View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by E-Journal Universitas Asahan

IMPLEMENTASI METODE BIT MATCHING UNTUK KEAMANAN PESAN TEKS MENGGUNAKAN VISUAL BASIC. NET

Reno Supardi

Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu. 38228 Telp.(0736) 22027, 265957 Fax.(0736) 341139
renosupardi00@gmail.com

ABSTRAK

Teknologi informasi dan komunikasi telah berkembang pesat, memberikan pengaruh yang besar bagi kehidupan manusia. Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi. Penulis menggunakan steganografi dengan metode *Bit Matching* yang akan menyembunyikan informasi berupa teks kedalam media citra digital lain. Setelah dianalisis dan diimplementasikan menggunakan bahasa pemograman Visual Basic 2010 diperoleh bahwa teks yang disisipkan kedalam citra masih tampak seperti normal sehingga tidak menimbulkan kecurigaan bagi orang yang melihat. Ukuran daya tampung citra digital mempengaruhi berapa besar jumlah karakter pesan teks yang dapat disembunyikan. Semakin besar jumlah karakter pesan teks yang akan disembunyikan maka akan semakin besar ukuran dari citra digital tersebut. Diharapkan aplikasi steganografi ini dapat berguna untuk bidang pendidikan dan ilmu pengetahuan khususnya dalam penyembunyian pesan teks dan dapat dilanjutkan untuk penelitian yang akan datang.

Kata Kunci : Citra Digital, Bit Matching, Visual Basic 2010

ABSTRACT

Information and communication technology has developed rapidly, providing great influence for human life. The development of network technologies and the Internet allows anyone to exchange data, information, or messages to others without limitation of distance and time. Security and confidentiality are important aspects required in the process of exchanging messages/information. The author uses steganography Bit Matching method that will hide information in the form of text into another digital image media.

Having analyzed and implemented using the programming language Visual Basic 2010 obtained that the text is pasted into the image still looks like normal so as not to arouse suspicion for those who see. Size capacity digital image affects how large the number of characters of text messages that can be hidden. The greater the number of characters of text messages to be hidden the greater the size of the digital image. Steganography application is expected to be useful for education and science, especially in the concealment of text messages and can be continued for future research.

Keywords: Digital Image, Bit Matching, Visual Basic 2010

I.PENDAHULUAN

Kemajuan teknologi komputer berperan penting pada kehidupan manusia. Dari hal yang terkecil sampai berbagai hal yang sangat rumit sekalipun bisa dikerjakan menggunakan teknologi komputer. Saat ini keamanan data sangat penting terutama keamanan pada bidang komputer, hal ini dikarenakan pengguna komputer pada kehidupan setiap hari telah menjadi kebutuhan utama terutama dalam dunia bisnis, dimana kegiatan transaksi data ataupun penyimpanan data sangatlah penting untuk dijaga keamanannya.

Berbagai teknik telah banyak digunakan untuk melindungi data-data penting tersebut. Steganografi merupakan salah satu teknik yang digunakan dalam pengamanan informasi, yaitu dengan menyembunyikan informasi kedalam media digital dengan metode tertentu agar tidak nampak perbedaan secara visual antara file asli dengan file yang telah disisipi informasi, sehingga tidak diketahui oleh pihak lain. Dengan demikian pihak lain tidak menyadari bahwa terdapat informasi rahasia yang tertanam dalam media tersebut.

Salah satu metode dari teknik steganografi adalah *bit matching*, yaitu metode pencocokan bit yang memecahkan masalah menjadi beberapa bagian terkecil, kemudian secara rekursif menyelesaikan masalah-masalah kecil tersebut.

II.TINJAUAN PUSTAKA

A. Pengertian Steganografi

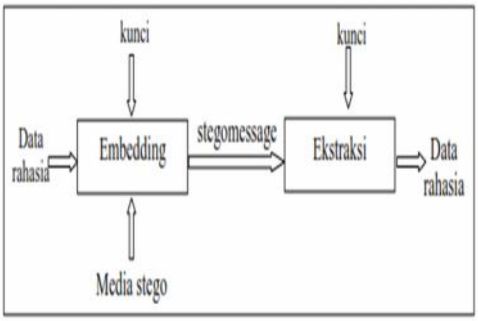
Menurut Sembiring (2013 : 3) Steganografi berasal dari kata Yunani yaitu *stegos* yang berarti penyamaran dan *graphia* yang berarti tulisan. Steganografi digunakan untuk menyembunyikan informasi rahasia kedalam suatu media sehingga keberadaan pesan tersebut tidak diketahui oleh orang lain.

Sedangkan menurut Purba dkk (2012 : 4) Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti “tulisan tertutup”. Pesannya terbuka, selalu terlihat tetapi tidak terdeteksi bahwa ada pesan rahasia. Popular untuk steganografi adalah *hidden in plan sight* yang artinya tersembunyi di depan mata.

Format yang biasa digunakan dengan menggunakan teknik steganografi diantaranya adalah :

a. Format *image* : bitmap (bmp), gif, Jpeg dan lain-lain
b. Format audio : wav, mp3, voc dan lain-lain
c. Format lain : teks file, html, pdf dan lain-lain

Prose penyembunyian data kedalam media citra disebut dengan penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi. Secara umum proses tersebut dapat diliha pada gambar 1.



Gambar 1. Proses Penyisipan Dan Ekstraksi Dalam Steganografi

Ada beberapa hal yang diperlukan untuk menyembunyikan pesan yaitu :

1. Algoritma penyisipan (*Embedding Algorithm)*
2. Fungsi detektor
3. *Carrier Document*
4. *Key*
5. *Secret Message / Plaintext*

B. Manfaat Steganografi

Steganografi adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. Steganografi juga dapat digunakan sebagai pengganti *hash.* Dan yang terutama, seperti disebutkan sebelumnya, steganografi dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Sayangnya, steganografi juga dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain, yang tidak berhak, tanpa ada yang curiga. Steganografi juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain.

C. Kriteria Steganografi Yang Baik

Menurut Munir (2004 : 37) Ada beberapa kriteria yang harus diperhatikan dalam steganografi, yaitu :

1. *Imperceptibility*,
2. *Fidelity*,
3. *Recovery*

D. Bit Matching (Pencocokan Bit)

Pencocokan bit pesan pada bit citra dilakukan dengan metode *divide and conquer* yang terdiri dari 3 proses yaitu *divide*, *conquer* dan *combine*. Artinya memecah masalah menjadi beberapa bagian kecil (*divide*), kemudian secara rekursif menyelesaikan setiap masalah-masalah kecil tersebut (*conquer*). Selanjutnya solusi dari setiap masalah kecil tersebut hasilnya digabung menjadi satu solusi utama (*combine*). (Challita & Farhat, 2011:201)

Adapun tahapan algoritma dari *Bit Matching* ini adalah sebagai berikut :

1. Mengkonversi pesan dan citra ke dalam bentuk biner
2. Mengambil nilai citra
3. Melakukan pencocokan pesan pada citra. Jika bit pesan terdapat pada citra, maka dilanjutkan dengan menyimpan posisi indeks bit. Penyimpanan indeks terdiri dari posisi indeks bit awal (*start*) dan posisi indeks akhir (*end*). Jika proses pencocokan tidak terjadi dilanjutkan ke proses 4
4. Membagi pesan menjadi 2 (dua) bagian sama panjang kiri (L[i]) dan kanan (R[i]).
5. Mengulangi langkah yang sama seperti pada langkah nomor 2, dengan L[i] dan R[i] sebagai masukan. Jika semua bit pesan terdapat pada citra, maka pencocokan selesai.
6. Menyimpan semua indeks bit hasil pencocokan

7. Keluaran berupa vektor yang memuat susunan indeks posisi bit
   Sebagai contoh, misalkan diketahui bit pesan dan bit citra sebagai berikut :
   Pesan (P) : 10110111
   Citra (C) : 100100011010110101010011
   Langkah pencocokan lokasi bit pesan pada citra :
   a. Mencocokan P = 10110111 dengan panjang 8 bit pada C : 100100011010110101010011
   b. Karena P tidak terdapat pada C maka P dipecah menjadi 2 bagian menjadi : L = 1011 dan R = 0111
      L[1] = 1011 diperoleh kesamaan bit pada lokasi indek ke 11 hingga 14, yaitu 10010001101101010101011
      R[1] = 0111, karena tidak ada yang cocok maka P_R dipecah menjadi 2 bagian sama yaitu L[2] = 01 dan R [2] =11
      L[2] = 01 diperoleh kesamaan bit pada lokasi indeks ke 3 hingga 4, yaitu 10010001101011010101011
      R[2] = 11 diperoleh kesamaan bit pada lokasi indeks ke 8 hingga 9, yaitu 10010001101011010101011
8. Menggabungkan semua solusi yang diperoleh yaitu 11 14 3 4 8 9

E. Citra Digital

Citra atau gambar dapat didefinisikan sebagai fungsi dua dimensi *f(x,y)*, dimana *x* dan *y* adalah koordinat bidang datar; dan harga fungsi *f* di setiap pasangan koordinat *(x,y)* disebut intensitas atau level keabuan (*grey level*) dari gambar di titik itu (Fajar, 2013 : 27). Apabila nilai *x,y* dan *f* secara keseluruhan berhingga (*finite*) dan bernilai diskrit maka dapat dikatakan bahwa citra tersebut adalah citra digital. Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek (Sutoyo,dkk, 2009 : 5). Citra sebagai keluaran suatu sistem perekam data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada media penyimpanan.

Sebuah citra digital dapat mewakili oleh sebuah matriks yang terdiri dari *M* kolom *N* baris, di mana perpotongan antara kolom dan baris disebut piksel (piksel = *picture element*), yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat *(x,y)* adalah *f(x,y)*, yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, citra digital dapat ditulis dalam bentuk matrik sebagai berikut :

Berdasarkan persamaan 1, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas *f(x,y)*, di mana harga *x* (baris) dan *y* (kolom) merupakan koordinat posisi dan *f(x,y)* adalah nilai fungsi pada setiap titik *(x,y)* yang menyatakan besar intensitas citra atau tingkat keabuan atau warna dari piksel di titik tersebut. Pada proses digitalisasi (sampling dan kuantitas) diperoleh besar baris *M* dan kolom *N* hingga citra membentuk matriks *M x N* dan jumlah tingkat keabuan piksel *G* (Sutoyo, dkk,2009 : 67).

Pada aplikasi pengolahan citra digital pada umumnya, citra digital dapat dibagi menjadi 3, *color image*, *balck and white image* dan *binary image.*

III.METODOLOGI PENELITIAN

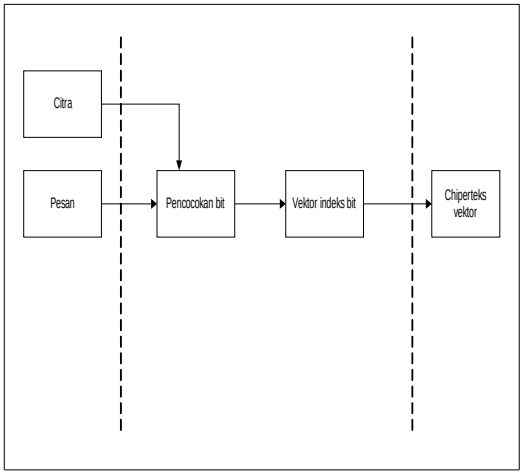
A. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode pengembangan sistem. Adapun langkah-langkah penelitian adalah :

1. Analisis sistem aplikasi steganografi menggunakan *algoritma bit matching*.
2. Implementasi dan pengujian sistem, yakni melakukan pengujian terhadap sistem yang telah dirancang.

B. Bagan Proses Embedding

Masukkan proses *embedding* berupa pesan, dan citra. Pada proses *embeeding* tahap yang dilakukan yaitu mencocokan bit pesan pada bit citra. Hasil pencocokan disimpan dalam vektor yang memuat indeks lokasi bit. Tahap selanjutnya yaitu melakukan proses enkripsi pada vektor tersebut. *Output* yang dihasilkan adalah chiperteks vektor yang telah terenkripsi. Proses *embedding* ditunjukkan pada Gambar 2.



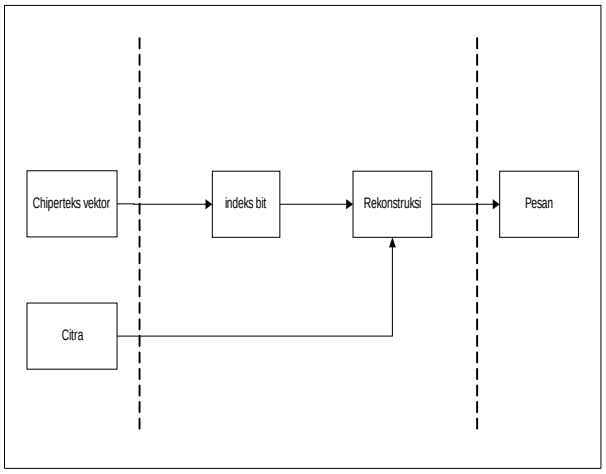
Gambar 2. Proses *Embedding*

Langkah-langkah *embedding* adalah sebagai berikut:

1. Memasukkan *input* berupa citra dan pesan
2. Mengkonversi pesan dan citra dalam bentuk biner.
3. Mencocokan bit pesan dengan bit citra. Posisi bit yang sama disimpan dalam vektor indeks bit.
4. Mengenkripsi vektor indeks bit.
5. Hasil keluaran berupa chiperteks. Chiperteks tersebut memuat vektor indeks bit yang telah terenkripsi.
6. Selesai.

C. Bagan Proses Ekstraksi

Masukkan proses ekstraksi berupa chiperteks vektor, dan citra. Proses ekstraksi meliputi dekripsi vektor dan dilanjutkan rekonstruksi . Hasil keluaran rekonstruksi berupa pesan semula. Bagan Proses ekstraksi ditunjukkan pada gambar 3.



Gambar 3. Proses Rekonstruksi

Langkah-langkah proses ekstraksi adalah sebagai berikut:

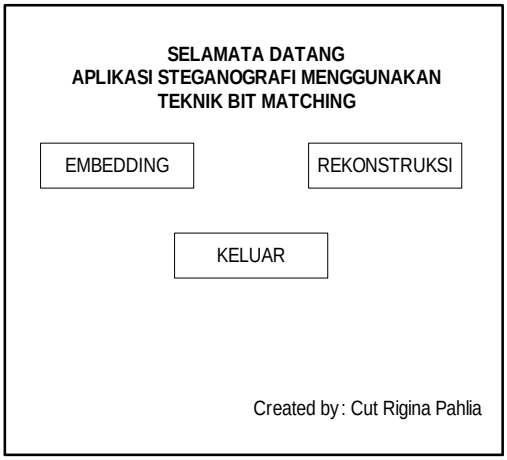
1. Memasukkan *input* chiperteks vektor, dan citra.
2. Mendekripsi vektor dengan kunci, hasil dekripsi berupa indeks bit.
3. Melakukan rekonstruksi pesan dengan mencocokan bit citra berdasar vektor indeks bit.
4. Hasil *output* berupa pesan.
5. Selesai.

D. Perancangan *Interface* Aplikasi

Antarmuka merupakan halaman atau jendela (*form/windows*) tempat *user* berinteraksi dengan aplikasi. Perancangan antarmuka bertujuan untuk memberikan gambaran desain dan tata letak menu yang akan digunakan. Perancangan antarmuka pada penelitian ini terdiri dari halaman awal, *embedding*, ekstraksi, dan *about*.

1. Implementasi Halaman awal

Halaman awal merupakan form yang pertama kali muncul ketika aplikasi dijalankan, seperti yang tampak pada gambar 4.



Gambar 4 Rancangan Tampilan Awal

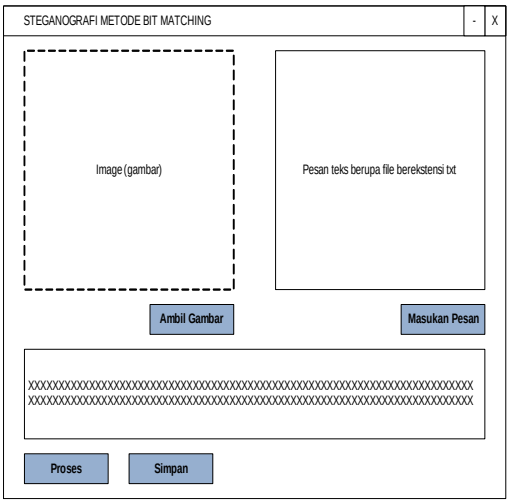
Keterangan :

Pada form halaman awan terdapat tombol embedding, rekonstruksi dan keluar.

a. Tombol *embedding* berfungsi untuk masuk pada form *embedding*,
b. Tombol rekonstruksi untuk masuk pada form rekonstruksi
c. Tombol keluar berfungsi untuk keluar dari aplikasi.

2. Implementasi Form Embedding

Pada *form embedding* terdapat 3 masukan, yaitu gambar dan *file*. Perancangan *form embedding* dapat dilihat pada gambar 5.



Gambar 5. Perancangan *Form Embedding*

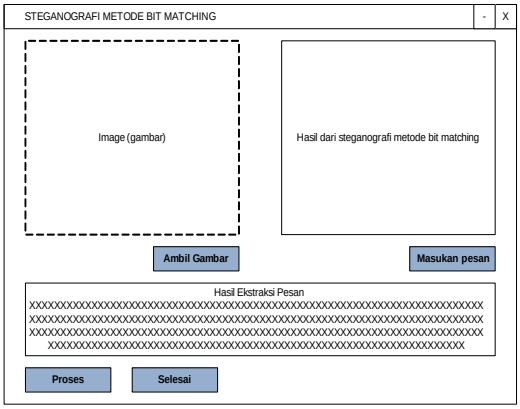
Keterangan :

Pada perancangan *form embedding* terdapat beberapa tombol yaitu :

a. tombol ambil gambar yang berfungsi untuk mengambil gambar baik yang terdapat pada hardisk ataupun pada media lain seperti flashdisk, disc atau yang lainnya.
b. Tombol ambil pesan, pesan yang dimaksud disini adalah file yang berekstensi *.txt seperti file *notepad.*
c. Untuk tombol password berfungsi untuk mengunci file, dan hasil output dari file txt tersebut berupa angka.

3. Perancangan Form Ekstraksi

Pada *form* ekstraksi terdapat 2 masukan, yaitu gambar dan *file*. Perancangan *form* ekstraksi ditunjukkan pada gambar 6.



Gambar 6. Perancangan *Form* Ekstraksi

Keterangan :

Form ekstrasi ini berguna untuk menampilkan pesan yang telah disisipkan, pada form ini juga terdapat beberapa tombol antara lain :

a. Tombol ambil gambar yang berfungsi untuk menampilkan gambar yang telah diproses pada form embedding,
b. Tombol masukan pesan berfungsi untuk memasukkan pesan.
c. Tombol proses adalah untuk menampilkan pesan yang telah terenksipsi dengan algoritma *bit matching* yang outputnya berupa angka. Setelah password berhasil dimasukan

maka akan tampil pesan asli pada *textbox* berupa hasil ekstraksi pesan.

d. Tombol selesai berfungsi untuk keluar dari aplikasi.

a. Perancangan Pengujian

Pengujian dilakukan dengan cara memberikan masukan (*input)* berupa pesan, citra, dan kunci. Kemudian dilakukan proses *embedding*. Keluaran *embedding* berupa chiperteks vektor yang memuat posisi indeks bit. Keluaran hasil *embedding* ini (vektor) selanjutnya menjadi masukan untuk proses ekstraksi. Proses ekstraksi diuji untuk memastikan pesan dapat dikembalikan seperti semula.

IV.HASIL DAN PEMBAHASAN

A. HASIL

Aplikasi steganografi metode *bit matching* telah dibuat sesuai dengan rancangan pada Bab III. Sedangkan untuk *source code* pembuatan aplikasi steganografi metode *bit matching* ini dibuat dengan menggunakan bahasa pemrograman Visual Basic 2010. Aplikasi ini dapat di aktifkan atau dijalankan dengan meng-klik *shortcut* yang ada pada dekstop seperti gambar 7.

Gambar 7.Tampilan Dekstop Aplikasi Steganografi *Bit Matching*

B. *Form Embedding*

Tampilan awal *form embedding* merupakan tampilan untuk melakukan proses pengamanan pesan teks dengan menggunakan media citra digital. Tampilan awal *form embedding* dapat dilihat pada gambar 8.

Gambar 8. Tampilan Awal *Form Embedding*

Keterangan :

a. Untuk pemilihan *file* citra yang hendak digunakan dengan memilih tombol ambil gambar.

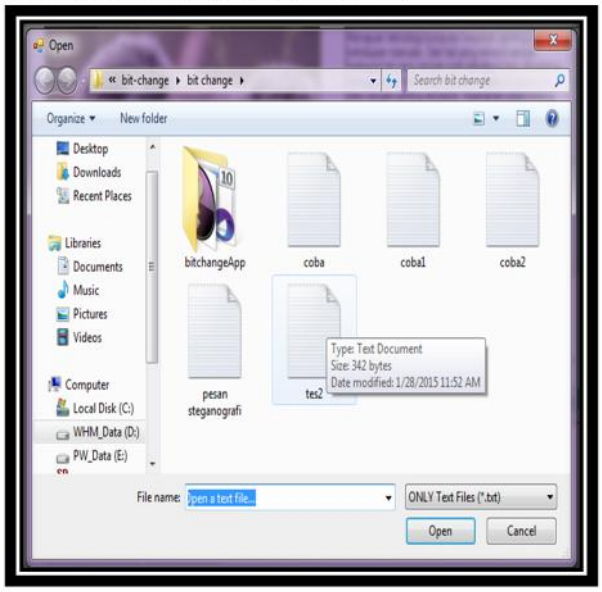
Tampilan untuk pemilihan *file* citra merupakan tampilan kotak dialog yang muncul jika dilakukan pemilihan tombol ambil citra berguna untuk melakukan pengambilan *file* citra dari komputer. Tampilan kotak dialog pemilihan *file* citra dapat dilihat pada gambar 9.

Gambar 9. Tampilan Kotak Dialog Pemilihan *file* Citra

Setelah kotak dialog mucul, maka lakukan pemilihan *file* citra :

b. Untuk memasukkan file pesan teks yang hendak digunakan dengan memilih tombol ambil pesan.

Tampilan untuk pemilihan *file* pesan teks merupakan tampilan kotak dialog yang muncul jika dilakukan pemilihan tombol ambil pesan berguna untuk melakukan pengambilan *file* pesan teks dari komputer. Tampilan kotak dialog pemilihan *file* pesan teks dapat dilihat pada gambar 10.



Gambar 10. Tampilan Kotak Dialog *File* Pesan Teks

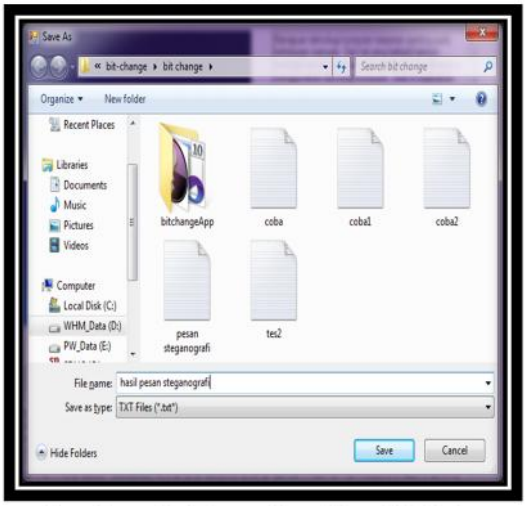
c. Tombol proses berfungsi untuk melakukan proses pengamanan pesan teks.

Setelah dilakukan pemilihan *file* citra dan *file* pesan teks, maka selanjutnya melakukan proses pengamanan pesan teks dengan menggunakan metode *bit matching* dengan cara meng-klik tombol proses, hasil setelah tombol pesan diklik dapat dilihat pada gambar 11.

Gambar 11. Tampilan Hasil Keamanan Pesan Teks

d. Tombol simpan berfungsi untuk menyimpan hasil pesan teks.

Setelah proses pengamanan pesan teks selesai, maka langkah selanjutnya adalah menyimpan pesan teks dengan cara meng-klik tombol simpan maka akan tampil kotak dialog *save* seperti gambar 12.

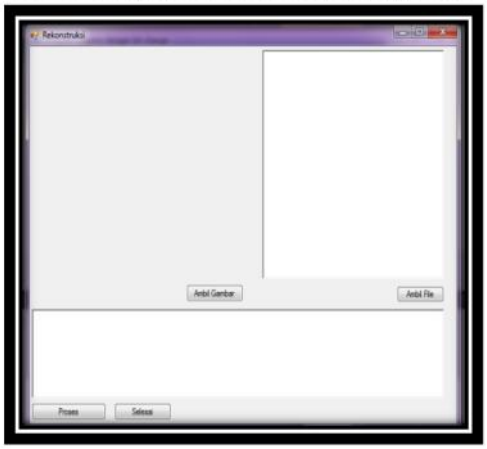


Gambar 12. Tampilan Kotak Dialog Simpan Pesan Teks

Hasil dari pesan teks tersebut adalah berbentuk angka-angka yang tidak bisa dibaca atau dengan kata lain pesan tersebut telah menjadi pesan yang telah dirahasiakan isinya.

C. *Form* Rekonstruksi

Form rekonstruksi ini berguna untuk membuka atau membaca hasil pesan teks yang telah diubah menjadi angka-angka. Pada *form* rekonstruksi ini terdapat tombol ambil gambar, tombol ambil *file*, tombol proses dan tombol selesai,seperti terlihat pada gambar 13.



Gambar 13.Tampilan *Form* Rekonstruksi

Keterangan :

a. Tombol ambil gambar

Tombol ambil gambar berfungsi untuk mengambil *file* gambar yang telah digunakan pada *form embedding* dikarenakan hanya dengan menggunakan *file* gambar *yang* sama yang bisa untuk membuka atau membaca *file* pesan teks, setelah tombol ambil gambar di klik maka akan tampil kotak dialog seperti gambar 14.

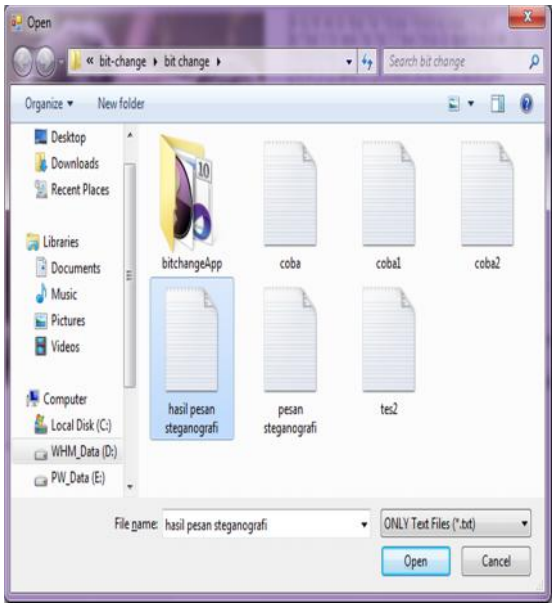
Gambar 14. Kotak Dialog *File* Gambar

Setelah *file* gambar dipilih maka *form* rekonstruksi akan terlihat seperti gambar 15.

Gambar 15. Tampilan *File* Gambar Pada *Form* Rekonstruksi

b. Tombol ambil *file*

Tombol ambil *file* berfungsi untuk mengambil *file* pesan teks yang telah disimpan, setelah tombol ambil *file* di klik maka akan tampil kotak dialog seperti gambar 16



Gambar 16. Kotak Dialog *File* Pesan Teks

Setelah *file* gambar dipilih maka *form* rekonstruksi akan terlihat seperti gambar 17.

Gambar 17.*File* Pesan Teks Pada *Form* Rekonstruksi

c. Tombol proses

Tombol proses berfungsi untuk memproses *file* pesan teks yang berupa angka-angka agar kembali menjadi pesan teks yang dapat dimengerti dan dibaca, seperti yang terlihat pada gambar 17.

d. Tombol selesai

Tombol selesai berfungsi untuk menutup *form* rekonstruksi

d. Pengujian Sistem

Pengujian dilakukan dengan menggunakan *file* yang berekstensi *.txt (*notepad*) dengan menggunakan citra gambar yang berbeda untuk mengetahui hasil dari apakah akan menghasilkan *file* yang terenkripsi yang sama atau tidak. Dari hasil pengujian menunjukan bahwa *file* *.txt (*notepad*) yang menggunakan citra gambar yang berbeda akan menghasilkan *file* yang terenkripsi yang beda juga.

Tabel hasil pengujian 1

Citra input	File input	Hasil	Keterangan
Citrabmp1.bmp	Uji1	HasilBMP1	Berhasil
Citragif1.gif	Uji1	HasilGIF1	Berhasil
Citratif1.tif	Uji1	HasilTIF1	berhasil
Image(4).jpeg	Uji1	hasilJPEG	Berhasil

Tabel pengujian 2

Citra input	File input	Hasil	Keterangan
Citrabmp1.bmp	HasilTIF1	Error	Gagal
Citragif1.gif	hasilJPEG	Error	Gagal
Citratif1.tif	HasilBMP1	Error	Gagal
Image(4).jpeg	HasilGIF1	Error	Gagal

Pada pengujian ke 3 (tiga) ini dilakukan dengan file uji2 yang kemudian menghasilkan file tesuji2, file tesuji2 ini yang akan dibuktikan apakah dengan ekstensi citra yang berbeda dapat, berikut

Tabel pengujian 3

Citra input	File hasil	Keterangan
Citrabmp1.bmp	Tesuji2	Berhasil
Citragif1.gif	Tesuji2	Gagal / error
Citratif1.tif	Tesuji2	Berhasil
Image2.jpeg	Tesuji2	berhasil

V.PENUTUP

A. Kesimpulan

Setelah melakukan studi literatur, perancangan, analisis, implementasi dan pengujian sistem untuk *steganografi* citra digital untuk pengamanan pesan teks dengan menggunakan metode *Bit Matching* maka dapat disimpulkan :

1. Pengamanan pesan teks dengan *steganografi* dapat diimplementasikan menggunakan metode *Bit Matching*
2. Tipe file atau ektensi citra digital (JPEG,GIF, TIF, BMP) sangat mempengaruhi hasil dari pesan teks yang disembunyikan, begitupun pada saat pesan akan dibuka kembali harus dengan menggunakan citra input yang sama pada saat pesan disembunyikan.
3. Perubahan tidak terjadi pada citra asli tapi terjadi pada pesan teks hal ini dikarenakan metode *bit matching* mencocokan atau mencari nilai bit yang mempunyai kesamaan antara citra dan pesan teks.

B. Saran

Untuk pengembangan lebih lanjut sistem *steganografi* dengan menggunakan metode *Bit Matching* ini, maka dapat diberikan beberapa saran sebagai berikut :

1. Menyediakan suatu fitur tambahan dimana *file image* hasil *steganografi* dapat dikirimkan kepada seseorang secara langsung salah satunya melalui *e-mail.*
2. Dilakukan penelitian lebih lanjut tentang *steganografi* yaitu bukan hanya menyembunyikan pesan teks kedalam citra tapi juga mampu menyembunyikan citra

digital ke dalam citra digital dengan metode *Bit Matching*.

DAFTAR PUSTAKA

[1]. Ariyus, D. 2009. *Keamanan Multimedia*. Yogyakarta: Andi Offset.

[2]. Challita, K., & Farhat, H. (2011). Combining Steganography And Cryptography : New Direction. *Computer Architectures* , 199-208.

[3]. Hermawati, F. A. (2013). *Pengolahan Cita Digital Konsep dan Teori.* Yogyakarta: Andi Offset.

[4]. Munir, R. 2006. *Kriptografi*. Bandung: Informatika.

[5]. Purba, J. V., Situmorang, M., & Arisandi, D. (2012). Implementasi Steganografi Pesan Teks Kedalam File Sound (.Wav) Dengan Modifikasi Jarak Pada Algoritma LSB. *Teknologi Informasi , I,* 1-6.

[6]. Putra, D. 2010. Pengolahan Citra Digital, Yogyakarta: Penerbit Andi

[7]. Sembiring, S. (2013). Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File. *Teknologi Informatika* , 1-7.

[8]. Sutarman, 2009. *Pengantar Teknologi Informasi*, Yogyakarta, Bumi Aksara

[9]. Setiawan, 2004. Perancanaan dan Pembangunan Ekonomi, Bandung, Yudistira

[10]. Usman, H,P, 2002. Implementasi Perancangan Teknologi, Yogyakarta, Graha Ilmu

[11]. Yakub, 2012. *Pengantar Sistem Informasi*, Yogyakarta, Graha Ilmu.