Data Penulis:

Dosen Universitas PGRI Semarang

Febrian Murti Dewanto, S.E., M.Kom	Program Studi Informatika
Bambang Agus Herlambang, M.Kom	Program Studi Informatika
Aris Tri Jaka Haryanta, M.Kom	Program Studi Informatika

Dosen STEKOM

Khoirur Rozikin, S.Kom, M.Kom	Program Studi Sistem Komputer
Purwanto, S.Kom	Program Teknik Elektronika
Iman Saufik Suasana, S.Kom, M.Kom	Program Studi Teknik Komputer
Arsito Ari Kuncoro, S.Kom, M.Kom	Program Studi Sistem Komputer
Danang, S.Kom, M.Kom	Program Studi Sistem Komputer
Dani Sasmoko, S.T., M.Eng	Program Studi Manajemen Informatika

Alumnus STEKOM

Achdlori, S.Kom	Program Studi Sistem Komputer
Bramuditya Adi Putra, S.Kom	Program Studi Sistem Komputer
Ilman Garwo Saputro, S.Kom	Program Studi Sistem Komputer
Lanni Dwi Saputri, S.Kom	Program Studi Sistem Komputer
Feriyanto, S.Kom	Program Studi Sistem Komputer

Penerbit: STEKOM Press

Jurnal ELKOM diterbitkan oleh Sekolah Tinggi Elektronika dan Komputer (STEKOM).
Jurnal ELKOM sebagai sarana komunikasi dan penyebarluasan hasil penelitian,
pemikiran serta pengabdian pada masyarakat

ISSN 1907-0012

Vol. 9 , No. 1, April 2016 ISSN 1907-0012

ELKOM
JURNAL ELEKTRONIKA DAN KOMPUTER

STEKOM
Sekolah Tinggi Elektronika dan Komputer
SEMARANG

ELKOM

JURNAL ELEKTRONIKA DAN KOMPUTER

Alamat Redaksi :
Lembaga Penelitian dan Pengabdian Masyarakat
Sekolah Tinggi Elektronika dan Komputer
Jl. Majapahit No. 605 Semarang Telp. 024-6723456
E-mail : elkom@stekom.ac.id

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa dengan terbitnya Jurnal ELKOM (Elektronika dan Komputer) Edisi April 2016, Volume 9 Nomor 1 Tahun 2016 dengan artikel-artikel yang selalu mengikuti perkembangan Ilmu Pengetahuan dan Teknologi dalam bidang Elektronika dan Komputer.

Semua artikel yang dimuat pada Jurnal Elektronika dan Komputer (ELKOM) ini telah ditelaah oleh Dewan Redaksi yang mempunyai kompetensi di bidang Elektronika dan Komputer.

Pada edisi ini kami menyajikan beberapa topik menarik antara lain makalah yang menggunakan aplikasi Android, multimedia, kerusakan *hardware* yaitu : "Desain Aplikasi *Augmented Reality* Berbasis Android Sebagai Media Promosi Universitas PGRI Semarang", "Multimedia Pembelajaran Interaktif Tuntunan Sholat Pada Mi Miftahul Ma'arif Kaliwungu Kudus", dan "Sistem Pakar Diagnosa Kerusakan Pada Televisi LED Dengan Menggunakan Metode *Forward Chaining* (Studi Kasus Di Wijaya Servis Elektronik)". Topik selanjutnya adalah makalah yang menggunakan aplikasi Sistem Informasi yaitu : "Sistem Monitoring BTS Berbasis Web Pada Divisi Telkom Flexi Semarang (Studi Kasus Pada Telkom Divre IV Jawa Tengah)", serta "Sistem Informasi Perpustakaan Menggunakan Radio Frequency Identification Berbasis *Client Server* Pada SMP Negeri 3 Juwana". Topik selanjutnya adalah makalah yang menerapkan Security System yaitu : "Integrasi *Or-Code* Pada Sistem Login Pembelajaran Online", dan "Perancangan Keamanan Data Dengan Sistem *Steganografi* Menggunakan Metode *Least Significant Bit*".

Terima kasih yang mendalam disampaikan kepada penulis makalah yang telah berkontribusi pada penerbitan Jurnal ELKOM edisi kali ini. Dengan rendah hati dan segala hormat, mengundang Dosen dan rekan sejawat peneliti dalam bidang Elektronika dan Komputer untuk mengirimkan naskah, *review*, gagasan dan opini untuk disajikan pada Jurnal Elektronika dan Komputer (ELKOM) ini.

Sebagai akhir kata, saran dan kritik terhadap Jurnal Elektronika dan Komputer (ELKOM) yang membangun sangat diharapkan. Selamat membaca.

Semarang, April 2016

Pemimpin Redaksi

Vol.9 No.1 April 2016

ELKOM

JURNAL ELEKTRONIKA DAN KOMPUTER

DAFTAR ISI

PERANCANGAN KEAMANAN DATA DENGAN SISTEM STEGANOGRAFI MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT*

Dani Sasmoko [1)], **Feriyanto** [2)]
[1)] Manajemen Informatika STEKOM Semarang
[2)] Sistem Komputer STEKOM Semarang

Sekolah Tinggi Elektronika dan Komputer
Jl. Majapahit 605 & 304 Semarang, Indonesia
E-mail : dani@stekom.ac.id

Abstract

Security is a preteksi to the destruction of data and use of data by users who do not have the authority and aims to maintain the confidentiality of information. Many companies are working to fortify its data security systems, but there are also companies that fortify security system is. One of them CV. AJI JAYA MANDIRI that the security system is less so susceptible entered into by parties who are not responsible.

From the problems arise the idea to do a data security by hiding information on other digital media that is not visible existence and this technique is called steganography. This research in the Research and Development (R & D), the system is designed with two main processes Embedding and Extracting stage and implemented in software Borland Delphi 7.0. Steganography Application can be used as an alternative security of confidential information without the need to make the other party feel suspicious, because it does not change the size of the file and does not degrade the quality of the image so that the chance of detection is very small
Keywords*: System data security, Steganography, Least Significant Bit*

Intisari

Keamanan merupakan suatu preteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan dan bertujuan menjaga kerahasiaan informasi. Banyak perusahaan yang berupaya membentengi sistem keamanan datanya, tetapi ada juga perusahaan yang membentengi sistem keamanannya apa adanya. Salah satunya CV. AJI JAYA MANDIRI yang sistem keamanannya kurang sehingga rentan dimasuki oleh pihak yang tidak bertanggung jawab.

Dari permasalahan tersebut muncul gagasan untuk melakukan pengamanan data dengan cara menyembunyikan informasi tersebut pada media digital lain agar tidak terlihat keberadaannya dan teknik ini disebut Steganography. Penelitian ini menggunakan metode *Research and Development* (R&D), sistem dirancang dengan dua buah proses utama yaitu tahap *Embedding* dan *Extracting* dan diimplemetasikan pada perangkat lunak Borland Delphi 7.0. Aplikasi Steganografi ini bisa dijadikan salah satu alternatif pengamanan informasi rahasia tanpa perlu membuat pihak lain merasa curiga, karena tidak merubah ukuran file dan tidak menurunkan kualitas gambar sehingga tidak terdeteksi.
Kata Kunci: Sistem keamanan data, Steganografi, Least Significant Bit

A. PENDAHULUAN

Keamanan data adalah suatu cara yang berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer (Gollmann, 1999). Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan. Sistem yang aman memastikan kerahasian data yang terdapat didalamnya. Beberapa aspek keamanan yaitu :

1. Mambatasi akses ke data dan servis.
2. Melakukan autentifikasi pada user.
3. Memonitor aktivitas yang mencurigakan seperti phishing ataupun sniffing.

Banyak sekali perusahaan-perusahaan yang berupaya membentengi data perusahaannya dengan berbagai cara. Tetapi ada juga perusahaan-perusahaan yang membentengi

sistem keamanan datanya apa adanya. Salah satunya yaitu CV. AJI JAYA MANDIRI.

CV. AJI JAYA MANDIRI adalah sebuah perusahaan yang bergerak dibidang jasa. Salah satu tugasnya yaitu membenahi sistem data dari perusahaan klien. Area kerja perusahaan ini mencakup seluruh Jawa Tengah misalnya Semarang,Yogyakarta dan Solo. Contoh klien dari perusahaan ini yaitu Jamsostek dan Dinas Imigrasi.

Tetapi walaupun bergerak dibidang sistem data perusahaan ini juga tidak memperhatikan keamanan pada sistem datanya karena semua orang yang berada didalam kantor tersebut dapat dengan mudah mengakses sistem datanya karena tidak adanya keamanan ganda pada sistem perusahaan tersebut. Sehingga dikhawatirkan ada pihak-pihak yang tidak bertanggung jawab yang menyalahgunakan kesempatan itu untuk mencuri data perusahaan.

Banyak aspek yang harus diperhatikan demi terciptanya keamanan data. Bisa saja seseorang mencuri komputer yang berisi data penting, mungkin juga karyawan yang diberi hak untuk mengakses data melakukan kejahatan dengan menjual informasi tersebut pada pihak lain demi kepentingan pribadi. Hal-hal tersebut memang termasuk kendala keamanan data yang harus mendapat perhatian, tetapi seorang administrator tidak dapat mengawasi kelemahan tersebut. Seorang administrator hanya fokus pada system data itu sendiri, dan hal inilah yang akan penulis bahas.

Tentunya perkembangan teknologi mengharuskan suatu perusahaan untuk mengimplementasikan sistem keamanan data yang bukan hanya aman tetapi juga mudah diakses dan handal, menyala 7 x 24 jam, 7 hari 1 minggu tanpa off. Oleh sebab itu diperlukan penyandian data seperti steganografi.

Steganografi merupakan teknik penyembunyian informasi dengan cara penyisipan pada suatu media. Kata steganography (steganografi) berasal dari bahasa Yunani yaitu steganos yang berarti menyembunyikan dan graptos artinya tulisan sehingga arti secara keseluruhan ialah tulisan yang disembunyikan (Stellars, 1996). Pengaplikasian steganografi ini dilakukan dengan menyisipkan pesan pada media gambar. Dengan metode ini pesan akan tersamarkan dengan baik pada file gambar yang dikirimkan, sehingga pengirim dapat dengan nyaman mengirimkan pesan rahasia pada gambar. Dengan cara ini akan sulit sekali untuk membaca secara kasat mata pesan yang disisipkan pada media gambar bila pesan tidak terlebih dahulu di ekstrak dari media gambar tersebut dan pesan akan tersimpan dengan aman.

Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi yang akan dibuat adalah dengan cara menyisipkan pesan ke dalam bit rendah (LSB - Least Significant Bit) pada data pixel yang menyusun file gambar. Metode penyisipan.LSB ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16, dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap pixel file gambar BMP 24 bit dapat disisipkan 3 bit pesan (Masaleno, 2006).

Dari uraian diatas maka penulis bermaksud memberikan solusi untuk perusahaan tersebut agar sistem keaamanan data lebih terjamin kerahasiannya yaitu dengan cara membuat aplikasi pengamanan data dengan sistem Stegamografi menggunakan Metode LSB (Least Significant Bit).

1. Rumusan Masalah

a. Bagaimana membuat sistem keamanan data pada CV Aji Jaya Mandiri yang menggunakan metode *sniffing* sehingga dapat dengan mudah diserang?
b. Bagaimana membuat sistem pengamanan data sehingga kerahasiaan datanya sangat terjamin?

2. Tujuan Penelitian

a. Membuat sistem keamanan data dengan aplikasi steganografi menggunakan metode *Least Significant Bit*.
b. Mengetahui efektifitas keamanan data menggunakan sistem steganografi

B. DASAR TEORI

1. Sistem

Menurut pendapat seorang ahli, sistem adalah himpunan dari unsur-unsur yang saling berkaitan sehingga membentuk satu kesatuan yang utuh dan terpadu. Sistem juga merupakan satu kesatuan yang terdiri dari elemen-elemen yang saling terkait antara satu dengan yang

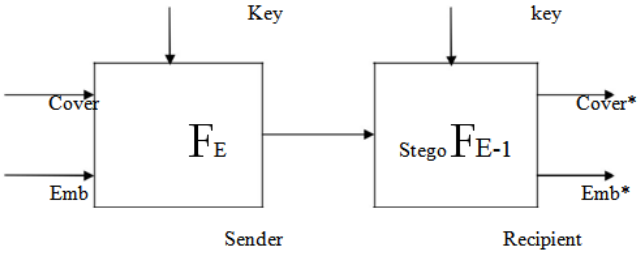
lainnya, tidak bisa dipisahkan (Hardware, Software, dan Brainware). (Al-Jufri, H; 2011).

Menurut John D. Howard dalam bukunya "*An Analysis of security incidents on the internet*" (2012:35) menyatakan bahwa :
"Keamanan data adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab". Menurut Sutarman (2012:3) "Data adalah fakta dari sesuatu pernyataan berasal dari kenyataan, di mana pernyataan tersebut merupakan hasil pengukuran atau pengamatan. Data dapat berupa angka-angka, huruf-huruf, simbol-simbol khusus, atau gabungan darinya".

2. Steganografi

Steganografi merupakan teknik penyembunyian informasi dengan cara penyisipan pada suatu media. Kata steganography (steganografi) berasal dari bahasa Yunani yaitu steganos yang berarti menyembunyikan dan graptos artinya tulisan. Jadi steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama (Ariyus, 2009).

Steganografi berbeda dengan Kriptografi, letak perbedaannya adalah hasil keluarannya. Hasil dari Kriptografi biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan dan dapat dikembalikan ke bentuk semula. Sedangkan Steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh komputer / perangkat pengolah digital lainnya.



Gambar 2. Cara kerja Steganografi secara umum

FE : Embedding (Penggabungan berkas cover dengan berkas pesan)
FE-1 : Extracting (Pengambilan berkas pesan dari berkas cover)
Cover : Berkas data yang akan disisipkan informasi (carrier)
Key : Kunci yang digunakan
Emb : Pesan yang akan disisipkan

Dalam proses Steganografi terdapat beberapa kriteria yang harus dipenuhi, kriterianya adalah sebagai berikut :

a. Impercepbility

Suatu kondisi dimana keberadaan pesan tidak dapat dipersepsi oleh indra manusia baik indera pendengaran maupun indera penglihatan.

b. Fidelity

Suatu kondisi dimana mutu media pembawa tidak berubah banyak akibat proses penyisipan.

c. Recovery

Suatu kondisi dimana pesan yang disembunyikan harus dapat diungkap kembali. Tujuan Steganografi adalah menyembunyikan informasi,maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai kebutuhan.

Steganografi menggunakan sebuah berkas yang disebut dengan cover atau biasa disebut dengan carrier, tujuannya sebagai pembawa dari pesan yang dirahasiakan. Banyak format carrier yang dapat dijadikan media untuk menyembunyikan pesan, diantaranya :

a. Format image (Format gambar) : Bitmap (.bmp), Graphics Interchange Format (.gif), Paintbrush Bitmap Graphic (.pcx),Join Photographic Expert Group (.jpeg), dll.
b. Format audio (Format suara) : Wideband Angular VibrationExperiment (.wav), Motion Picture Expert Group Audio

Stream Layer III (.mp3), Musical Instrument Digital Interface (.midi), dll.

c. Format lain : teks file, HyperText Markup Language (.html),Portable Document Format (.pdf), video dll.

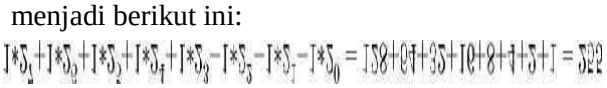
Pada dasarnya setiap media digital dapat digunakan sebagai media pembawa pada proses Steganografi. Penerapan Steganografi pada media digital menggunakan metode tertentu dan tergantung dari media yang dipilih sebagai carrier-nya.

3. Steganalisis

Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi yang tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendeteksian bahwa sebuah berkas yang diyakini berisikan data terselubung. Seperti dalam Kriptanalisis, diasumsikan bahwa sistem steganografi telah diketahui oleh si penyerang. Maka dari itu, keamanan dari sistem steganografi bergantung hanya pada fakta bahwa kunci rahasia tidak diketahui oleh si penyerang.

4. Least Significant Bit (LSB)

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling kecil. Letaknya adalah paling kanan dari barisan bit. Contohnya adalah bilangan biner dari 255 adalah 11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 11111111b).Bilangan tersebut dapat diartikan menjadi berikut ini:



Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan least significant bit (bit yang paling tidak berarti),Least significant bit sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain, salah satu yang memanfaatkan Least significant bit sebagai metode penyembunyian adalah steganografi audio, gambar dan video . Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. misalnya terdapat data raster original file gambar adalah sebagai berikut :

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka akan dihasilkan

00100110	11101001	11001000
00100110	11001000	11101000
11001000	00100111	11101001

Pada contoh diatas, hanya sebagian dari Least Significant Bit file carrier yang berubah (ditunjukkan dengan cetak tebal). Berdasarkan teori yang didapat bahwa kemungkinan terjadinya perubahan bit adalah sekitar 50%, karena peluang perubahannya antara 0 atau 1 dan dengan mengubah Least Significant Bit maka ukuran dari file pembawa tidak akan berubah sehingga akan sulit untuk terdeteksi (Bender, 1996). Sebagai contoh, untuk citra bitmap 24-bit yang berukuran 256 x 256 pixel terdapat 65536 pixel dan setiap pixel berukuran 3 byte (R=1 byte, G=1 byte dan B=1 byte), berarti seluruhnya ada 65536 x 3 = 196608 byte. Karena dalam setiap byte hanya bisa menyembunyikan 1 bit pada LSB-nya, maka ukuran berkas rahasia maksimum yang dapat disimpan pada citra tersebut adalah 196608/ 8 = 24576 byte atau 1/8 dari ukuran citra tersebut. Misalkan penyisipan pada citra 24-bit. Setiap pixel panjangnya 24 bit (3 x 3 byte, masing-masing komponen R (1 byte), G (1 byte), dan B (1 byte)

00110011 10100010 11100010
(misalkan pixel dipersepsi sebagai warna ungu)
Misalkan bit-bit embedded message: 010
Encoding:
00110010 10100011 11100010
(pixel berwarna "ungu berubah sedikit", manusia tidak dapat membedakan secara visual dengan citra aslinya).(ema utami,2009)

5. Borland Delphi

Menurut Tedy Budiman, (2008:29) bahwa "Delphi adalah suatu bahasa pemrograman berbasis Microsoft Windows yang didesain untuk dapat memanfaatkan fasilitas Microsoft Windows dengan optimal, khususnya Microsoft Windows 2000, Microsoft Windows XP, Microsoft Net, Delphi adalah perangkat pengembangan aplikasi yang berjalan di sistem operasi Windows. Delphi merupakan kelanjutan dari Turbo Pascal yang merupakan produk Borland, sekarang telah berganti menjadi Inprise Corporation. Delphi diluncurkan pertama kali pada tahun 1995. Borland menyatakan bahwa Delphi merupakan alat yang dapat digunakan untuk Rapid Application Development (RAD), yang hingga kini tetap terbukti menjadi bahasa pemrograman yang paling baik. Dengan keberhasilan ini maka Borland (sebelum menjadi Inprise), mengembangkan produk lain yang mirip yakni C++Builder, Jbuilder (Java Language). Dengan demikian jika telah menguasai Delphi maka dengan mudah dapat berpindah menggunakan bahasa pemrograman lainnya yaitu C++Builder atau Jbuilder. Kedua produk ini sengaja dibuat memiliki IDE yang sama dengan Delphi. Selain sebagai aplikasi biasa dengan mudah Delphi membuat aplikasi untuk internet. Seperti Win-CGI (Windows Common Gateway Interface), ISAPI (Internet Service Application Program Interface), Bahkan Borland menyatakan sebagai satu langkah menuju ActiveX. Seperti dengan mudah membuat sebuah aplikasi ActiveForm yang dapat berjalan pada Internet Explorer sebagai suatu aplikasi biasa. Selain itu Delphi dapat membuat aplikasi MIDAS, dimana pada aplikasi ini diharuskan membuat dua lapis, lapis pertama adalah aplikasi Server yang melayani permintaan aplikasi kedua yaitu Client. Delphi dapat mengakses database Paradox, xBase, MS-Access juga dengan menggunakan ODBC Delphi dapat mengakses database lain seperti Oracle, Sybase, Interbase, DB2, MS-SQL, MySQL

C. DESAIN PENELITIAN

1. Jenis Penelitian

Dalam penelitian ini penulis menggunakan penelitian Research and Development (R&D). Menurut Sugiyono (2009:407) metode penelitian Research and Development yang selanjutnya akan disingkat menjadi R&D adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Produk tersebut tidak selalu berbentuk benda atau perangkat keras (hardware), seperti buku, alat tulis, dan alat pembelajaran lainnya. Akan tetapi, dapat pula dalam bentuk perangkat lunak (software).

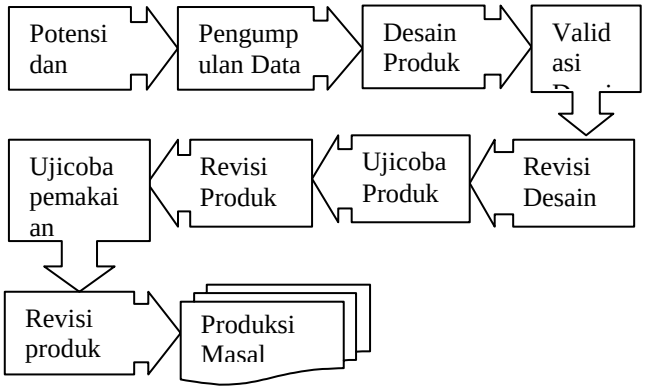
Menurut Gay (1990), penelitian pengembangan merupakan suatu usaha untuk mengembangkan suatu produk yang efektif untuk digunakansekolah, dan bukan untuk menguji teori. Sedangkan menurut Borg & Gall (1983), penelitian dan pengembangan merupakan suatu proses yang dipakai untuk mengembangkan dan memvalidasi produk pendidikan.

Penelitian ini mengikuti suatu langkah-langkah secara siklus terdiri atas kajian tentang temuan penelitian produk yang akan dikembangkan, mengembangkan produk berdasarkan temuan-temuan tersebut, melakukan uji coba lapangan sesuai dengan latar belakang dimana produk itu akan dipakai, dan melakukan revisi terhadap hasil yang diperoleh dari uji coba lapangan. Penelitian pengembangan juga didefinisikan sebagai kajian secara sistematik untuk merancang, mengembangkan, dan mengevaluasi program-program, proses dan hasil-hasil pembelajaran yang harus memenuhi kriteria konsistensi dan keefektifan secara internal. (Seels & Richey, 1994). Sedangkan Plomp

(1999) menambahkan kriteria "dapat menunjukkan nilai tambah" selain ketiga kriteria tersebut.

2. **Metode Pengembangan**

Teori yang dipergunakan adalah metode (R & D) *Research and Development* yang menurut Sugiyono (2010) menyebut bahwa metode ini memiliki 10 tahapan yaitu : (1) Potensi dan masalah, (2) Pengumpulan data, (3) Desain produk, (4) Validasi desain, (5) Revisi desain, (6) Ujicoba produk, (7) Revisi produk, (8) Ujicoba pemakaian, (9) Revisi produk, dan (10) Produksi masal. Bagan tahapan – tahapan dalam metode R & D (Research And Development) adalah sebagai berikut ini :



Gambar 2. Tahapan Metode R & D
Sumber : Sugiyono (2010)

D. HASIL DAN PEMBAHASAN

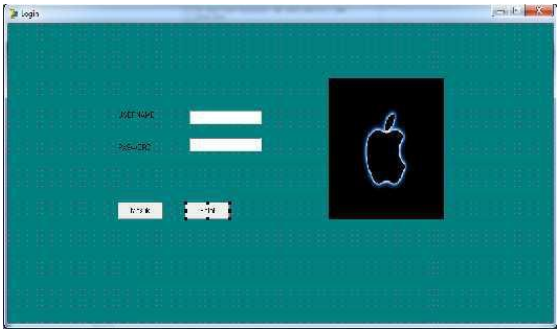
1. Pengumpulan Data Awal

Dalam tahapan ini akan dilakukan identifikasi perkiraan kebutuhan pemakai dan juga mempelajari literatur dan meneliti lebih terperinci tentang permasalahan yang ada di CV.AJI JAYA MANDIRI. Penulis mengumpulkan data-data yang ada melalui berbagai kegiatan mulai observasi dan wawancara secara langsung dan juga melihat fakta secara langsung mengenai Sistem Keamanan yang ada di CV.AJI JAYA MANDIRI tersebut, kemudian dibandingkan maupun diperkuat dengan teori-teori yang didapatkan dari hasil studi pustaka dari literatur-literatur. Kegiatan ini di lakukan pada CV.AJI JAYA MANDIRI Semarang dengan melibatkan beberapa permasalahan yang ada didalamnya. Penelitian awal dilakukan untuk mendapatkan informasi kebutuhan dalam penelitian.

Pembuatan Produk Awal Pada bagian ini membahas tentang teknik pengembangan sistem sesuai dengan desain sistem. Proses pengembangan diawali dengan pembuatan project baru menggunakan Borland Delphi 7, penyusunan menu utama kemudian menyusun form-form utuk baca pesan, form untuk tulis pesan yang berkaitan dengan Sistem Keamanan Data tersebut. Bagian-bagian tersebut merupakan hal penting bagi sebuah sistem.

2. Hasil Pengembangan desain

a. Tampilan Form Login

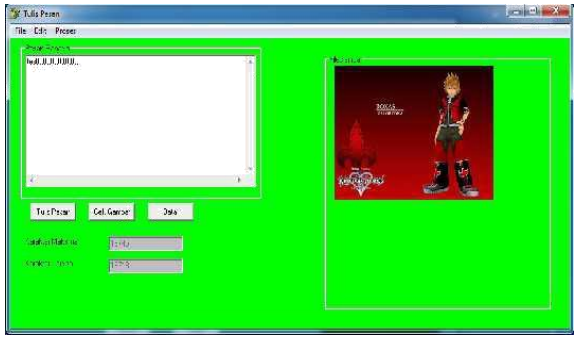


Gambar 3. Tampilan Form Login

b. Tampilan Form Menu Utama

Gambar 2. Tampilan Form Menu Utama

c. Tampilan Form Tulis Pesan



Adapun untuk tampilan proses penyisipan suatu pesan di dalam gambar yaitu seperti diatas.Setelah itu ketika proses enkripsi suatu pesan selesai maka tampilannya akan seperti dibawah ini:

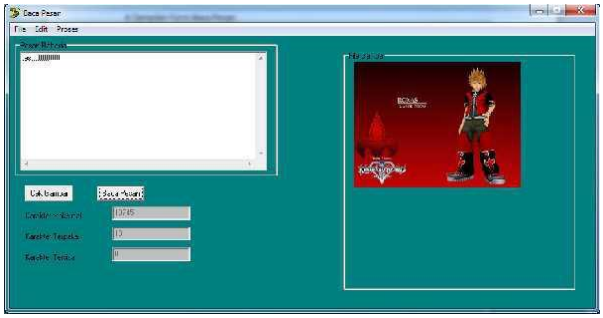
a. Tampilan proses setelah penyisipan

Gambar 4. Tampilan proses setelah penyisipan

b. Tampilan Form Baca Pesan

Gambar 4. Tampilan Form Baca Pesan

Sekarang kita akan melihat apakah didalam gambar tersebut ada pesan tersembunyi atau tidak ada.Kita cari file gambar yang kita sisipi pesan tadi seperti gamabar diatas.Untuk melihat apakah gambar tadi berisi pesan rahasia atau tidak maka kita perlu untuk menekan tombol Baca Pesan agar keliatan isi pesan tersebut.Berikut tampilan setelah saya menekan tombol baca pesan untuk melihat pesan tersebut.



Gambar 5. Tampilan setelah proses descripsy

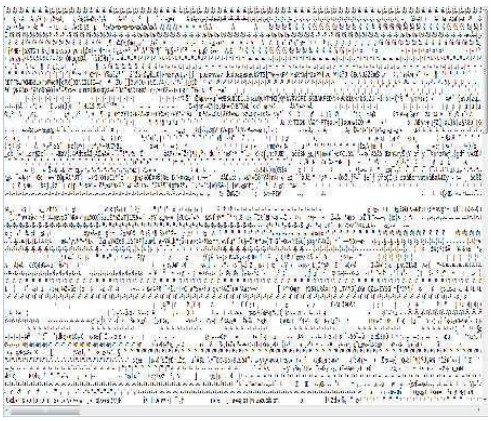
3. Pengujian Ukuran File sebelum dan setelah disispi pesan

Tabel 4.3 perbandingan ukuran file

No	Nama File	Ukuran pixel	Ukuran Sebelum	Ukuran file text	Ukuran sesudah
1	Boy.bmp	254x150	147 kb	200 bytes	147 kb
2	Apple.bmp	240x230	156 kb	300 bytes	156 kb
3	Car.bmp	225x230	145 kb	350 bytes	145 kb
4	Wall.bmp	325x320	200 kb	375 bytes	200 kb

Dari data diatas dapat diketahui bahwa ukuran file yang disisipi pesan tidak berubah sehingga tidak mengundang kecurigaan dari pihak lain jika file tersebut terdapat pesan rahasia didalamnya.

4. Pengujian pendeteksian data jika dibuka secara paksa



Gambar 4.11 File yang dibuka paksa

Dari gambar diatas maka bisa disimpulkan bahwa gambar yang telah disisipi pesan rahasia sangat aman kerahasiaannya walaupun jatuh kepihak yang tidak bertanggung jawab. Karena data yang berada didalam gambar tidak dapat dibaca jika tidak menggunakan proram yang sudah penulis rancang. Jadi dapat ditarik kesimpulan bahwa produk ini bisa digunakan di CV.AJI JAYA MANDIRI walaupun mungkin masih ada sedikit kekurangan

E. SIMPULAN DAN SARAN

1. Simpulan

   Setelah dianalisa dan dievaluasi keadaan di CV.AJI JAYA MANDIRI dan membandingkan dengan teori, maka pada bab ini akan diambil kesimpulan dan saran yang mungkin berguna bagi pihak perusahaan. Beberapa kesimpulan yang diambil oleh penulis adalah sebagai berikut:
   1) Dengan menggunakan metode Least Significant Bit (LSB) yaitu suatu metode penyembunyian pesan rahasia melalui media digital file image, maka aplikasi steganografi tersebut dapat di bangun yaitu dengan cara mengganti bit ke-8, 16, dan 24 pada representasi biner file image bmp 24-bit dengan representasi biner pesan rahasia yang akan disembunyikan.
   2) Ukuran file gambar yang sudah disisipkan informasi tidak mengalami perubahan. Dengan tidak berubahnya ukuran file tersebut maka kemungkinan besar orang lain tidak akan mngetahui bahwa ada informasi rahasia didalam file tersebut.

2. Keterbatasan Produk

   Produk hasil pengembangan penulis ini masih memiliki keterbatasan sebagai berikut :
   1) Implementasi Steganografi hanya menggunakan media gambar/citra untuk menyisipkan pesan, tidak dapat diimplementasikan dalam media lain seperti audio dan video.
   2) Program hanya dapat menyisipkan pesan teks karakter, tidak dapat menyisipkan data atau file dokumen.
   3) Aplikasi hanya dapat berjalan dilingkungan sistem operasi windows, tidak dapat digunakan oleh pengguna sistem operasi lainnya seperti Linux dan MacOSX.

3. Saran

   Adapun saran-saran yang dapat dikemukakan oleh penulis adalah sebagai berikut:
   1) Program bisa dikembangkan tidak hanya media text saja tetapi media citra dan video, audio maupun media digital lainnya.
   2) Pengembangan lebih lanjut untuk memakai data selain BMP sepeti JPEG Dan PNG.

DAFTAR PUSTAKA

Binanto, Iwan. 2005; "Konsep Dasar Program" , Jakarta: PT. Elex Media Komputindo

Borg, Walter R., & Gall, M.D, 1983; "Educational research: An introduction (4ed)", New York & London: Longman

Bentley, Lonnie D & Whitten, Jeffrey L, 2007; "Systems Analysis and Design for the Global Enterprise, (7ed)" McGrawHill, New York

Connolly, Thomas & Begg, Carolyn, 2010; "Database Systems: A Practical Approach to Design, Implementation, and Management (5ed)" Pearson Education, Boston.

Jogiyanto, HM, 2007; "Analisis dan Desain Sistem Informasi 2", Yogyakarta: Andi Offset

Kadir, A, 2009; "Membuat Aplikasi Web dengan PHP dan Database MySQL",Yogyakarta: Andi Offset

Masaleno, Andino, 2006,"Pengantar steganography", www.ilmu komputer.com.

Mulyanto, Agus, 2009; "Sistem Informasi Konsep & Aplikasi", Yogyakarta: Pustaka Pelajar

Nugroho, Bunafit, 2012; "Panduan Membuat Program Toko dengan PHP, MySQL dan Dreamweaver Point Of Sale (POS) Berbasis Web", Yogyakarta: Alif Media

Sutarman, 2012; "Buku Pengantar Teknologi Informasi", Jakarta: Bumi Aksara.

wikipedia.org/wiki/Least_significant_bit.diakses pada tanggal 07 april 2013