# Analisa Aplikasi Keamanan Data dengan Cryptography dan Steganography menggunakan Visual Basic.Net 2010

Farizal Herry Saputra
Teknik Informatika, Program Pascasarjana, Universitas Pamulang
*e-mail*: farizal.saputra@doktersiber.id

**Abstrak—Keamanan data yang menjadi sebuah pesan saat ini mulai rentan terhadap pencurian data dari pesan tersebut karena kini penggunaan email gratis (*free mail*) sudah semakin banyak dan tidak menjamin terhadap keamanan dari data atau pesan yang akan dikirimkan dari pengirim (*sender*) kepada penerima (*receiver*). Melihat kondisi diatas penulis bermaksud melakukan penelitian untuk memberikan solusi sistem keamanan data sesuai dengan model kebijakan keamanan informasi CIA triad (*confident, integrity, availability*) dalam bentuk pesan ini, sehingga menjamin keamanan bagi pemilik pesan atau hingga diterima nya pesan tersebut oleh penerima. Metode pendekatan system yang digunakan oleh penulis pada system informasi ini menggunakan metode program berorientasi objek (*Object Oriented Programming*) dengan metodologi *sequential linier* terdiri dari pentahapan : analysis, design, coding, testing. Aplikasi system keamanan yang dibuat ini mampu mengolah data berupa teks menggunakan persandian (*cryptography*) dan penyisipan teks pada media gambar (*steghanography*) dengan menggunakan *Visual Basic .Net 2010* sebagai media *development* aplikasi keamanan data ini. Sehingga memungkinkan system ini mengamankan data yang bersifat rahasia berdasarkan kekuatan kunci persandiaan dan penyisipan teks pada media gambar. Aplikasi system keamanan ini dapat dimanfaatkan bagi masyarakat dan khusus nya lembaga atau institusi pemerintah dalam bidang keamanan negara untuk menyimpan data atau menyampaikan data berupa pesan kepada penerima pesan antar institusi dengan tingkat pengamanan data yang sangat baik.**

***Kata Kunci*—Keamanan Data; *Object Oriented Programming*; Kriptografi; Steganografi; Vb. Net 2010**

## I. PENDAHULUAN

Di dunia digital cyber seperti sekarang ini masih sangat minim tingkat keamanan dalam bidang teknologi informasi seperti halnya keamanan data penting atau rahasia (*secret*), yang mungkin akan didelegasikan kepada orang tertentu dan tidak dapat diketahui orang lain kecuali orang yang sudah di tentukan oleh pengirim untuk menerima file atau pun pesan tersebut dari si pengirim, karena penggunaan media pengiriman yang menggunakan jaringan akses publik, sangat mudah sekali dilakukan pencurian data dari pesan penting oleh orang – orang yang tidak bertanggung jawab dan kemudian menyebarkan nya atau bahkan menjadi milik pribadi si pencuri pesan tersebut.

Adam O'Donnell, (*director of emerging technologies at message security vendor Cloudmark Inc.*) mengatakan bahwa *automated password-reset* merupakan kebijakan pada mail berbasis web terlepas layanan itu gratis seperti *yahoo, hotmail, gmail,* atau berlangganan, pada *internet service provider* [1].

Untuk menghadapi masalah tersebut seorang pemilik data dari pesan yang bersifat penting atau rahasia (*secret*) dapat mengamankan data tersebut, jika ingin melakukan pengiriman menggunakan jaringan non publik sehingga dapat meminimalisir terjadinya pencurian data dari pesan tersebut. Terkadang masih tetap ditemukan celah pada jaringan non publik untuk seorang hacker melakukan pembobolan jaringan non publik dan mengambil data – data penting yang dikirimkan dari seorang pengirim (*sender*) kepada seorang penerima (*receiver*). Penting nya mengetahui tentang keamanan data sebagai usaha untuk melindungi dan menjamin tiga aspek terpenting dalam dunia keamanan siber seperti kerahasian data, keutuhan data dan ketersedian data (Grafinkel & Lipford, 2014) [2].

Keamanan data sendiri merupakan bagian dari perkembangan teknologi informasi. Ketika mulai berpikir bahwa data yang di miliki merupakan data yang sangat penting, maka harus berusaha untuk melindunginya agar jangan sampai jatuh ke tangan orang yang tidak bertanggung jawab[3]. Untuk menangani kekhawatiran dalam proses pengiriman data yang bersifat rahasia tapi keamanan data tetap terjaga secara privasi, maka perlu ada nya penggunaan keamanan data dengan sistem cryptography dan steganography pada saat dilakukan pengiriman data melalui jaringan publik yang menggunakan *push mail*.

Kriptografi (c*ryptography*) sebagai ilmu ataupun seni dalam mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman (Schneier, 1996). Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptology). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer [4].

Steganografi (*steganography*) berasal dari bahasa yunani yaitu steganos, yang artinya "tersembunyi atau terselubung" , dan graphein, "menulis". Steganografi adalah proses penyimpanan pesan rahasia berupa teks dalam bentuk lain sehingga tidak diketahui oleh orang lain. Berbagai macam steganografi antara lain menyembunyikan pesan dalam file gambar, file audio dan file video[5]. *Steganography* adalah ilmu menyembunyikan teks pada media digital yang telah ada, sehingga teks yang tersembunyi

dapat menyatu dengan media digital, Media yang digunakan sebagai tempat penyembunyian pesan tersembunyi dapat berupa gambar, audio dan video. Steganography yang kuat memiliki sifat media yang tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi dapat diekstraksi[6].

Dengan memanfaatkan *free email* sebagai contoh: *gmail.com*, *mailyahoo.com*, *hotmail.com*, dll. Akan tetapi dari sekian banyak *email* gratisan tersebut tidak disarankan untuk pemilik perusahaan mengirimkan dokumen yang bersifat rahasia melalui *free mail*, dikarenakan tingkat keamanan yang masih bisa di tembus keamanan nya sehingga data – data di dalam email dari pengirim kepada penerima dapat diambil dan bahkan dimanfaatkan untuk kepentingan pribadi nya. Khusus nya di sebuah instansi pemerintahan yang berkaitan dengan keamanan negara, seperti indonesia ada sebuah lembaga yang menangani terkait sebuah keamanan dalam bidang teknologi informasi yaitu Badan Siber dan Sandi Negara yang khusus bertugas bertugas menyelenggarakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua pihak yang terkait dengan keamanan siber [7].

Untuk itu penulis membuat aplikasi keamanan data yang dapat mengamankan data serta pesan yang terenkripsi sehingga walaupun data – data tersebut diambil oleh orang yang tidak berkepentingan data tersebut akan tetap aman dan bahkan tidak tahu bahwa di sebuah gambar dengan menggunakan konsep steganography orang tersebut tidak tahu bahwa terdapat data dari pesan tersebut di dalamnya.

## II. METODE PENELITIAN

Metodologi yang digunakan oleh penulis berdasarkan dari masalah yang telah diidentifikasi menjadi, rumusan masalah, dan batasan dari masalah sehingga penelitian ini dapat dijalankan dengan dua metode yaitu:

### *A. Metode Pengumpulan Data*

*1) Observasi*

Aktivitas yang dilakukan makhluk cerdas, terhadap suatu proses atau objek dengan maksud merasakan dan kemudian memahami pengetahuan dari sebuah fenomena berdasarkan pengetahuan dan gagasan yang sudah diketahui sebelumnya, untuk mendapatkan informasi-informasi yang dibutuhkan untuk melanjutkan suatu penelitian.

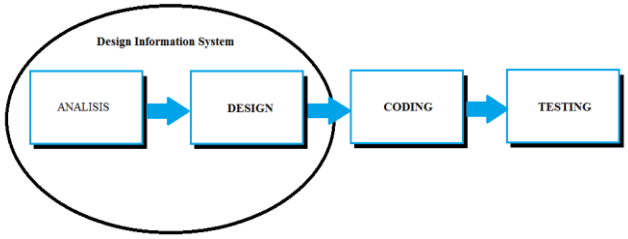
*2) Studi Pustaka*

Kegiatan Studi Pustaka merupakan kegiatan pengumpulan data untuk mencari teori-teori pendukung dalam membuat sebuah aplikasi. Penulis pada kegiatan studi pustaka membaca dan mempelajari dari beberapa media informasi sebagai referensi seperti buku, artikel, tulisan ilmiah, internet, ebook dan perpustakaan.

### *B. Metode Pengembangan Perangkat Lunak*

Rekayasa perangkat lunak dalam penelitian ini yang memfokuskan pada awal sebuah perancangan design dari sebuah sistem yang akan dibangun atau dikembangkan berdasarkan metode, proses dan alat bantu (*tools*). Perangkat lunak saat ini, memiliki dua peran. Di satu sisi berfungsi sebagai sebuah produk, dan di sisi lain sebagai kendaraan sebuah produk. Sebagai produk, perangkat lunak mengantarkan potensi perhitungan yang dibangun oleh perangkat lunak komputer. Sebagai kendaraan yang dipakai untuk mengantarkan produk, perangkat lunak berlaku sebagai dasar untuk kontrol komputer (*operating system*), komunikasi informasi (*network*), dan penciptaan serta kontrol dari program-program lain (peranti dan lingkungan perangkat lunak).

Tahapan ini merupakan tahapan untuk membuat perencanaan sistem yang akan dibangun dari beberapa model pengembangan perangkat lunak, maka dalam perancangan perangkat lunak penulis menggunakan model sekuensial linier, karena pada model sekuensial linier mengusulkan sebuah pendekatan kepada perkembangan perangkat lunak yang sistematik dan sekuensial yang di mulai pada tingkat dan kemajuan sistem pada seluruh analisa, design, kode ,pengujian dan pemeliharaan.




Gambar 1.
Siklus hidup sequential linier

*1) Analysis*

Proses pengumpulan kebutuhan diintensifkan dan difokuskan, khususnya pada perangkat lunak. Untuk memahami sifat program yang dibangun, perekayasa perangkat lunak (analis) harus memahami domain informasi, tingkah laku, untuk kerja, dan antar muka (interface) yang diperlukan. Kebutuhan sistem maupun perangkat lunak didokumentasikan dan dilihat lagi dengan pelanggan.

*2) Design*

Desain perangkat lunak sebenarnya adalah proses multilangkah yang berfokus pada empat atribut sebuah program yang berbeda, struktur data, arsitektur perangkat lunak, representasi interface, dan detail (algoritma) prosedural. Proses desain menerjemahkan syarat/kebutuhan ke dalam sebuah representasi perangkat lunak yang dapat diperkirakan demi kualitas

sebelum dimulai coding dari sebuah program. Sebagai persyaratan, desain didokumentasikan dan menjadi bagian dari konfigurasi perangkat lunak.

3) *Coding*
Desain telah dibuat dilanjutkan dengan tahapan sebuah desain harus diterjemahkan ke dalam bentuk Bahasa mesin yang bisa dibaca. Langkah pembuatan kode melakukan tugas ini. Jika desain dilakukan dengan cara yang lengkap, pembuatan kode dapat diselesaikan dengan cara mekanis.

4) *Testing*
Setelah proses pembuatan kode, pengujian program dimulai. Proses pengujian berfokus pada logika internal perangkat lunak, memastikan bahwa semua pernyataan telah diuji, pada eksternal fungsional yaitu mengarahkan pengujian untuk menemukan kesalahan-kesalahan dan memastikan input yang dibatasi akan memberikan hasil yang aktual yang sesuai dengan hasil[8].

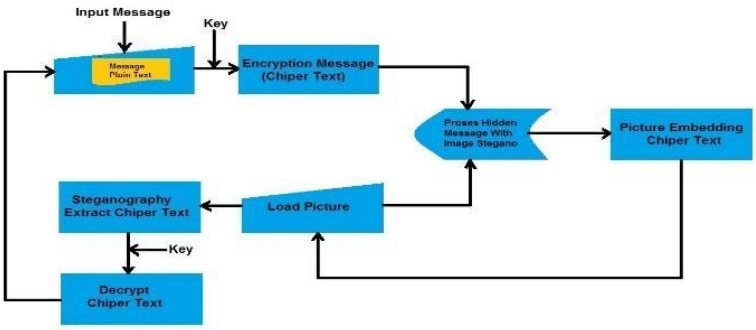
## III. PERANCANGAN SISTEM

Metode merupakan prosedure atau cara mengetahui sesuatu dengan langkah-langkah sistematis,16 yang akan dilakukan dalam proses penelitian terhadap sebuah obyek penelitian[9].

### *A. Analisa Sistem*

Dari tahapan ini kebutuhan (*requirement*) dari user adalah aplikasi yang memiliki tingkat keamanan data yang menjadi sebuah pesan tetap terjamin keamanan nya dan tidak mudah diubah (*modification*) dan disadap (*Intercept*) jika pesan tersebut dikirimkan lewat *free mail* seperti, Google.Inc. dengan gmail, Microsoft Corp. dengan windows live hotmail, dan Yahoo.Inc.

Berdasarkan kebutuhan tersebut membuat alur kerja dari setiap proses dari aplikasi tersebut dengan membuat block chart yang memiliki fungsi untuk memodelkan masukkan, keluaran, referensi, master proses ataupun transaksi dalam simbol – simbol tertentu. Pada dasarnya tidak berorientasi pada fungsi, waktu ataupun aliran data, tetapi lebih ke arah proses. Dengan menggunakan block chart proses dari aplikasi cryptography dan steganography ini dapat digambarkan dengan block chart, seperti berikut ini :




Gambar 2.
block chart proses cryptography dan steganography

Kerahasiaan sebuah pesan dari analisa tersebut terletak pada kekuatan enkripsi pesan itu sendiri dengan mengikuti acuan kekuatan password enkripsi pesan tersebut seperti pada tabel dibawah ini.

Tabel 1.
*karakter berbanding waktu bruteforce attack*

| Panjang Password | Penggunaan Karakter | | | |
|---|---|---|---|---|
| | Huruf Kecil | Huruf Kecil dan Angka | Huruf Besar dan Kecil | Semua Pritable Karakter ASCII |
| < = 4 | Instan | | | 2 menit |
| 5 | Instan | 2 menit | 12 menit | 4 jam |
| 6 | 10 menit | 72 menit | 10 Jam | 18 hari |
| 7 | 4 Jam | 43 Jam | 23 hari | 4 tahun |
| 8 | 4 hari | 65 hari | 3 tahun | 463 tahun |
| 9 | 4 bulan | 6 tahun | 178 tahun | 44530 tahun |

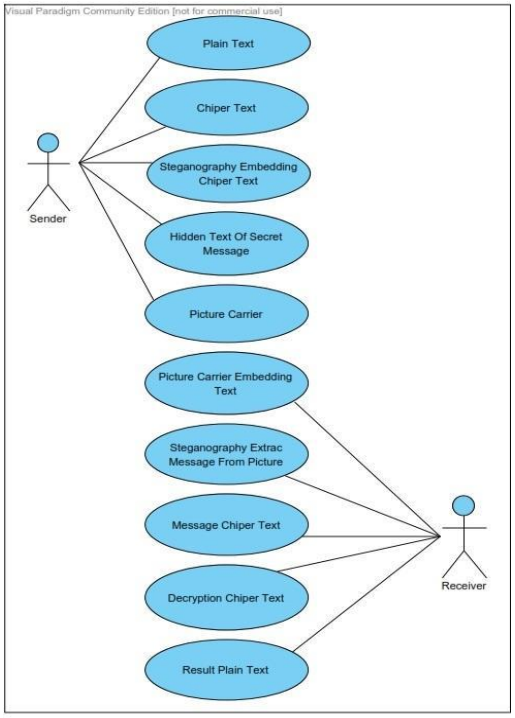
Tabel tersebut berdasarkan hasil uji dari brute force attack yang merupakan calculator perhitungan kekuatan password untuk bisa dibuka oleh orang lain dengan ada nya acuan tersebut. Seorang programmer dapat membuat aplikasi enkripsi dengan mempertimbangkan kekuatan dari password yang akan mengenkripsi file tersebut.

### *B. Desain Perancangan Sistem*

Desain perancangan menggunakan sistem USDP (Unified Software Development Process) yang merupakan proses pengembangan sistem berkelanjutan, dimana masing-masing bagian dilakukan secara iteratif. Dalam hal ini USDP menggunakan diagram-diagram UML yang sesuai dengan fungsi nya masing-masing[10]. UML (unified modeling language), merupakan sistem arsitektur yang bekerja dalam OOAD (Object Oriented Analysis and Design) dengan satu bahasa yang konsisten untuk menentukan, visualisasi, mengkonstruksi, dan mendokumentasikan artifact yang terdapat dalam sebuah software.

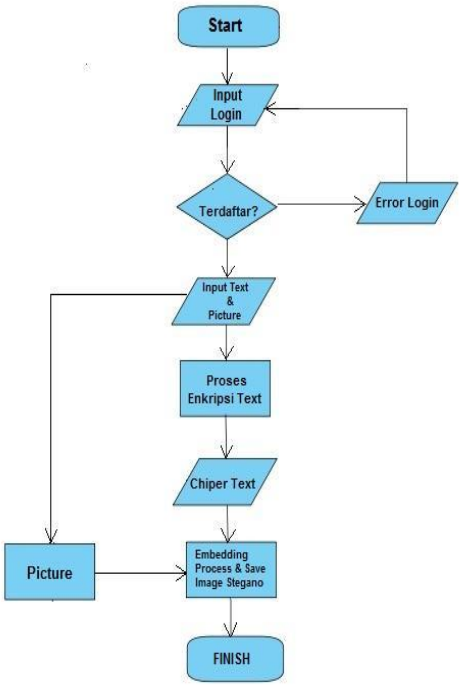
UML merupakan bahasa pemodelan yang paling sukses dari tiga metode OO (Object Oriented) yang telah ada sebelumnya, yaitu Booch, OMT, OOSE. UML merupakan kesatuan dari ketiga metode pemodelan tersebut dan ditambah kemampuan lebih karena mengandung metode tambahan untuk mengatasi masalah pemodelan yang tidak dapat ditangani ketiga metode tersebut[11].

Berikut ini use case dalam membangun aplikasi keamanan data yang menggunakan sistem keamanan berlapis dengan metode cryptography dan steganography:



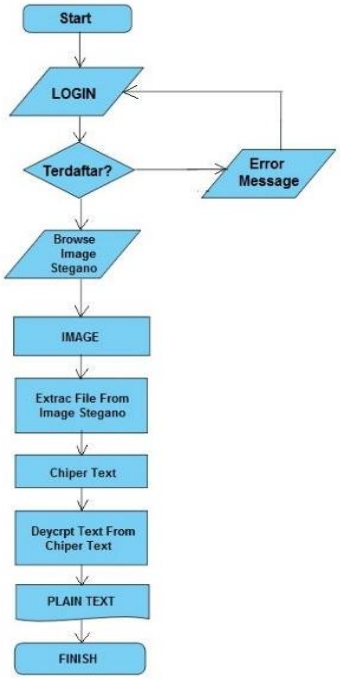

Gambar 3.
diagram use case cryptography dan steganography

Tahapan lanjutan ini yang merupakan alir (*flow*) dari sebuah program yang ditunjukan dalam sebuah bagan (*chart*) kerja dari sebuah sistem yang akan berjalan untuk diimplementasikan di dalam program atau prosedur sistem secara logika. Berikut ini bagan alir (*flowchart*) dari proses kerja aplikasi *cryptography* dan *steganography.*




Gambar 4.
flowchart proses encryption text dan embedding text

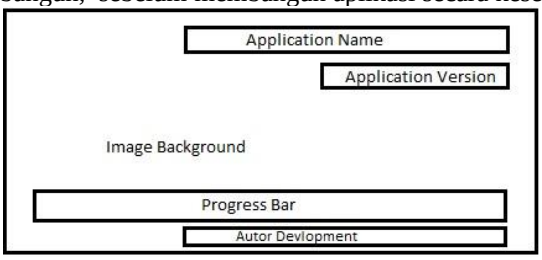
Tahapan *flowchart extract and decrypt* ini menjelaskan proses penerima pesan dapat menerima pesan secara utuh dan dapat di baca oleh penerima pesan. Pada bagan alir ini akan dijelaskan proses tersebut.



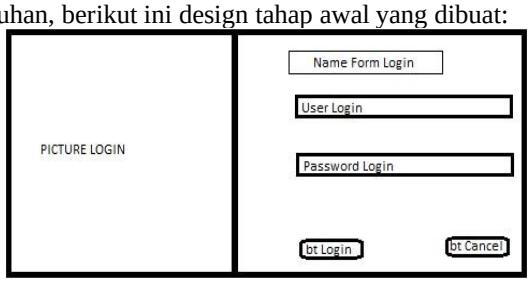

Gambar 5.
flowchart proses extrac image ke file dan decrypt file

*C. Blueprint Desain Aplikasi*

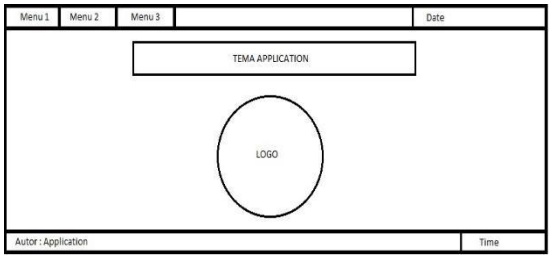
Dari flowchart di atas dapat dilakukan design tahap awal dengan membuat sketsa tiap bagian dari tampilan design aplikasi yang akan dibangun, sebelum membangun aplikasi secara keseluruhan, berikut ini design tahap awal yang dibuat:



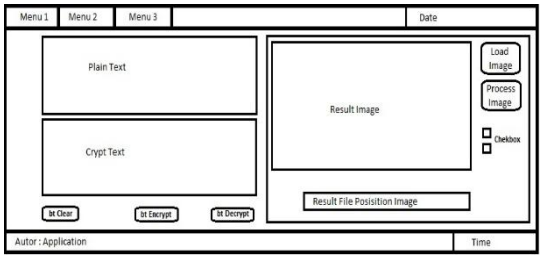

Gambar 6.
blueprint design splash screen



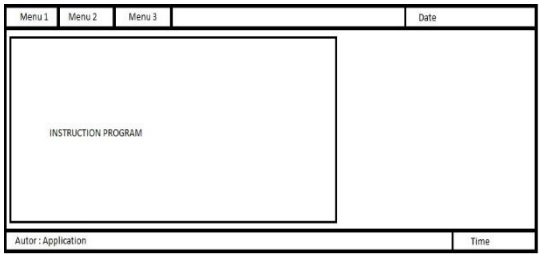

Gambar 7.
blueprint design form login



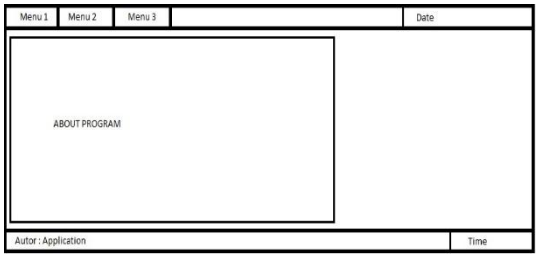

Gambar 8.
blueprint form menu



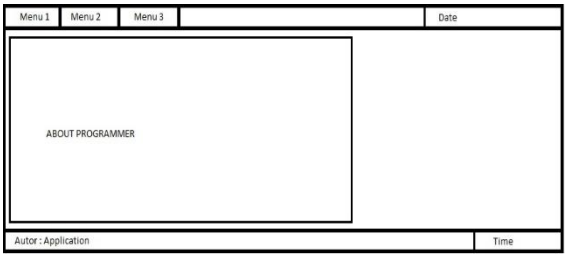

Gambar 9.
blueprint form main design




Gambar 10.
blueprint design form instruction




Gambar 11.
blueprint design about program



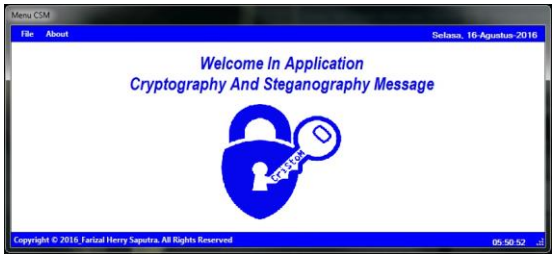

Gambar 12.
blueprint design about programmer

*D. Implementasi perancangan desain*

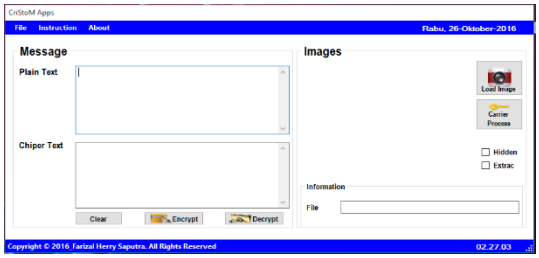
Setelah membuat desain tahap awal dengan membuat blueprint design perancangan aplikasi, kemudian hasil dari perancangan dapat diimplementasikan menggunakan tools development program, microsoft visual studio 2010 yang merupakan bahasa pemrograman yang menawarkan Integrated Development Environment (IDE) Visual untuk membuat program perangkat lunak berbasis sistem informasi Microsoft Windows menggunakan model pemrograman (COM)[12] untuk menerapkan alur kerja dari flowchart agar menghasilkan tampilan dari program yang akan dibuat.


Gambar 13.
*splash screen*

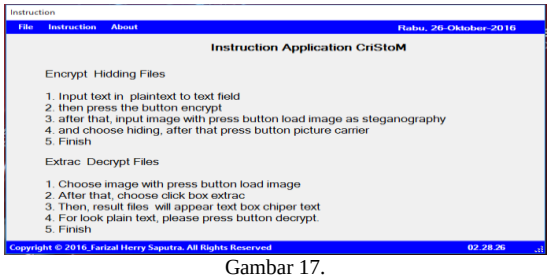

Gambar 14.
*form login*



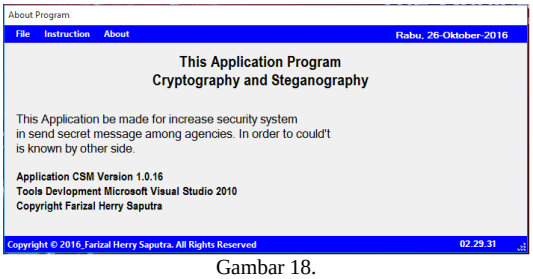

Gambar 15.
*form menu*



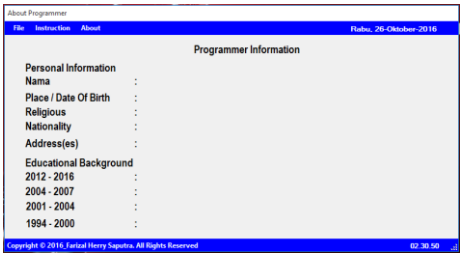

Gambar 16.
*form main design*




Gambar 17.
*form instruction*




Gambar 18.
*about program*



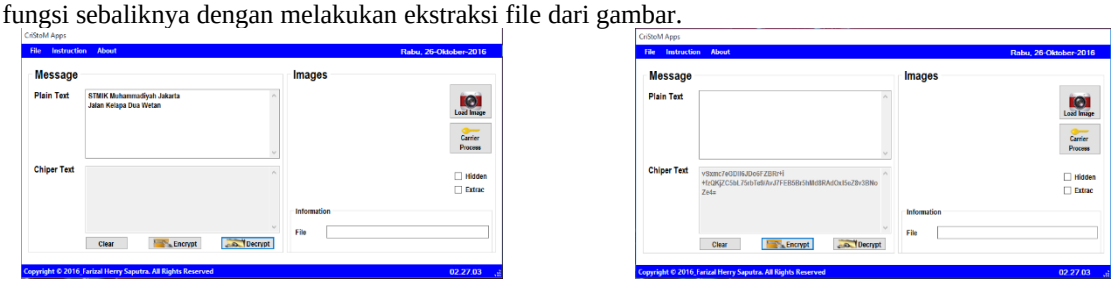

Gambar 19.
*about programmer*

## IV. IMPLEMENTASI DAN PENGUJIAN

Pada tahapan ini penulis melakukan implementasi dengan melakukan inputan bahasa pemrograman menggunakan tools visual basic.net 2010 dari rancangan desain yang dibuat dan melakukan tahap pengujian pada system pengamanan saat login, cek fitur, pengujian kriptografi dan steganografi, pengujian image output system dengan histogram dan pengujian decrypt kriptografi dan steganografi:

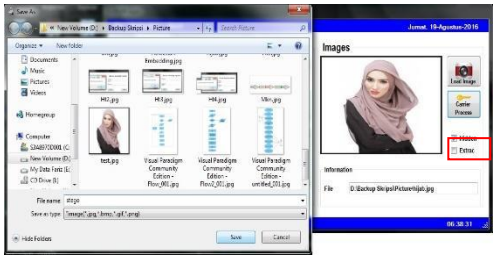
### *A. Test fungsi kriptografi dan steganografi*

Untuk test fungsi enkripsi dan dekripsi, pada aplikasi ini akan dilihat hasil proses enkripsi data terlebih dahulu dan sebaliknya proses dekripsi data dengan menggunakan algoritma *Message Digest* 5 (MD5) merupakan salah satu alat untuk memberi garansi bahwa pesan yang dikirim akan sama dengan pesan yang diterima[13] dan dilanjutkan test fungsi untuk aplikasi steganografi yang menggunakan teknik *Least Significant Bit* (LSB) untuk menyembunyikan data di dalam gambar sehingga tidak akan ada perubahan yang terlihat pada gambar aslinya[14] dan file hasil enkripsi akan disembunyikan, pada sebuah citra digital berupa gambar yang dijadikan tempat penyembunyian (embedding) dari pesan terenkripsi dengan system menjalankan fungsi hiding files dan melakukan fungsi sebaliknya dengan melakukan ekstraksi file dari gambar.




(a) (b)

Gambar 20.
(a) text asli (*plain text*), (b) hasil text enkripsi (*chipertext*)

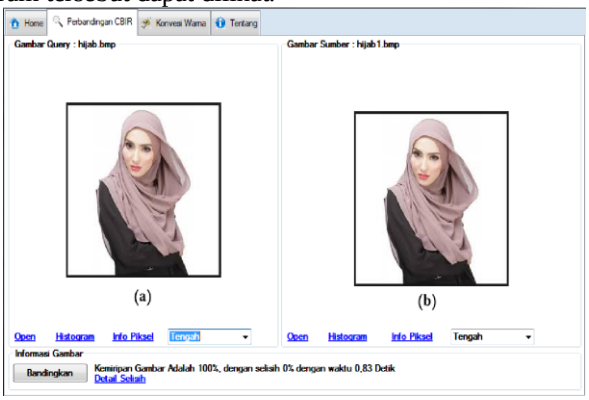



Gambar 21.
*proses embedding file chipertext*


Gambar 22.
*proses extrac files chipertext*

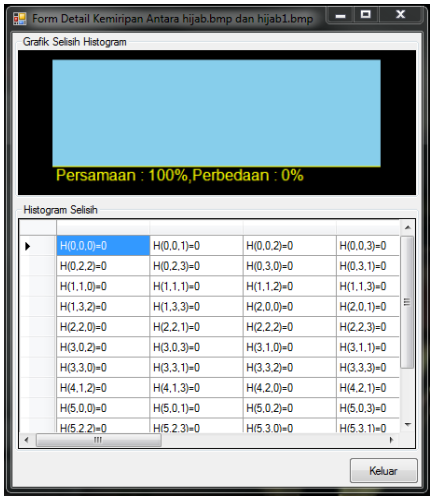
### *B. Test implementasi program*

Dari hasil test aplikasi cryptography dan steganography dapat dilihat dari serangkaian proses yang ada di atas, pada image dengan nama file image hijab1.bmp tidak mengalami perubahan sama sekali dari fisik image, color dan image size semua tampak normal dan dari hasil implementasi program tersebut dapat dilihat.

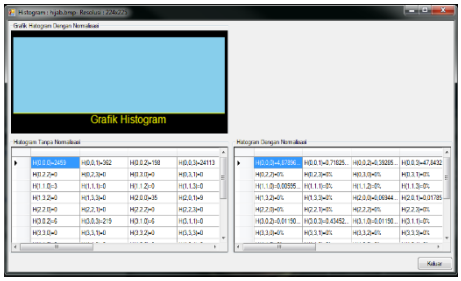



Gambar 23.
(a) *original image* (hijab.bmp), (b) *image already stego with crypto* (hijab1.bmp)

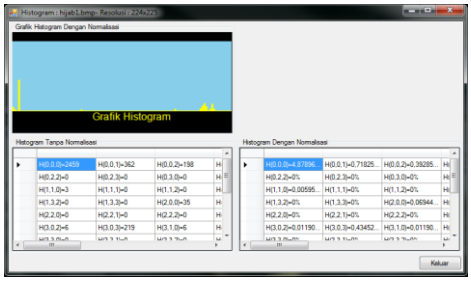
Dari gambar diatas dilanjutakan dengan penilaian grafik Histogram pada kedua gambar, seperti (gambar 22). Berdasarkan hasil implementasi antara gambar asli dengan gambar yang sudah dilakukan proses memasukkan teks yang sudah terenkripsi kedalam gambar tidak ada perubahan pada fisik gambar tersebut dan jika dibandingkan dari aplikasi perbandingan HSV ini menunjukan kemiripan gambar adalah 100%, dengan selisih 0% dengan waktu melakukan proses perbandingan 0,83 detik dan dari (gambar 23). detail perbandingan antara kedua gambar memiliki nilai 100%. Selanjutanya akan dilakukan perbandingan.




Gambar 24.
Histogram hasil perbandingan kedua gambar




(a)



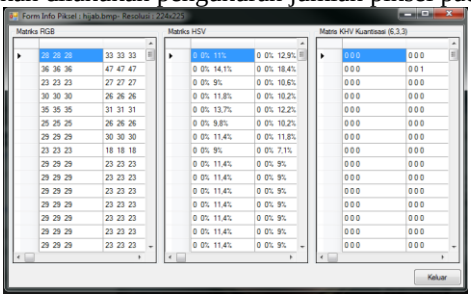

(b)

Gambar 25.
(a) nilai grafik histogram (hijab.bmp), (b) nilai grapfik histogram (hijab1.bmp)

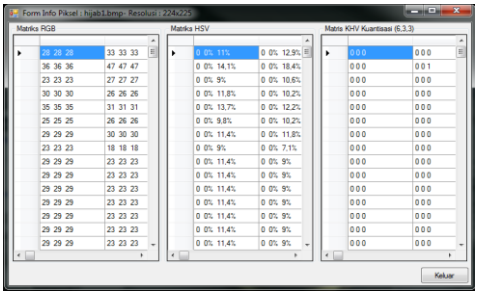
Dari hasil grafik nilai histogram antara kedua gambar tidak mengalami perubahan dari nilai grafik histogram dengan normalisai dan tanpa normalisasi sebesar :

1) *Gambar hijab.bmp*
   a. Histogram Dengan normalisasi H(0.0.0)=4.87896
   b. Histogram Tanpa normalisasi H(0.0.0)=2459
2) *Gambar hijab1.bmp*
   a. Histogram Dengan normalisasi H(0.0.0)=4.87896
   b. Histogram Tanpa normalisasi H(0.0.0)=2459

Tahapan hasil implementasi dengan mengukur piksel pada kedua gambar apakah mengalami perubahan yang signifikan atau tidak, untuk itu akan dilakukan pengukuran jumlah piksel pada kedua gambar tersebut.




(a)




(b)

Gambar 24. (a) nilai pixel hijab.bmp (b) nilai pixel hijab1.bmp

Berdasarkan hasil test piksel dikedua gambar dapat dilihat jumlah piksel dari kedua gambar tidak mengalami perubahan dari tiga macam pengukuran piksel ini:

1) *Gambar hijab.bmp*
   a. Matriks RGB = 28 28 28
   b. Matriks HSV = 0.0% 11%
   c. Matriks KHV Kuantitas = 000
2) *Gambar hijab1.bmp*
   a. Matriks RGB = 28 28 28
   b. Matriks HSV = 0.0% 11%
   c. Matriks KHV Kuantitas = 000

## V. KESIMPULAN

Berdasarkan dari hasil implementasi dan berbagai penjelasan yang telah diuraikan dalam laporan ini, maka dapat disimpulkan berbagai hal sebagai berikut:

a. Aplikasi ini menunjukan hasil dari kedua gambar tidak mengalami perubahan secara fisik, warna dan ukuran byte dari gambar yang telah dimasukkan pesan enkripsi didalam nya.
b. Aplikasi di atas sama sekali tidak mengubah fisik gambar akan tetapi menambah kapasitas data pada gambar dengan satuan terkecil Bit, jika teks dengan jumlah data yang terlalu banyak akan mengalami kompresi dengan menyesuaikan hasil enkripsi dari *plaintext* menjadi *chipertext*, hasil enkripsi akan tetap berpengaruh dengan jumlah Bit data dan agar tidak mengalami perubahan perlu memperhatikan besaran nilai kapasitas bytes pada gambar yang akan menjadi media *embedding* dengan menambahkan enkripsi tambahan di dalam nya.
c. Dengan aplikasi keamanan data ini menjadikan, data yang bersifat rahasia menjadi aman sampai data tersebut diterima oleh penerima data yang menggunakan aplikasi ini atau orang yang ditunjuk untuk menerima data tersebut secara khusus dengan begitu aspek *confident, integrity, Availability* dan *Authority*.

## DAFTAR PUSTAKA

[1] Sulinta, Feri. (2014). “Teknik Membongkar dan Mengamankan Password’, Jakarta; PT Elex Media Komputindo. hal 69-70
[2] Indra Gunawan, ST., M.Kom., CEH., CHFI. (2021). “Keamanan Data : Teori dan Implementasi”. Jawa Barat; CV Jejak. hal 6
[3] Andik Susilo. (2010). “Teknik Cepat Memahami Keamanan Komputer dan Internet*”,* Yogyakarta:Elek Media Komputindo. hal 59
[4] Emy Setyaningsih, S.Si, M.Kom,. (2015) “*Kriptografi & Implementasi Menggunakan MATLAB”*, Yogyakarta: Andi Yogyakarta. hal 1-4
[5] Dony Ariyus. (2008). “Pengantar Ilmu Kriptografi teori, analisis dan implementasi”, Yogyakarta:AndiOffset. hal 10-11
[6] Ridki Sadikin. (2012). “Kriptografi Untuk Keamanan Jaringan”, Yogyakarta:AndiYogyakarta. hal 10
[7] Sudarmadi, DA , & Runturambi, AJS (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia . Jurnal Kajian Strategi Ketahanan Nasional , 2 (2). 157-178
[8] Roger S. Pressman. Ph.D,. (2002). Rekayasa Perangkat Lunak Pendekatan Praktisi (Buku Satu). hal 36-39
[9] Prof. DR. Hj. Sedarmayanti, M.Pd. (2014). APU & Drs. Syarifudin Hidayat, M.Si., Metodologi Penelitian, Bandung:CV Mandar Maju. hal 25
[10] Adi Nugroho. (2009). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP (*unified software development process*). hal 80
[11] ----------. (2009). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP (*unified software development process*). hal 24-25
[12] Stefano, S.Kom. (2014). Cara Mudah Membangun Sistem Informasi Menggunakan VB.NET dan Komponen DXperience, Yogyakarta:CV Andi Offset.hal 2
[13] A. Sofwan, A. Budi P, and T. Susanto. (2012). "Aplikasi Kriptografi dengan Algoritma Message Digest 5 (MD5)". Transmisi: Jurnal Ilmiah Teknik Elektro, vol. 8, no. 1, pp. 22-27
[14] Arun Kumar Singh, Juhi Singh, Dr, Harsh Vikram Singh. (2015). “Steganography in Images using LSB technique”, Transmisi: International Journal of Latest Trends in Engineering and Technology (IJLTET).