STEGANOGRAFI UNTUK KEASLIAN TANDA TANGAN YANG TERDIGITALISASI ALGORITMA RC4

Imam Himawan
Informatika, Universitas Indraprasta PGRI
imamhimawann@gmail.com

Abstrak

Steganografi untuk keaslian tandatangan yang terdigitalisasi Dengan Algoritma RC4 (Ron's Code #4). Kami menggunakan konsep ini dimana teks yang tersembunyi di balik citra dan penerima yang dimaksud mampu melihatnya. Tujuan dari penelitian ini adalah untuk menjaga keaslian tandatangan yang terdigitalisasi dengan menyembunyikan pesan didalamnya. Sehingga apabila ada masalah mengenai tandatangan palsu atau mencurigakan terkait dalam dokumen dapat diselesaikan dengan baik dengan menggunakan sistem ini, maka dokumen tersebut bisa diketahui keasliannya. Sisten ini menggunakan Algoritma RC4 yang dibuat dengan bahasa pemrograman visual basic 6. Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya: Format gambar : bitmap, gif, jpeg, dll, Format audio : wav, voc, mp3, dll, Metode yang digunakan adalah menyisipkan pesan dan menampilkan kembali pesan tersebut Teknik pengujian sistem dengan RGB (*Red Green Blue*). Kualitas perangkat lunak yang dihasilkan diuji berdasarkan empat karakteristik kualitas perangkat lunak model ISO 9126, yaitu *functionality*, *reliability*, *usability*, dan *efficiency*. Hasil dari penelitian ini akan menjadi dokumentasi di kantor PT. Jaya Guna Lancar yang sesuai kebutuhan perusahaan

Kata Kunci : Steganografi, Enkripsi, Deskripsi for Signature Digitaled by RC4 Algorithm.

Abstract

Steganography for digitalized signature authenticity with the RC4 algorithm (Ron's Code # 4). We use this concept where the text is hidden behind the image and the intended recipient is able to see it. The purpose of this research is to maintain the authenticity of the digitalized signature by hiding the message therein. So that if there is a problem regarding a fake or suspicious signature related to the document, it can be resolved properly using this system, the authenticity of the document can be known. This system uses the RC4 Algorithm made with visual basic 6 programming language. In the steganography method this method is very useful if used on computer steganography because there are many digital file formats that can be used as a medium to hide messages. Commonly used formats include: Image format: bitmap, gif, jpeg, etc., Audio format: wav, voc, mp3, etc., The method used is to insert a message and display the message Technique testing the system with RGB (Red Green Blue) . The quality of the software produced is tested based on fourthe quality characteristics of the ISO 9126 model software, namely functionality, reliability , usability , and efficiency. The results of this study will be documentation in the office PT. Jaya For Current that fits the needs of the company

Keywords*: Steganography, Encryption, Description for Signature Digitaled by RC4 Algorithm*

1. PENDAHULUAN

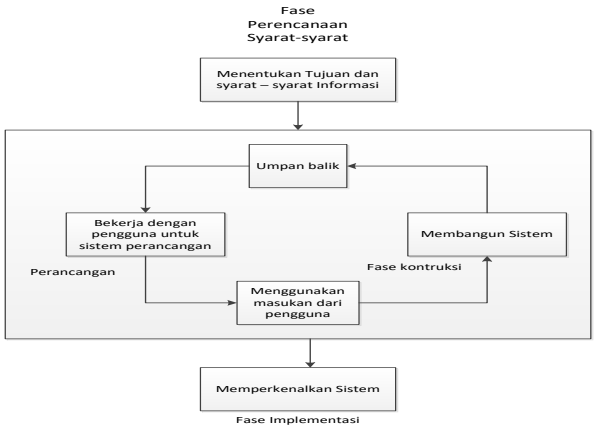
Di era globalisasi saat ini, mendapatkan informasi sangatlah mudah. Setiap orang dengan mudah mendapatkan data ataupun berita yang diinginkan. Hal ini didukung dengan teknologi informasi dan

komunikasi yang terus berkembang pesat dari tahun ke tahun. Akan tetapi kemudahan mendapatkan informasi juga memberikan ancaman. Beberapa ancaman yang diberikan adalah masalah tentang keamanan, kerahasiaan, dan keotentikan data. Oleh karena itu diperlukan suatu sistem pengamanan data yang bertujuan untuk meningkatkan keamanan data, melindungi suatu data atau pesan agar tidak dibaca oleh pihak yang tidak berwenang, dan mencegah pihak yang tidak berwenang untuk menyisipkan, menhapus, ataupun merubah data. Terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau *plaintext* menjadi *ciphertext* (teks tersandi). Sedangkan Dekripsi adalah proses penyandian kembali *ciphertext* menjadi *plaintext*. Salah satu metode enkripsi yang terkenal adalah metode RC4. RC4 pertama kali dibuat oleh *Ron Rivest* di Laboraturium RSA pada tahun 1987. Awalnya RC4 adalah sebuah rahasia dagang, akan tetapi pada September 1994, kode tersebut dikirim oleh seseorang yang tidak diketahui ke *milist Chypermunks* dan menyebar ke banyak situs internet. Kode yang bocor tersebut akhirnya dikonfirmasi sebagai RC4 karena memiliki output yang sama dengan *software* dengan *license* RC4 di dalamnya. Karena algoritma sudah diketahui, RC4 tidak lagi menjadi rahasia dagang. Nama "RC4" sekarang adalah sebuah merek dagang namun sering disebut sebagai "*ARCFOUR*" atau "*ARC4*" (artinya diduga RC4 karena algoritma ini tidak pernah dirilis secara resmi oleh RSA) untuk menghindari kemungkinan masalah tentang merek dagang. RC4 (*Ron's Code* #4) adalah sebuah *synchrone stream cipher* yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi *plaintext* secara digit per digit atau *byte* per *byte* dengan cara mengkombinasikan dengan operasi biner (biasanya XOR) dengan sebuah angka semiacak.

2. METODE PENELITIAN

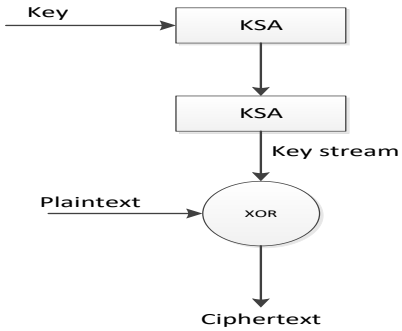
Penelitian steganografi menggunakan Algoritma RC4. yang dilakukan merupakan jenis penelitian terapan (*Apllied Research*). Penelitian terapan yang hasilnya dapat langsung diterapkan untuk memecahkan permasalahan yang dihadapi. Moeddjiono 2012 [1] Hasil penelitian ini berupa aplikasi terdigitalisasi tanda tanggan dengan Algoritma RC4 yang langsung dapat di terapkan untuk memecahkan masalah yang dihadapi. Pengembangan *system* dalam penelitian ini penulis lakukan menggunakan tiga tahap siklus pengembangan model LSB (*Least Significant Bit Insertion*) Jamaludin, 2010 [5] yaitu pendekatan yang umum untuk menanamkan informasi dalam media citra, bila menggunakan gambar 24-bit, bit dari masing – masing komponen warna merah, hijau dan biru dapat digunakan karena masing
– masing ditampilkan dalam bentuk byte. Dengan kata lain, Citra dengan kata lain seseorang dapat menyimpan 3 bit disetiap *pixel*.

Kendall, K.E 2003 [2] mengilustrasikan model RAD seperti gambar dibawah ini :



Gambar 1. Siklus Pengembangan Sistem Model RAD.

Metode RC4 RC4 (Ron' Code #4) merupakan suatu algoritma enkripsi *stream cipher* dan *symmentic key*, dimana algoritma ini melakukan proses enkripsi / deskripsi *one byte at a time* dan menggunakan kunci yang sama. Algoritma RC4 terdiri dari 2 bagian yaitu *Key Scheduling Algoritm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA).



Gambar 2. Blok Diagram Algoritma RC4

Dari uraian diatas, maka metode penelitian yang dilakukan adalah merancang bangun perangkat lunak aplikasi enkripsi RC4 dengan menggunakan Visual Basic Ver.6 dan menganalisa proses dari KSA dan PRGA hingga mendapatkan hasil ekripsi(*Chipertext*) yang di inginkan.

Sistem steganografi yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada *Objek Gambar yang* terdigitalisasi sebagai *file* otentik yang tidak dilakukan pemalsuan dalam surat yang sudah di *approval*. Sistem penyisipan informasi atau pesan berfungsi untuk melakukan proses penyembunyian pesan ke file citra digital gambar. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia. Keamanan data tidak hanya berkenan dengan data yang ada pada saja, tetapi juga meliputi bagian lain dari *system database*. Agar memiliki suatu keamanan yang efektik dibutuhkan kontrol yang tepat. Seseorang yang mengontrol dan mengatur *database* adalah administrator, seorang administrator yang memagang peranan penting pada suatu *system database*. Keamanan merupakan suatu proteksi terhadap pengerusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan. [3] Ir. Yusuf Kurniawan, MT., 2004

Tinjauan Studi Penelitian B.B.Gite, Divya Choksey, Mahesh Jambhulkar, Rahul Ramath, Yashovardhan Jhamvar / *International Journal of Engineering Reserch and Applications* (IJERA) Mengungkapkan Sistem yang diusulkan bertujuan untuk mengatasi kekurangan dari sistem yang ada yang bertujuan mengembangkan lingkungan yang lebih aman untuk melaksanakan Gambar Steganografi. Sistem ini akan memberikan pengguna tanda tangan digital yang mereka dapat menanamkan dalam *image* steganografi untuk memvalidasi sumber gambar.[4] B.B.Gite, Divya Choksey, 2013

Metode Pemilihan Sampel

Teknik penentuan sampel yang digunakan adalah *Purposive Sampling*

yang artinya bahwa pengambilan sampel dengan *purposive sampling* merupakan tehnik pengambilan sampel dengan mengambil responden yang terpilih betul oleh peneliti menurut ciri-ciri spesifik yang dimiliki oleh sampel tersebut. Responden dalam penelitian ini adalah Pimpinan, Staff HRD, Staf FTTH, Staff BTS, Staff Arsitektur. Pemilihan responden sampel ini dengan pertimbangan berdasarkan keterlibatan di dalam system sehingga pemilihan sampel menjadi lebih *representative*.

Metode Pengumpulan Data

1. Studi kasus
   Dilakukan dengan cara membaca dan mempelajari buku – buku dan artikel yang berhubungan dengan keamanan data khusunya tentang steganografi, serta buku – buku yang mendukung dengan topic yang akan dibahas dalam penyusunan penelitian ini.
2. Literature
   Menggunakan beberapa jurnal dan makalah yang terkait dengan keamanan data khusunya steganografi dan teknik signatur digital sebagai refrensi bagi penulis.
3. Diskusi
   Melakukan diskusi dengan dosen dan teman teman serta orang orang yang mengerti terhadap materi bahasan agar mendapatkan bahan masukan untuk penyusunan makalah ini.

Tinjauan Studi Penelitian Hanriyawan A. Mooduto dan Albar [6]

Dengan judul "Enkripsi Data dan Albar" memberikan kesimpulan bahwa Algoritma RC4 lebih cepat proses enkripsinya karena berbasis *Stream Cipher* yang melakukan enkripsi *one byte at time*.

Tinjauan Objek Penelitian

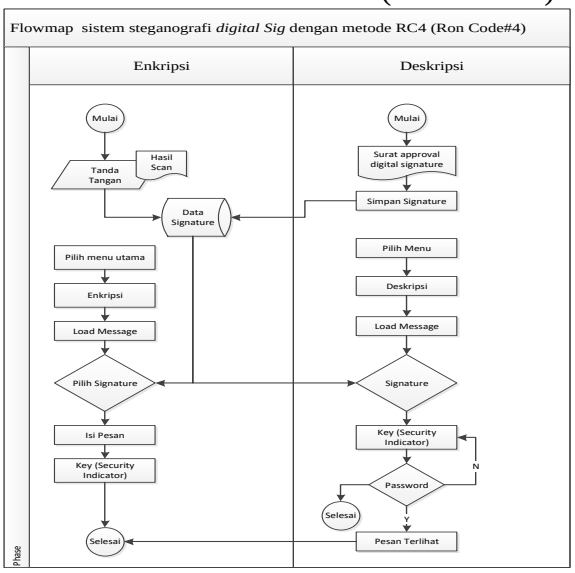
PT. Jaya Guna Lancar biasa disingkat PT. JGL dengan 50 karyawan dan pada tahun ke-dua meningkat menjadi 75 karyawan. Secara kuantitas angka ini menunjukkan bahwa pekerjaan banyak dibutuhkan. Pesatnya perkembangan industri pekerjaan dengan jumlah masyarakat tidak seimbang yang sehingga banyaknya pengganguran.

Kerangka Konsep

Perusahaan PT. Jaya Guna Lancar adalah perusahaan yang bergerak dibidang jasa untuk pemasangan BTS Signal dan Jaringan Fiber Optic ISP dan OSP, dengan banyak permintaan customer perusahaan belum memiliki sistem mengenai tanda tanggan digital yang sehingga mengacu pengesahan administrasi document terlambat dan banyaknya document administrasi yang disalah gunakan dan pemalsuan, indikasi masalah yang sudah dijelaskan di atas maka dibuatkan sistem mengenai tanda tanggan terdigitalisasi guna pengesahan sebuah document. Aplikasi dibuat berdasarkan kebutuhan fungsional terhadap kantor PT. Jaya Guna Lancar agar dapat menjadi solusi untuk memecahkan masalah yang ada, pengembangan sistem akan dikembangkan lebih lanjut guna membuat sistem yang lebih baik lagi dengan adanya masukan saran dan kritik, Pembuatan aplikasi ini di dukung dengan kebutuhan fungsional seperti sebuah aplikasi Visual Basic 6.0, bahasa yang digunakan yaitu bahasa C++, peralatan

pendukung alat Scanner, dan type file yang digunakan JPG, BMP dll.

Berikut adalah bagan alir / *flowmap* sistem steganografi *digital Sig* dengan metode RC4 (RonCode#4)

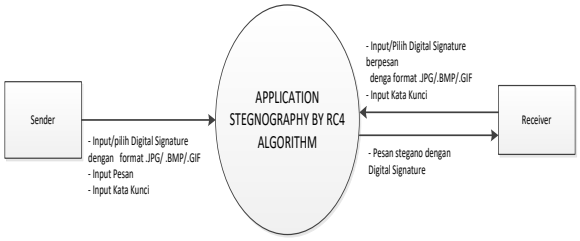


Gambar 3. *Flowmap* Steganografi Citra Digital Gambar.

Dari *flowmap* diatas terlihat proses pembuatan pesan steganografi dengan menyisipkan pesan kedalam Objek gambar yang terdigitalisasi, dan mengestrak Objek gambar yang terdigitalisasi berpesan dengan sebuah aplikasi steganografi.

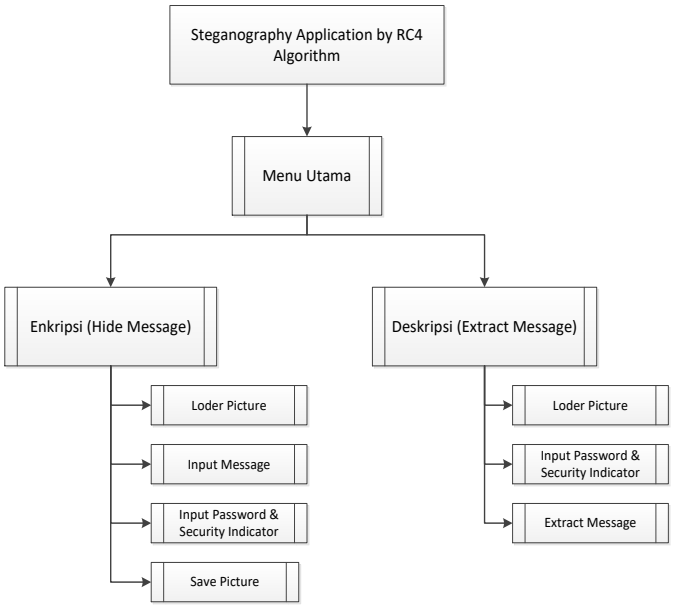
Diagram Konteks

Berikut adalah diagram konteks



Gambar 4 Diagram Konteks Aplikasi Steganografi.

Hipo



Gambar 5 HIPO Aplikasi Steganografi.

Pengujian Spesifikasi dengan *Focus Group Discussion* (FGD)

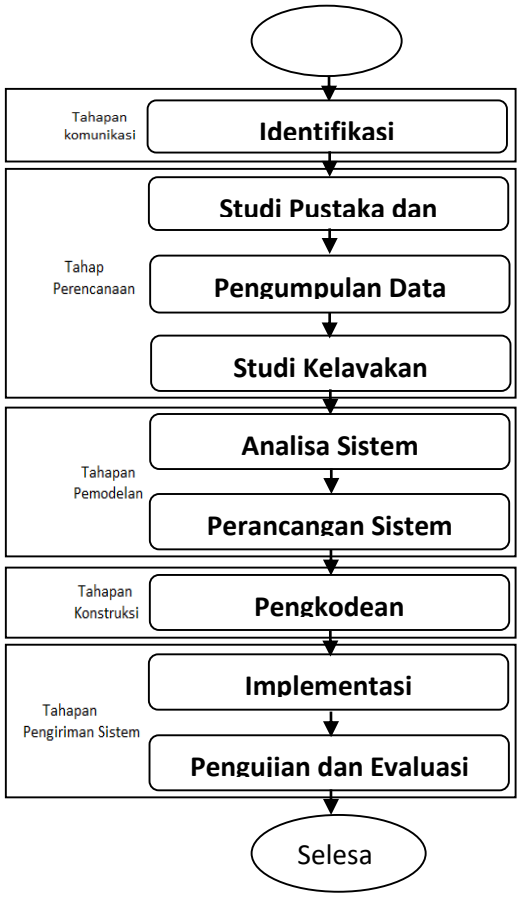
Pengujian spesifikasi aplikasi yang dibuat dengan pendekatan *focus group discussion* bertujuan untuk mengecek dan menilai apakah aplikasi yang dibuat telah sesuai dengan spesifikasi dan keinginan owner dan pimpinan pada PT. Jaya Guna Lancar. Teknik pengujian ini dilakukan dengan cara diskusi kelompok dengan 4 (empat) yang telah dipilih menjadi informan sehingga mampu memberikan kemudahan dan peluang bagi peneliti untuk mendapatkan informasi, kepercayaan, dan jawaban yang valid mengenai spesifikasi aplikasi yang telah dibuat sehingga dapat menjawab hipotesis yang telah dibuat. Jenis pengujian ini termasuk pengujian RGB *(Red Green Blue)* yaitu pengujian aspek fundamental sistem perangkat lunak. Metode ini digunakan untuk mengetahui apakah perangkat lunak berfungsi dengan benar sesuai kebutuhan spesifikasi yang ada.

Pengujian Kualitas aplikasi dengan ISO 9126

Dimana model ini berkaitan dengan model kualitas perangkat lunak yang merupakan pengembangan dari model 9126. Pengujian kualitas aplikasi Steganografi untuk keaslian tanda tangan yang terdigitalisasi dengan algoritma RC4 dilakukan untuk menguji dan mengevaluasi tingkat kualitas perangkat lunak sistem informasi yang dihasilkan berdasarkan 4 (empat) karakteristik kualitas perangkat lunak yang terdapat pada ISO 9126, yaitu Kesesuaian Fungsional (*Functional Suitability*), Keandalan (*Reliability*), mampu dijalankan (*Operability*), Efisiensi Kinerja (*Performance Efficiency*), Keamanan (*Security*), Kompatibilitas (*Compatibility*), Perawatan (*maintainability*), dan Transfer Lingkungan (*Transferability*). Dari delapan karakteristik kualitas sebuah aplikasi ditetapkan hanya 4 (empat) karakteristik saja yang dijadikan variabel dalam penelitian ini, yaitu Kesesuaian Fungsional (*Functional Suitability*), Keandalan (*Reliability*), mampu dijalankan (*Operability*), dan Efisiensi Kinerja (*Performance Efficiency*), sedangkan empat karakteristik lainnya tidak akan dilakukan pengujian. Teknik pengujian kualitas perangkat lunak ini dilakukan untuk membuktikan hipotesis penelitian. Jumlah responden yang digunakan berjumlah 50 responden.

Rancangan kegiatan penelitian

Dalam pengembangan penelitian pengembangan Steganografi untuk keaslian tanda tangan yang terdigitalisasi dengan algoritma RC4, peneliti melakukan langkah-langkah kegiatan penelitian secara berurutan dan sistematis yang dapat dilihat pada gambar sebagai berikut:



Gambar 6 Langkah – langkah penelitian.

3. HASIL DAN PEMBAHASAN

Dalam analisa pendahuluan ini. Peneliti akan menganalisa pernyataan-pernyataan yang telah diajukan kepada responden yang telah di pilih yang sesuai dengan kriteria yang telah ditetapkan mengenai kebutuhan sistem secara umum yang akan dirancang dan diberi nama Steganografi untuk keaslian tanda tangan yang terdigitalisasi dengan algoritma RC4 berdasarkan kebutuhan pengguna, sehingga nantinya fitur-fitur yang dihasilkan sesuai dengan kebutuhan dalam kemudahan pengguna dalam menggunakan sistem yang dihasilkan.

Analisa Kebutuhan Modul

Berdasarkan hasil dari wawancara seperti yang terlihat pada lampiran 1 hipotesis dari

kajian teoritis dan kerangka konsep yang telah dikemukakan diduga dengan steganografi menggunakan Algoritma RC4 dapat di uji dengan Visual Basic 6.0 yang dapat membantu pekerjaan dengan baik dikantor PT. Jaya Guna Lancar.

dan pengamatan umum mengenai steganografi untuk keaslian tanda tangan yang terdigitalisasi dengan algoritma RC4 yang akan dibuat, maka modul-modul yang dibutuhkan antara lain modul admin, dan modul user personal. Dari hasil wawancara yang dilakukan dapat di ambil kesimpulan bahwa kebutuhan akan sistem menurut masing-masing responden yang diwawancara.

Rancangan Perangkat Sistem

Mengimplementasikan penelitian yang dibuat maka diperlukan beberapa komponen yang digunakan sebaagai pendukung penelian, diantaranya :

Perangkat Keras (Hardware) Spesifikasi Minimal hardware atau komputer yang diusulkan untuk mengoperasikan aplikasi ini adalah sebagai berikut :

- Prosesor Core 2 Duo
- Harddisk 350 GB
- Memory RAM 2 GB
- Perangkat pendukung keluaran (monitor)
- Perangkat masukan (keyboard, mouse)
- Scanner

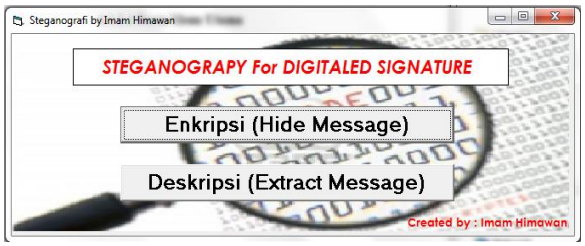
Perangkat Lunak (Software)

- Windows XP atau Windows 7
- Bahasa pemrograman yang digunakan pada aplikasi steganografi ini adalah dibuat menggunakan bahasa pemrograman VB 6.0
- Adobe Acrobat Pro (Software untuk membuka File Pdf)

Rancangan Interface Aplikasi Steganografi

Ada beberapa *form* yang dibuat dalam aplikasi steganografi untuk memasukan pesan kedalam gambar. *Form-form* tersebut terdiri dintaranya:

Form Menu Utama

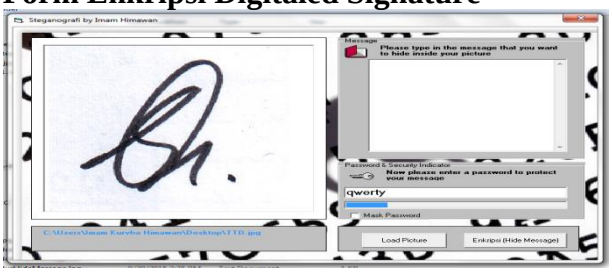


Gambar 7. Form Menu

Menu utama terdiri dari :

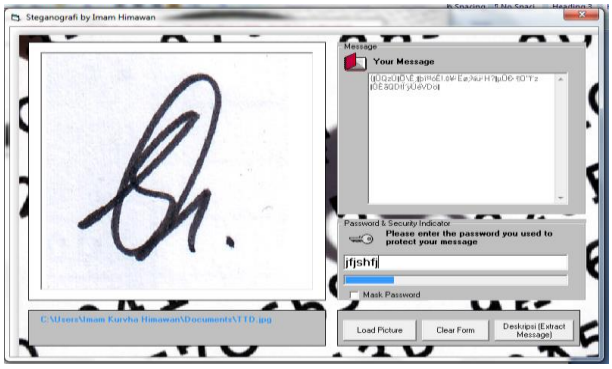
1. Enkripsi (*Hide Message*) menu ini digunakan untuk memasukan pesan pada tandatangan yang terdigitalisasi.
2. Deskripsi (*Extract Message*) menu ini digunakan untuk mengextract pesan yang telah dimasukan kedalam gambar.

Form Enkripsi Digitaled Signature



Gambar 8 Enkripsi Digitaled

Signature.**Form Deskripsi Tandatangan yang terdigitalisasi**

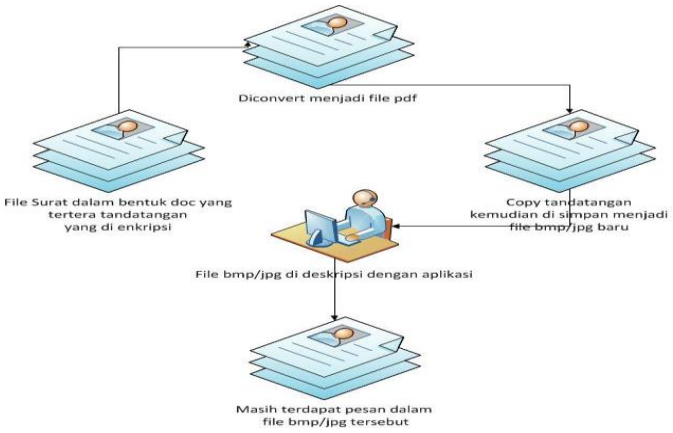


Gambar 9 Deskripsi Tandatangan yang terdigitalisasi (*Extract Message*)

Nama File	Format File	Ukuran Awal	Ukuran	Status
Gambar1 b.bmp	.bmp	226 kb	225kb	Sukses
Gambar2 b.bmp	.bmp	226 kb	225kb	Sukses
Gambar1 .jpg	.jpg	18 kb	225kb	Sukses
Gambar1 2.jpg	.jpg	18 kb	225kb	Sukses

Pengujian Keaslian Document

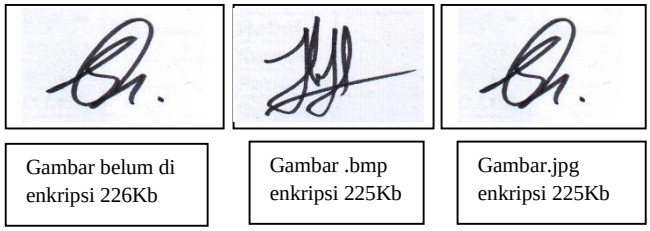
Cara yang dilakukan untuk pengujian keaslian *file* tandatangan, penulis membuat *file* surat dalam bentuk *file document*(.doc) yang disipkan *file* tandatangan yang telah di enkripsi, kemudian *file* tersebut di rubah menjadi *file* pdf. Dari *file* pdf tersebut tandatangan di *copy* dan disimpan dengan nama *file* bmp/jpg, kemudian di Deskripsi apakah pesan yang dibuat masih ada atau tidak. Gambaran pengujian sistem digambarkan dalam bagan berikut.



Gambar 10 Proses Pengujian Enkripsi.

Pengujian File yang telah dienkripsi

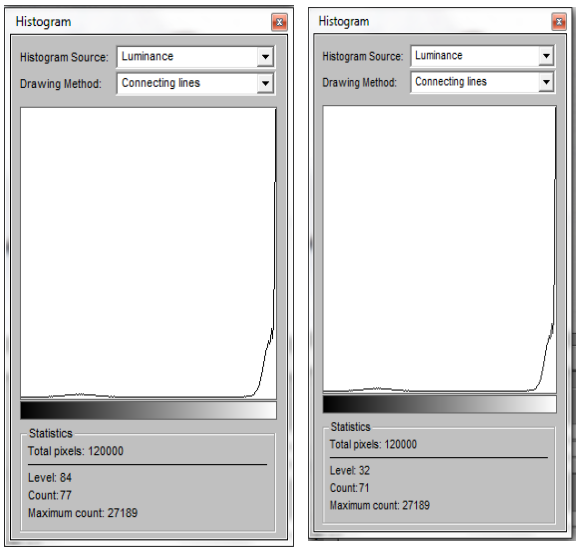
Pengujian yang dilakukan adalah memasukan beberapa *file* jpg dan bmp dengan ukuran *file* yang berbeda kemudian dilakukan perbandingan antara *file* yang telah di enkrip dan yang belum di enkrip. Tabel 1.1 adalah beberapa *file* gambar yang telah dilakukan pengujian.



Gambar belum di enkripsi 226Kb	Gambar .bmp enkripsi 225Kb	Gambar.jpg enkripsi 225Kb

Dari tabel diatas diketahui bahwa enkripsi dengan menggunakan algoritma RC4 tidak ada perubahan dalam ukuran *file* maupun perubahan gambar yang terjadi. Kemudian gambar-gambar tersebut dilakukan uji coba dengan membandingkan beberapa gambar dengan cara membagi warna dengan beberapa bagian *Red*, *Green* dan *Blue* yang dikenal dengan RGB, dari cara tersebut dapat diketahui perbedaan gambar yang terjadi sebelum di enkrip dan setelah

di enkrip. Gambar dibawah adalah tampilan dari gambar yang telah dipecah menjadi beberapa warna.



Gambar 11 Proses pengujian hasil deskripsi dan enkripsi.

Hasil Pengujian Validasi

Tahap pengujian validasi ini dilakukan untuk memastikan perangkat lunak yang telah dibuat apakah sesuai dengan spesifikasi kebutuhan fungsional yang diharapkan. Hal ini juga menguji hipotesis pertama dalam penelitian ini, yaitu: Berdasarkan dari kajian teoritis dan kerangka konsep yang telah dikemukakan diduga dengan steganografi menggunakan Algoritma RC4 dapat di uji dengan Visual Basic 6.0 yang dapat membantu pekerjaan dengan baik dikantor PT. Jaya Guna Lancar. Metode yang digunakan adalah *Focus Group Discussion* (FGD). Pada tahapan ini dimulai dengan diskusi dengan responden terpilih, kemudian peneliti melakukan presentasi dan demi rancangan aplikasi sistem informasi yang sudah dikembangkan dan menjelaskan setiap fungsi yang ada berdasarkan *instrument* yang sudah disiapkan, selanjutnya peserta FGD memberikan informasi, tanggapan dan persetujuan dengan formulir yang telah diberikan oleh peneliti.

Pengujian Kualitas Aplikasi dengaan ISO 9126

Pengujian kualitas aplikasi steganografi untuk tanda tangan yang terdigitalisasi dengan algoritma RC4 dilakukan untuk menguji dan mengevaluasi tingkat kualitas perangkat lunak sistem yang dihasilkan dengan menggunakan ISO 9126. Berdasarkan hasil pengujian yang diperoleh dari kuesioner, berikut rekapitulasi hasil pengujian kualitas berdasarkan empat kriteria kualitas perangkat lunak berdasarkan model ISO 9126:

Tabel 1. Hasil Pengujian ISO 9126

Aspek	Skor Aktual	Skor Ideal	% Skor Aktual	Kriteria
Functionality	159	180	88.33%	Sangat Baik
Reliability	90	100	90%	Sangat Baik
Usability	141	160	88%	Sangat Baik
Efficiency	57	60	95%	Sangat Baik
Total	448	500	89.6%	Sangat Baik

Berdasarkan table di atas dapat disimpulkan bahwa tingkat kualitas perangkat lunak sistem informasi berbasis web untuk memperoleh jurnal secara keseluruhan dalam kriteria sangat baik dengan persentase 89.6%. Aspek kualitas tertinggi adalah berdasarkan aspek *Efficiency* dengan persentase 93.33% selanjutnya berdasarkan aspek *Functionality* dengan persentase 92.77%. Aspek *Reliability* adalah aspek urutan ketiga dengan persentase 88%. Aspek

yang mempunyai nilai terendah adalah aspek berdasarkan pada *Usability* dengan persentase 85.63%.

4. PENUTUP

Kesimpulan

Berdasarkan metode yang digunakan dalam pembuatan aplikasi steganografi dengan metode RC4 (Ron Code #4) menggunakan bahasa pemrograman visual basic 6.0 dapat digunakan untuk membuat atau menyisipkan informasi atau pesan rahasia didalam file *Tandatangan yang terdigitalisasi* dengan format .JPG, .BMP dan .GIF, dan dengan aplikasi ini dapat juga untuk mengekstrak pesan yang terdapat dalam *Tandatangan yang terdigitalisasi* tersebut dengan kata kunci yang sesuai.

DAFTAR PUSTAKA

[1] Moedjiono, "Pedoman Penelitian, Penyusunan dan Penilaian Tesis (v.5)". Jakarta: Universitas Budi Luhur, 2012. http://pascasarjana.budiluhur.ac.id/2012/10/pedoman-tesis-pps-ubl-v5-010112

[2] Kendall, "Analisis dan Perancangan Sistem". Jakarta, Prehallindo. 2003.

[3] Ir. Yusuf Kurniawan, MT., "Kriptografi: Keamanan Internet dan Jaringan. 2004.

[4] B.B.Gite, Divya Choksey, "Internatiional Journal Of Engineering Research and Aplications" Penerbit www.ijera.com. 2013.

[5] Jamaludin, " Aplikasi Keamanan Informasi Mengunakan Teknik Steganografi dengan Metode Least Significant Bit (LSB) Insertion Dan RC4" Penerbit Universitas Islam Negeri. 2010.

[6] Hanriyawan A. Mooduto, Albar ."Enkripsi Data Mengunkana Algoritma RC4". 2014