JURNAL SKRIPSI

PENGAMANAN DATA MENGGUNAKAN *STEGANOGRAPHY* DENGAN METODE *LEAST SIGNIFICANT BIT* PADA PT THE NIELSEN COMPANY INDONESIA SEMARANG

Penulis:

MASRUKHAN, SISWANTO, S.Pd, S.Kom, M.Kom

PROGRAM STRATA-1
SISTEM KOMPUTER
Sekolah Tinggi Elektronika dan Komputer
STEKOM - SEMARANG
2014

PENGAMANAN DATA MENGGUNAKAN *STEGANOGRAPHY* DENGAN METODE *LEAST SIGNIFICANT BIT* PADA PT THE NIELSEN COMPANY INDONESIA SEMARANG

Penulis : MASRUKHAN, SISWANTO, S.Pd, S.Kom, M.Kom

Program Studi Sistem Komputer – STEKOM Semarang

Rukhan.nielsen@yahoo.com

ABSTRAK

Semakin berkembangnya teknologi komunikasi pada erah saat ini kebutuhan akan keamanan dalam berkomunikasi jadi sangat penting. Maka penulis melakukan penelitian ini bertujuan untuk mengamankan pesan teks yang dikirim. PT. The Nielsen Company Indonesia Semarang dihadapkan dengan beberapa kendala, salah satu kendala adalah pengiriman hasil audit yang dilakukan oleh auditor dilapangan belum ada sistem pengamannya.

Metode penelitian yang digunakan adalah *Research and Development* (R&D) yang terdiri dari 10 langkah namun pengembangan sistem yang dilaksanakan pada penelitian ini hanya sampai pada tahan ke 6 (enam) menghasilkan produk akhir berupa *prototype,* sehingga tidak sampai pada tahap implementasi produk. Keenam langkah tersebut adalah *Research and information collecting, Planning, Develop prelminaryformof product, Preliminary field testing, Main product revision* dan *Main field testing.*

Dengan teknik *steganography* dan metode *least significant bit,* Serta *viginere cipher* untuk melakukan proses enskripsi dan deskripsi pesan teks yang disisipkan pada file gambar. Pesan yang dikirim hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut dengan menggunakan kunci rahasia. Aplikasi ini dibuat dengan menggunakan *Microsoft Visual Basic 6.0* dan *database Microsoft Access.*

Hasil dari analisa penelitian ini menunjukan hasil yang baik bila digunakan untuk mengirim pesan rahasia, karna *image* tidak kasat mata bila dipandang. Sehingga pesan yang dikirim terjamin keamanannya.

Kata kunci : *Steganography, Least Significant Bit, Viginere Ciper,* Citra GIF, *Research and Development* (R&D),

Jumlah Halaman : 74 + Lampiran 15

1. Latar Belakang

Seiring dengan perkembangan teknologi, ancaman terhadap keamanan data semakin besar, terutama untuk data yang dirahasiakan. Berbagai ancaman di dunia maya seperti *hacker, cracker, carder* membuat orang khawatir akan keamanan data yang dikirimnya. Kekhawatiran inilah yang membuat pengiriman data sedikit terhambat, sedangkan data tersebut sangat penting bagi orang-orang tertentu. Data adalah kenyataan yang menggambarkan suatu kejadian dan merupakan kesatuan nyata yang nantinya akan digunakan sebagai bahan dasar suatu informasi.

Untuk mengamankan data atau informasi tersebut dapat dilakukan dengan beberapa cara, salah satunya adalah *Steganography*. Istilah

Steganography berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan. Jadi, *Steganography* 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. Kita semua menyadari bahwa bahwa Teknologi Informasi Dan Komunikasi (TIK) berkembang sangat cepat dan telah membantu di berbagai bidang kehidupan manusia, TIK juga memudahkan manusia dalam menyelesaikan segala macam permasalahan di berbagai bidang seperti bidang riset, bidang perdagangan, bidang kesehatan, bidang pemasaran, bidang pendidikan dan sebagainya, di bidang Riset Teknologi Informasi Dan Komunikasi (TIK) bisa memberikan informasi seperti mengetahui sejauh mana tingkat penerimaan konsumen terhadap produk, mengetahui sejauh mana minat konsumen terhadap pembelian produk, dan mengetahui tingkat pangsa pasar.

Nielsen adalah suatu perusahaan yang bergerak di bidang jasa yang berfokus pada suatu penelitian dan melakukan suatu riset pasar. Dalam memberikan suatu informasi tentang pemasaran dan konsumen kepada *client* auditor melakukan pengecekan langsung di lapangan, sehingga produsen dapat memahami *psikologis, sosiologis* dan selera konsumen. Inilah yang menjadi celah bocornya data ke pihak pihak yang tidak berwenang.

Dari uraian permasalahan di atas, maka penulis ingin membuat rancang bangun pengamanan data menggunakan *Steganography* untuk membantu para auditor dalam proses pengiriman data agar data aman sampai tujuan. Sedangkan strategi penyembunyian data citra yang digunakan untuk menyisipkan citra kedalam media citra adalah dengan metode *Least Significant Bit (LSB)*. Untuk teknik LSB, menggunakan teknik subtitusi, dimana nilai bit terakhir pada tiap- tiap pixel citra digital akan digantikan dengan nilai bit tiap-tiap karakter pesan rahasia yang akan disembunyikan. Pada file citra 24 bit setiap piksel pada citra terdiri dari susunan tiga warna, yaitu merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Informasi dari warna biru berada pada bit 1 sampai bit 8, dan informasi warna hijau berada pada bit 9 sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24. Pengamanan data menggunakan *Steganography* Dengan Metode *Least Significant Bit* di harapkan dapat membantu auditor pada PT The Nielsen Company Indonesia Semarang dalam meningkatkan kemanan data yang di kirim.

2 Rumusan Masalah

Berdasarkan latar belakang permasalahan yang telah diuraian diatas sebelumnya maka dapat dirumuskan permasalahan sebagai berikut

a. Bagaimana membuat desain sistem pengamanan data, untuk proses pengiriman data di PT The Nielsen Company Indonesia Semarang yang valid ?
b. Apakah prototaipe produk aplikasi *Steganography* untuk pengamana dalam proses pengiriman data yang di kembangkan di PT The Nielsen Company Indonesia Semarang efektif di gunakan di lapangan ?

3. Tujuan

Tujuan dari penelitian skripsi ini adalah :

a. Membuat desain sistem untuk pengamanan dalam proses pengiriman data yang valid dengan *Steganography* menggunakan metode *Least Significant Bit (LSB)*.
b. Menghasilkan sistem untuk pengamanan data dengan metode *Least Significant Bit (LSB)* yang efektif untuk membantu auditor dalam proses pengiriman data.

4. Manfaat

Adapun penulisan penelitian ini dapat memberikan beberapa manfaat antara lain sebagai berikut :

a. Manfaat praktis
   Hasil penelitian ini diharapkan dapat memberikan masukan kepada perusahaan sehingga terwujudnya suatu proses keamanan dalam pengiriman data.
b. Manfaat teoritis
   Hasil penelitian ini diharapkan dapat memberikan sumbangan untuk pengembangan teori yang berkaitan dengan proses keamanan pengiriman data.

c. Manfaat Bagi Peneliti

Bagi Peneliti, dapat menambah wawasan dan mengaplikasikan ilmu yang telah diperoleh selama menempuh studi di STEKOM dan sekarang dapat menerapkan ilmu tersebut langsung dilapangan.

Sebagai acuan bagi peneliti selanjutnya, khususnya penelitian yang berkaitan dengan pengembangan proses pengiriman data.

5. Deskripsi Teoritik

5.1 Pengertian Pengamanan

Menurut Gollmann pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa : keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer

5.2 Pengertian Data

Menurut Connolly dan Begg (2010), data adalah komponen yang paling penting dalam DBMS, berasal dari sudut pandang *end-user*. Data bertindak sebagai jembatan yang menghubungkan antara mesin dengan pengguna.

5.3 Pengertian *Steganography*

Steganography merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan *Steganography* adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis (Cox et al, 2008).

5.4 Pengertian *Least Significant Bit*

Metode LSB merupakan teknik substitusi pada *Steganography*. Biasanya, arsip 24-bit atau 8-bit digunakan untuk menyimpan citra digital. Representasi warna dari piksel–piksel bisa diperoleh dari warna–warna primer, yaitu merah, hijau dan biru. Citra 24-bit menggunakan 3 byte untuk masing–masing piksel, dimana setiap warna primer direpresentasikan dengan ukuran 1 byte. Penggunaan citra 24-bit memungkinkan setiap piksel direpresentasikan dengan nilai warna sebanyak 16.777.216. Untuk teknik LSB, menggunakan teknik subtitusi, dimana nilai bit terakhir pada tiap- tiap pixel citra digital akan digantikan dengan nilai bit tiap-tiap karakter pesan rahasia yang akan disembunyikan (Ariyus, 2009).

5.5 Enkripsi dan Dekripsi

Enkripsi adalah hal yang sangat penting dalam *Steganography*, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bias diartikan dengan cipher atau kode.

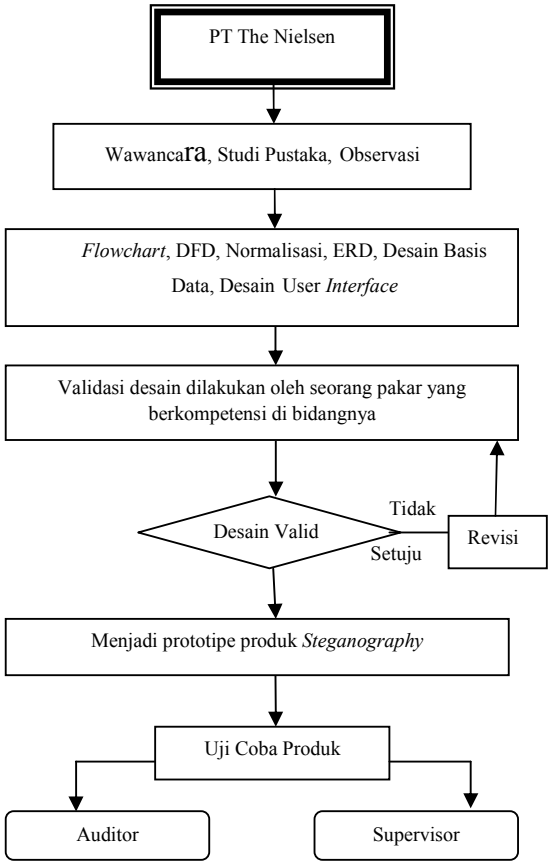
Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya(teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

Keamanan dari *Steganography* modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan keamanan algoritma tergantung pada kunci yang dipakai, maka algoritma ini bisa dipublikasikan dan dianalisa orang lain.

5.7 *Vigenere Cipher*

Definisi *Vigenere Cipher* menurut Budi Satrio (2007), *Vigenere Cipher* adalah salah satu jenis *kriptography* klasik yang pada dasarnya adalah melakukan substitusi *cipher* abjad majemuk (*polyalphabetic substitution*), yaitu mengubah *plaintext* dengan kunci tertentu biasanya berupa sebuah kata atau kalimat yang berulang sepanjang *plaintext* sehingga didapatkan *ciphertext.* Diharapkan dengan metode ini, kunci yang dihasilkan untuk *Vigenere Cipher* menjadi lebih panjang dan acak sehingga akan menyulitkan *kriptanalisis* untuk menyerang dengan metode *Kasiski* maupun dengan analisis frekuensi.

5.8 Kerangka Pikir

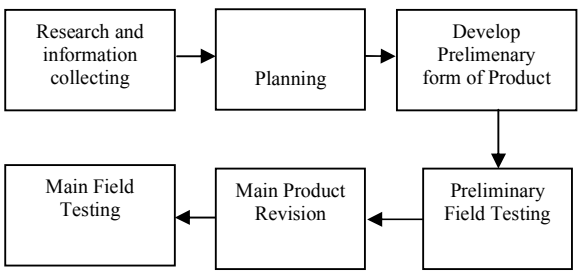


Gambar 5.1 Kerangka Penelitian

6. Metode Penelitian

6.1 Model Pengembangan

Dalam penelitian ini penulis menggunakan pendekatan metode R & D (*Research and Development*) menurut Brog & Gall (1983:775) yang merupakan suatu metode penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji produk tertentu. Dalam penelitian ini digunakan hanya 6 langkah yaitu :

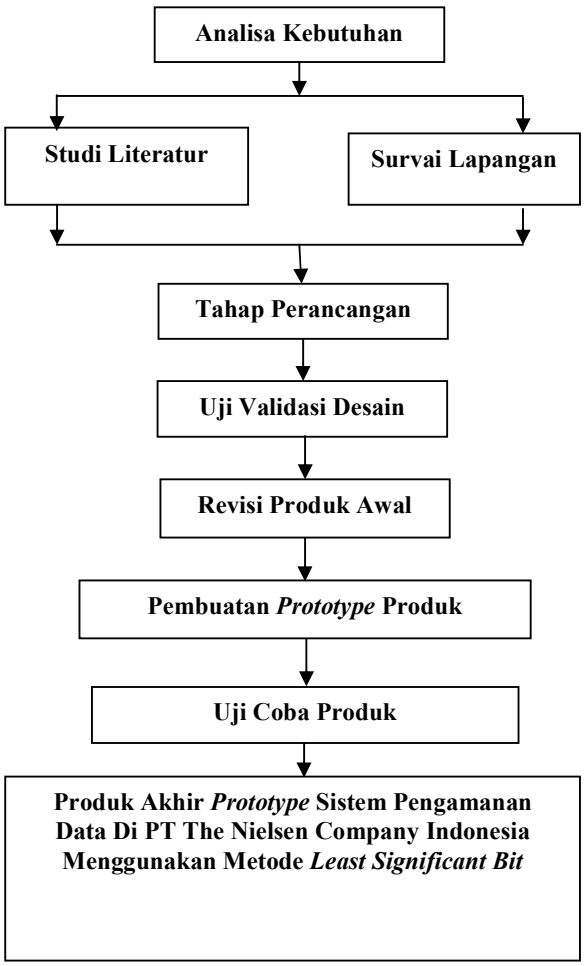


Gambar 6.1 Model Pengembangan

6.2 Prosedur Pengembangan

Berdasarkan model pengembangan yang dilakukan menggunakan model *Research and Development* (*R&D*) Borg dan Gall, prosedur pengembangan yang ditempuh terdiri dari enam langkah, yaitu (1) *Research and information collecting,*(2) *Planning,*(3) *Develop prelminaryformof product,*(4) *Preliminary field testing,* (5) *Main product revision,* (6) *Main field testing.* Maka prosedur pengembangan dalam penelitian pengembangan ini mengikuti langkah yang di instruksikan dalam model desain tersebut.

Adapun prosedur pengembangan sistem pengamanan data digambarkan sebagai berikut :



Gambar 6.2 Prosedur Pengembangan

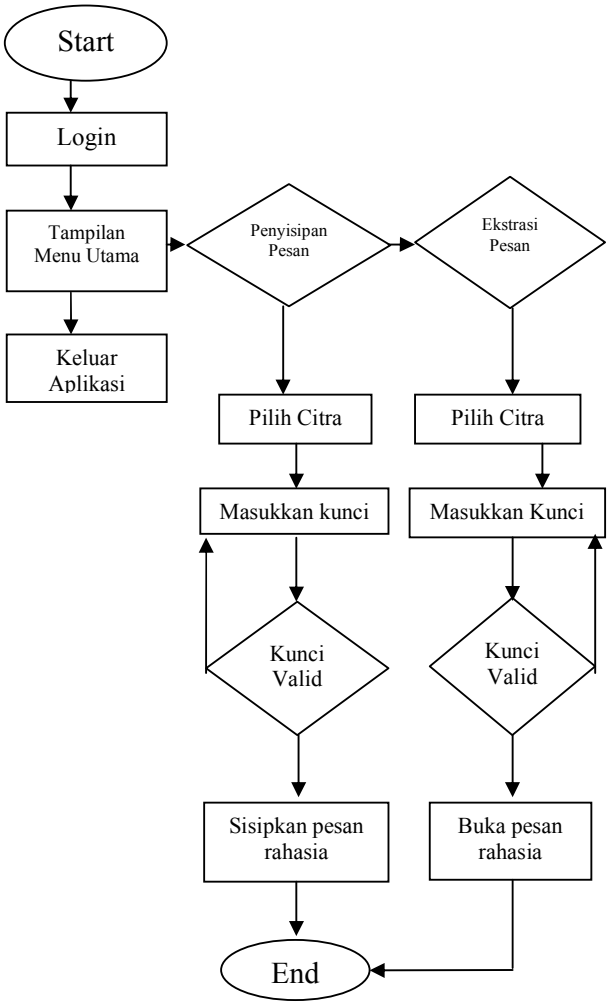
7. Tahap Desain Produk

7.1 Desain Awal

Untuk mendapatkan sistem yang terancang baik digunakan beberapa alat bantu seperti *Flowchart,* Data Flow Diagram (DFD), Dekomposisi Diagram, Entity Relational Diagram (ERD), tampilan input dan output. Berikut adalah perancangan sistem yang akan dibangun.

a) Flowchart

Flowchart Sistem Pengamanan Data

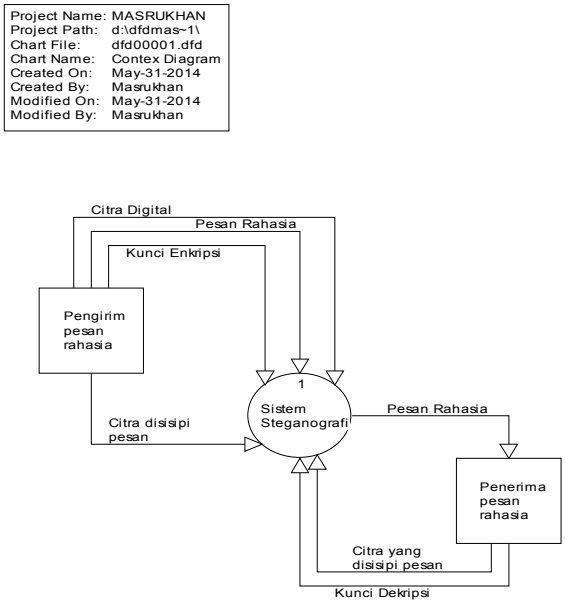


Gambar 7.1 *Flowchart*

b) *Data Flow Diagram* (DFD)

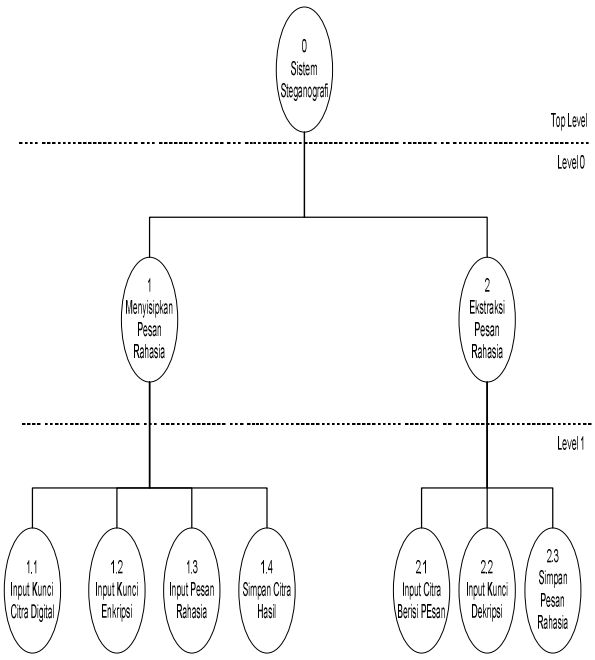
1.*Contex Diagram*

Contex Diagram atau Diagram Kontex menggambarkan hubungan antar entitas sistem digitaliasi data, dalam hal ini adalah sistem penginputan data yang dipresentasikan dengan lingkaran tunggal yang mewakili keseluruhan sistem. Adapun context diagramnya sebagai berikut:



Gambar 7.2 Contex Diagram Sistem Pengaman Data

2. Dekomposisi Diagram

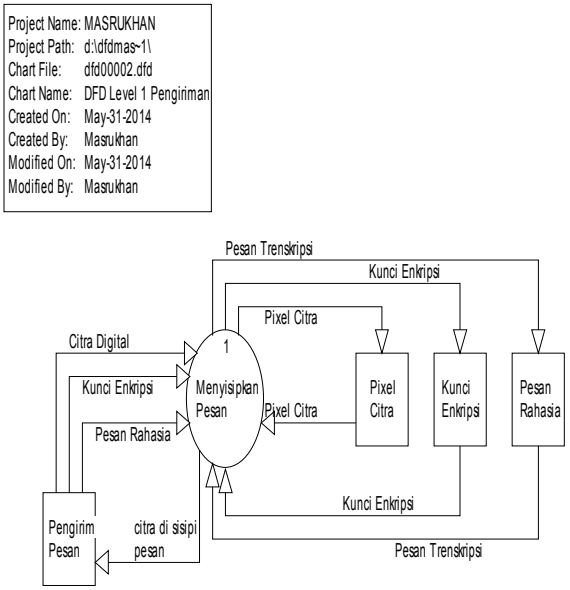


Gambar 7.3 Dekomposisi Diagram

Dekomposisi diagram menggambarkan hierarki proses- proses di dalam system steganografi. Proses- proses tersebut nantinya akan digunakan sebagai dasar penyusunan diagram DFD Leveled. Pada system steganografi ini memiliki total sembilan buah proses.

3. DFD Level 1 Pengiriman

Berikut ini merupakan gambar dari DFD Level 1 Pengiriman

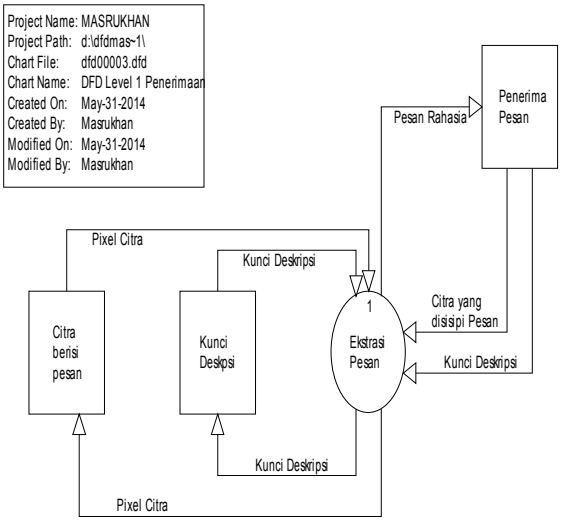


Gambar 7.4 DFD Level 1 Pengiriman

Gambar di atas merupakan diagram DFD Level 1 pengiriman, yang menggambarkan proses penyisipan pesan kedalam gambar dan enkripsi pesan.

4. DFD Level 1 Penerimaan

Berikut ini merupakan gambar dari DFD Level 1 Penerimaan



Gambar 7.5 DFD Level 1 Penerimaan

Gambar di atas merupakan diagram DFD Level 1 penerimaan, yang menggambarkan proses deskripsi pesan. Agar pesan dapat terbaca oleh penerima pesan.

8. HASIL DAN PEMBAHASAN

8.1 Hasil Penelitian

Pada skripsi ini ada dua uji validasi yang dilakukan yaitu validasi desain oleh pakar dan validasi produk oleh *user*. Validasi desain ini dilakukan oleh pakar yang diwakili oleh dosen STEKOM yaitu Bp. Dani Sasmoko, S.T, M.Eng yang berkompeten untuk rancangan desain yang akan dibuat. Validasi uji coba produk dilakukan dengan subjek penelitian adalah para calon *user* yaitu empat orang pegawai PT. The Nielsen Company Indonesia Semarang perwakilan dari supervisor dan auditor.

Validasi desain yang dilakukan oleh pakar dan validasi produk oleh *user* ini mempunyai penilaian yang digunakan sebagai indikator dan kesimpulan dalam pemberian nilai terhadap hasil validasi, seperti yang ditunjukkan tabel di bawah ini :

Tabel 4.1 Indikator

SKOR	NILAI
$1 \leq n \leq 10$	Tidak baik
$11 \leq n \leq 20$	Cukup
$21 \leq n \leq 30$	Baik
$31 \leq n \leq 40$	Sangat baik

Tabel 4.2 Kesimpulan

No	Kesimpulan
1	Belum dapat digunakan dan harus diganti
2	Dapat digunakan dengan banyak revisi
3	Dapat digunakan dengan sedikit revisi
4	Dapat digunakan tanpa revisi

Hasil dari validasi desain yang dilaksanakan pada tanggal 5 juni 2014 terhadap desain yang dilakukan oleh pakar yang berkompeten di bidang sistem pengamanan data. Rancangan

aplikasi sistem pengamanan data ini memperoleh total poin sebesar 37. Dosen yang telah ditunjuk sebagai pakar diberikan angket instrument penelitian yang telah disiapkan oleh peneliti. Sesuai dengan tabel indikator nilai, hasil yang didapatkan untuk rancangan desain aplikasi ini adalah "Sangat Baik". Kesimpulan yang diambil oleh pakar untuk rancangan sistem ini adalah "Sangat Baik, sehingga dapat digunakan.

Sedangkan untuk uji coba produk ke pengguna dilakukan 24 juli 2014 dan diperoleh hasil sangat baik. Data-data tersebut merupakan data kualitatif yang didapatkan dari hasil penilaian, masukkan, tanggapan, kritik, dan saran perbaikan melalui angket pertanyaan terbuka yang diberikan kepada calon pengguna.

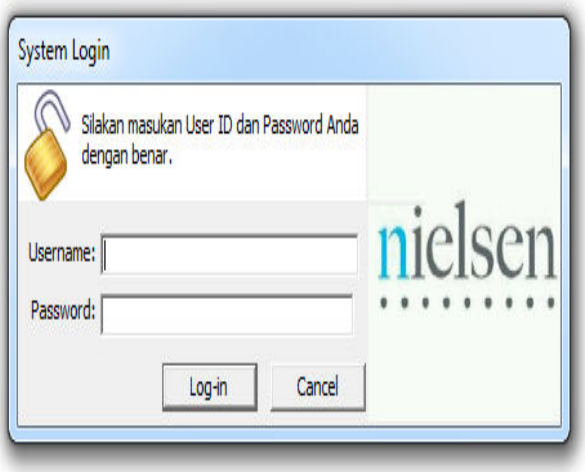
Prototype sistem yang dibuat sudah melewati tahapan validasi oleh pakar dan ujicoba oleh *user*. Hal ini dilakukan untuk menilai *prototype* yang dibuat apakah telah sesuai dengan tujuan penelitian yang diharapkan.

Dari total nilai seluruh *user* yang mengisi angket dengan nilai rata- rata hasil pengujian produk adalah 35 dan didapatkan indikator "Sangat Baik". Kesimpulan yang diambil oleh *user* untuk *prototype* ini adalah "Sangat Baik, sehingga dapat digunakan tanpa revisi".

8.2 Hasil Pengembangan

1. Halaman Login

Halaman login administrator digunakan untuk masuk ke sistem pengamanan data dengan memasukkan username dan password.

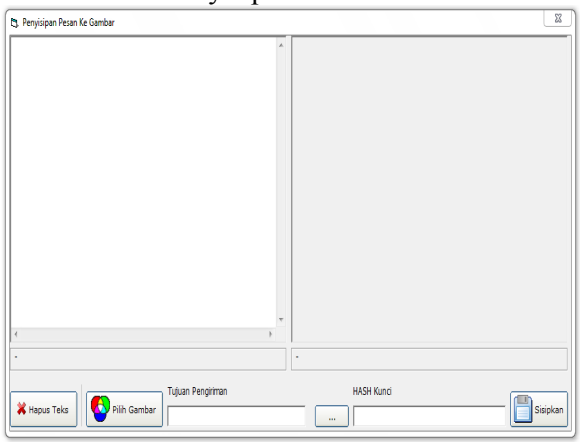


Gambar 8.1 Halaman Utama

2. Halaman Utama

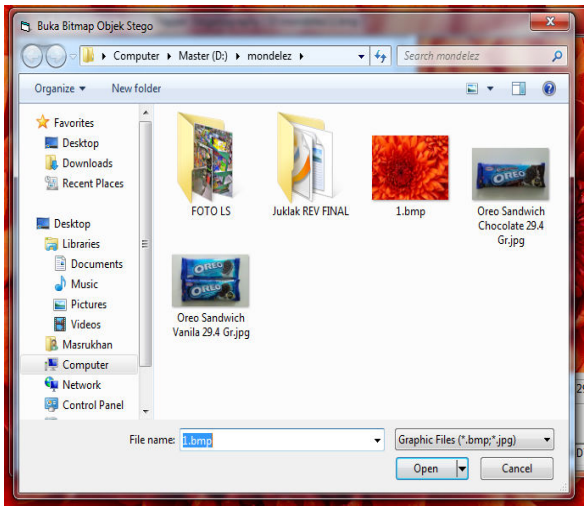
Gambar 8.2 Halaman Utama

3. Halaman Penyisipan Pesan



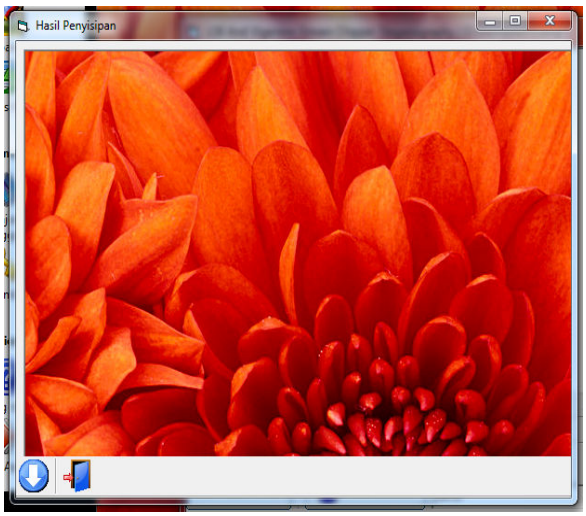
Gambar 8.3 Halaman Penyisipan Pesan

4. Halaman Pilih Gambar



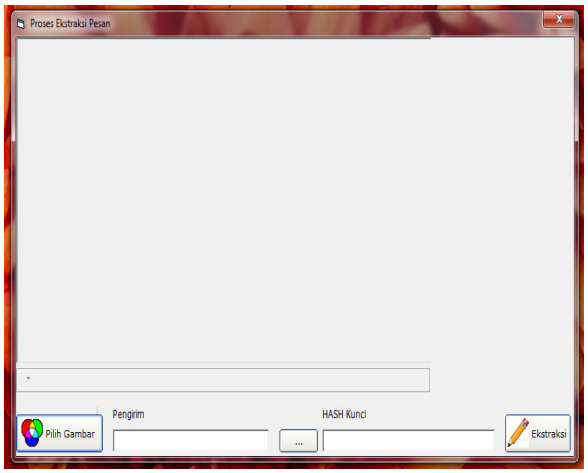
Gambar 8.4 Halaman Pilih Gambar

5. Halaman Hasil Penyisipan Pesan



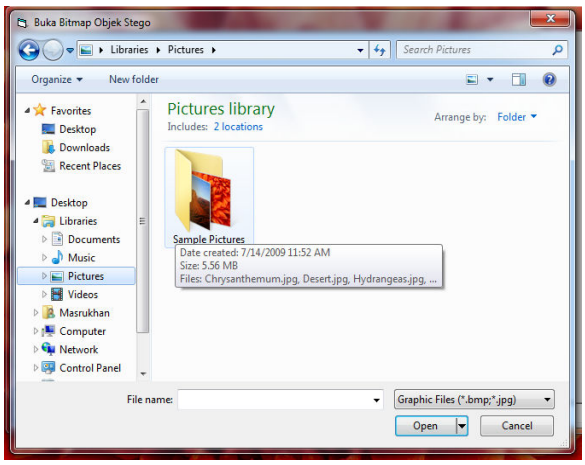
Gambar 8.5 Halaman Hasil Penyisipan Pesan

6. Halaman Ekstrasi Pesan



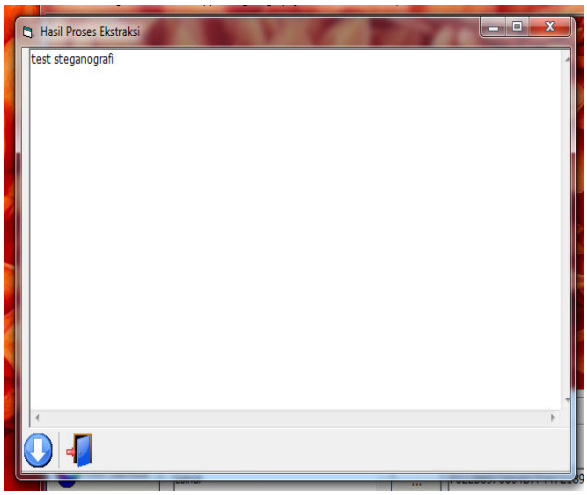
Gambar 4.6 Halaman Ekstrasi Pesan

7. Halaman Pilih Gambar Ekstrasi Pesan



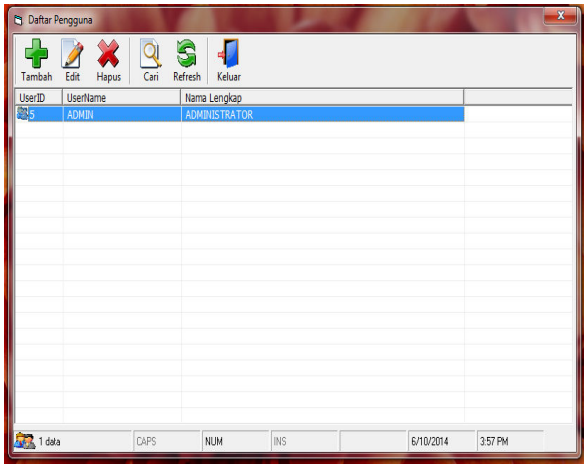
Gambar 8.7 Halaman Pilih Gambar Ekstrasi Pesan

8. Halaman Hasil Ekstrasi Pesan



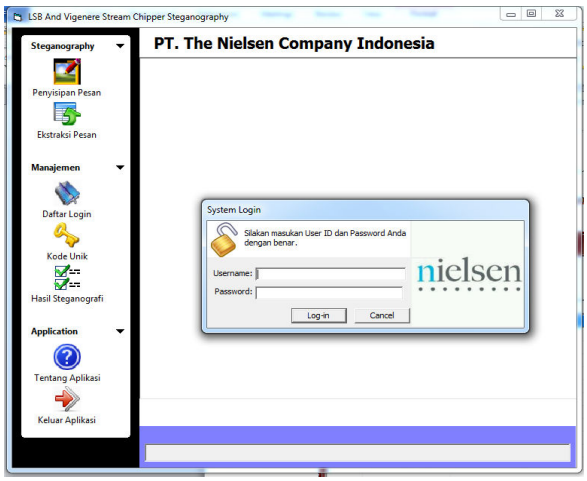
Gambar 8.8 Halaman Hasil Ekstrasi Pesan

9. Halaman Daftar Login



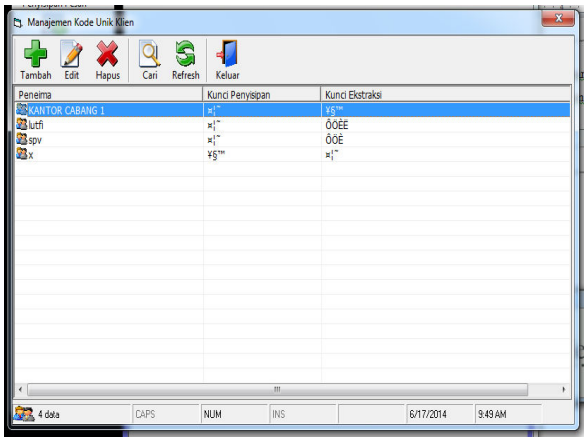
Gambar 8.9 Halaman Daftar Login

10. Halaman Login Kode Unik



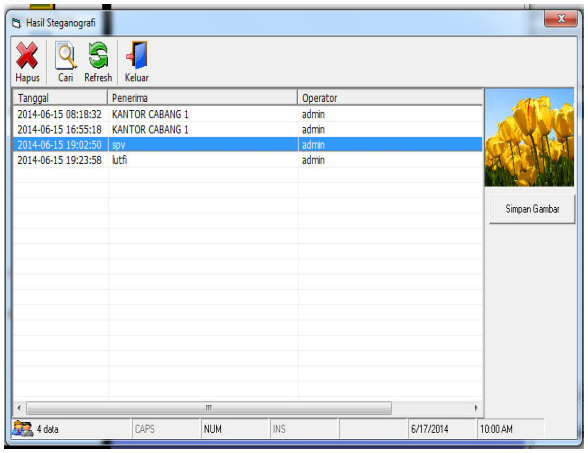
Gambar 8.10 Halaman Login Kode Unik

11. Halaman Kode Unik



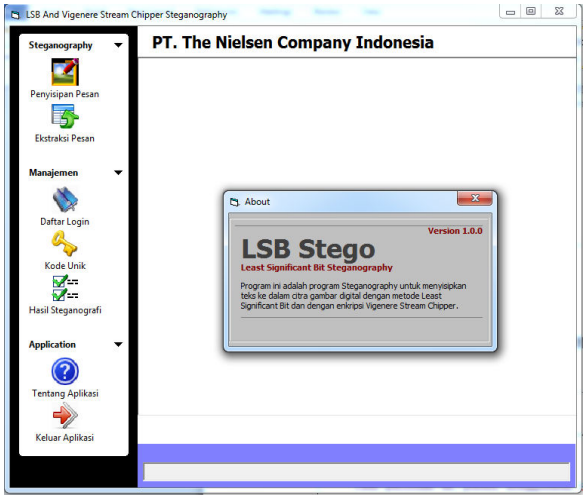
Gambar 8.11 Halaman Kode Unik

12. Halaman Hasil *Steganography*



Gambar 8.12 Halaman Hasil *Steganography*

13. Halaman Informasi *Steganography*



Gambar 8.13 Halaman Informasi *Steganography*

9. SIMPULAN, IMPLIKASI, DAN SARAN

9.1 Simpulan Tentang Produk

Setelah melakukan rancang bangun dan pengujian terhadap sistem pengamanan data di PT. The Nielsen Company Indonesia Semarang, maka dapat ditarik kesimpulan sebagai berikut :

a. Program sistem pengamanan data yang dikembangkan dengan menggunakan metode *least significant bit* dikatakan layak karena mengamnankan data yang dikirim sehingga data terjamin keamanannya.
b. Dalam sistem baru ini juga membantu dalam pengiriman data yang dilakukan auditor dilapangan sehingga akan menjadi lebih efektif dari sistem yang lama.

9.2 Keterbatasan Hasil Penelitian

Produk sistem pengamanan data yang penulis kembangkan ini menggunakan metode *Least Significant Bit* yang terbilang sudah lama, untuk enkripsi menggunakan metode *Vigenere Cipher*, sedangkan saat ini sudah dikembangkan metode baru yaitu *Anvanced Encryptionn Standard* (AES) yang menggunakan kunci simetris pada proses enkripsi dan dekripsi.

Hasil akhir dari proses penyisipan pesan rahasia ini tidak bisa otomatis terkirim karna aplikasi yang penulis buat ini bukan berorientasi pada situs web, hasil citra gambar akan dikirim tersendiri melalui jaringan internet.

9.3 Saran

Berdasarkan hasil analisis dan perancangan sistem pengamanan data dengan metode *least significant bit* ini, maka Penulis memberikan saran yaitu :

a. Saat uji ekstrasi setelah citra dilakukan distorsi brightness, pesan hasil ekstrasi tidak dapat dibaca. Untuk penelitian selanjutnya harus menemukan metode untuk memecahkan masalah tersebut.
b. Dalam sistem pengamanan data dengan metode *least significant bit* ini mungkin masih banyak kekurangan sehingga masih perlu pengembangan sistem yang lanjut

lagi agar dalam kinerja sistem bisa lebih membantu dalam kerja sehingga bisa lebih baik dan lebih sempurna.

c. Sistem pengamanan data dengan metode *least significant bit* masih bisa dikembangkan lagi, sehingga dalam pengerjaannya akan lebih mudah.

DAFTAR PUSTAKA

[1] Ariyus, Dony, 2008; "*Pengantar Ilmu Kriptografi: Teori, Analisis dan implementasi",* Yogyakarta: Penerbit Andi.

[2] Ariyus, Dony, 2009; "*Keamanan Multimedia, Penerapan Steganografi dalam Berbagai Bidang Multimedia",* Yogyakarta: Penerbit Andi.

[3] Ary Budi Warsito dkk, "Proteksi Keamanan Dokumen Sertifikat File Jpeg Pada Perguruan Tinggi Dengan Menngunakan *Steganography* Dan *Kriptografi*", Jurnal TELEMATIKA MKOM Vol.4 No.1, Maret 2012 ISSN: 2085-725X, Teknik Informatika STMIK Raharja, Tanggerang.

[4] Borg, Walter, R & Gall, Meredith, D.1983.*Educational research: An introduction (4th ed)*.NewYork:Longman Inc.

[5] M.A. Pakereng, Y.R. Beeh, and S. Endrawan, "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) Antara Waktu Proses dan Ukuran File Gambar," *Universitas Kristen Duta Wacana*.

[6] Madkom, dan Penerbit Andi, 2005; "Panduan Pemograman Dan Referensi Kamus Visual Basic 6.0.

[7] Rosa Hasan, "Implementasi Algorithma Enkripsi Vigenere Stream Chipper Pada Steganografi Citra Gambar Dengan Metode Least Significant Bit (LSB)," 2011.

[8] Sando Sembiring, "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File", Pelita Informatika Budi Darma, Volume : IV, Nomor: 2, Agustus 2013 ISSN : 2301-9425, Mahasiswa Program Studi Teknik Informatika STMIK Budi Darma Medan, Medan.

[9] Yogie Aditya, "Studi Pustaka Untuk Steganografi Dengan Beberapa Metode. Universitas Islam Indonesia," *Universitas Islam Indonesia*, 2010.