem operasi *windows* (*Windows Operating System)*. Oleh karena itu, diharapkan untuk pengembangan selanjutnya dapat dibuat aplikasi yang mampu dijalankan pada sistem operasi lain, misalnya *Linux* dan *Apple*.
4. Aplikasi ini menggunakan algoritma kriptografi *BLOWFIST* dan *LSB* untuk pengembangan selanjutnyanya diharapkan agar dapat dibuat suatu aplikasi keamanan dokumen dengan algoritma lain, karena masih banyak algoritma kriptografi dan steganografi yang perlu dikaji lagi.

DAFTAR PUSTAKA

A.R Akmal, 2009, "*Implementasi Keamanan Data Dengan Kombinasi Algoritma RSA, DES, GOST",* Skripsi S-1, Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta.

Adhitya, Rhesa, 2006, "*Studi dan Deteksi Steganografi pada File Bertipe JPEG dengan Steganographic System"*, Departemen Teknik Informatika, Institu Teknologi Bandung.

Aribowo, Eko, 2002, "*Organisasi Berkas"*, Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta.

Dini, Armyta, 2006, "*Studi Mengenai Aplikasi Steganografi Camuflage Beserta Pemecahan Algoritma"*, Departemen Teknik Informatika, Institut Teknologi Bandung.

Hardinan, Imam, 2005, "*Pengamanan Informasi Menggunakan LSB pada Metode Steganography Menggunakan Delphi"*, Skripsi S-1, Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta.

Nazir, M., "*Metode Penelitian"*, Ghalia Indonesia, Jakarta.

Rahayu, Baeti, 2005, "*Pengamanan Data Teks dengan Teknik LSB"*, Skripsi S-1, Ilmu Komputer, Universitas Gajah Mada. Yogyakarta.

Rahman, Chumaidi, 2009, "Sutdy Implementasi Algoritma *Blowfish* untuk Enripsi Email, Makalah Tugas Akhir", Institut Sepuluh November.

Setiadi, Tedy, 2006, "*Modul Analisis dan Desain Sistem Informasi"*, Teknik Informatika, universitas Ahmad Dahlan, Yogyakarta.

Usman, Fadli, 2009, "*Keamanan Data Bertingkat Menggunakan Algoritma Simetris Ghost dan Rijndael",* Skripsi S-1, Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta.