MENJAGA KEAMANAN BASIS DATA
DENGAN MENGGUNAKAN METODE STEGANOGRAPHY

Oleh: Edson Yahuda Putra

Abstrak

Pada saat terjadi pengiriman data dari suatu tempat ke tempat lain, selalu timbul rasa was-was. Apakah data yan dikirimkan itu sampai ke tujuan apa tidak? Apa data yang dikirimkan itu tidak dibaca orang? Apa data yang dikirimkan itu tidak dimodifikasi oleh orang lain?

Metode steganography adalah salah satu metode untuk memberikan keamanan data pada saat dikirimkan. Metode ini bekerja dengan meng-enkripsi data asli lalu dilakukan men-steganography baru data dikirimkan. Setelah data tersebut diterima oleh si penerima data tersebut di-desteganograpy dan terakhir data tersebut di-dekripsi. Hasil pen-dekripsi-an akan menjadi data yang asli (plain-text).

Keywords: plan text, chipper text, steganography, enkripsi, dekripsi

1. Pendahuluan

Keamanan data adalah masalah yang sangat penting dalam pengiriman data. Data yang dikirimkan dari satu tempat ke tempat lain harus terhindar dari beberapa gangguan seperti gangguan yang tidak disengaja seperti noise, desau, splatter, dan gangguan yang tidak disengaja seperti attack (serangan). Beberapa macam serangan terhadap pengiriman data adalah data tersebut juga bisa dibaca oleh orang lain (Interception), data dibaca oleh orang lain dan dilakukan perubahan baru dikirim ke tujuan (Modification) (Stalling, 2003)

Gangguan komunikasi data yang disengaja bisa dicegah, salah satunya yaitu menggunakan metode steganography. Metode ini dilakukan setelah data di-enkripsi baru data dibungkus dengan media cover dengan format gambar (.bmp) proses pembuatan cover ini disebut dengan steganography. Dengan steganography data akan aman setidaknya data walaupun sedang diserang, data tersebut tudak tidak akan bisa dibaca oleh si penyerangnya.

Metode steganography ini diaplikasikan pada database identitas seseorang. Data seseorang akan aman apabila sedang dikirimkan dari satu tempat ke tempat lain. Kata steganografi (steganography) berasal dari bahasa Yunani steganos, yang artinya "tersebunyi" atau terselubung", dan graphien, "menulis" sehingga kurang lebih artinya "menulis (tulisan) terselubung". Teknik ini meliputi banyak sekali metode komunikasi untuk menyembuntikan pesan rahasia. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersebunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerangan potensial, sebagai contoh sebuah gambar yang telihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada crypthography) dan pesan untuk disembunyikan.

Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

2. Batasan Sistem

Untuk mendukung penelitian, program yang dibuat diharapkan mampu menunjukkan bagaimana data-data identitas seseorang dapat disimpan ke dalam basis data multimedia melalui proses steganografi. Untuk itu sistem akan dibatasi sebagai berikut:

1. Sistem hanya dirancang untuk mencatat data-data identitas tertentu dari seseorang, seperti nama, tempat dan tanggak lahir, pekerjaan, golongan darah, alamat dan lain-lain
2. Untuk melengkapi data alamat dan untuk menunjukkan bahwa tabel memiliki relasi maka data-data tersebut akan didukung dengan tabel data desa, kecamatan, kabupaten dan propinsi.
3. *Media cover* yang digunakan untuk menyembunyikan sata dapat dipilih yaitu *file* gambar (BMP).
4. Metode enkripsi yang digunakan untuk mengenkripsi data sebelum disteganografikan yaitu dengan menggunakan metode *VIGENERE CIPHER*, dimana kunci yang dipakai untuk melakukan proses enkripsi diinputkan oleh masing-masing user.

3. Metodologi

Penelitian ini dengan membuah sebuah program aplikasi yang mampu menyimpan data-data umuk tentang seseorang, dimana data-data tersebut akan disimpan dengan teknik steganografi pada sebuah tabel basis data yang hanya terdoro dari *field* ID, dan *field* Gambar. Data-data umum yang disimpan dengan teknik steganografi pada tabel basis data juga akan didukung oleh tabel-tabel basis data yang lainnya yang berelasi untuk menunjukkan bahwa *field-field* tabel yang disteganografi juga masih dapat direlasikan.

Objek penelitian akan difokuskan pada tabel basis data yang disteganografikan dengan tidak mengsampingkan tujuan pokok pembuatan sebuah tabel basis data dan relasinya, sedangkan *file* yang dipakai untuk memproses steganografi adalah *file* BMP (gambar digital).

Sistem yang akan dibuat secara umum hanya digunakan untuk membuktikan bahwa teknik steganografi pada tabel basis data multimedia dapat dilakukan. Sistem terdiri dari sebuah form yang berfungsi untuk mencatat data perinadi seseorang dan menyimpanannya ke dalam tabel basis data multimedia.

Sebelum data-data asli disimpan ke dalam tabel basis data multimedia, data tersebut terlebih dahulu digabungkan menjadi sebuah barisan data string. (data text) dengan masing-masing *field* data dipisahkan oleh tanda "|", setelah semua data digabungkan, data tersebut kemudian dienkripsi dan disteganografikan pada *file* multimedia yang dipilih untuk menyembunyikan data-data asli tersebut. *File* multimedia yang dipilih yaitu *file* gambar digital (*file* BMP-24 bit).

Untuk menampilkan kembali data asli, maka data diekstrak terlebih dahulu dari tabel basis data multimedia. Data-data asli yang sebelumnya disembunyikan di dalam *media cover* dikeluarkan dimana data yang dihasilkan akan berupa barisan datastring yang masih dalam keadaan terenkripsi. Setelah data diekstrak kemudian barisan string terenkripsi yang dihasilkan dikembalikan ke dalam bentuk semula dengan proses dekripsi.

Proses dekripsi selesai, data menjadi bentuk text biasa yang di dalamnya terdapat data-data asli yang disimpan dengan masing-masing *field* dipisahkan dengan penanda "|", dari data-data tersebut kemudian dilakukan pemisahan/pencacahan data sehingga data akan dapat dikembalikan ke dalam *field-field* tabel basis data yang bersuaian.

Data-data pribadi yang akan dicatat terdiri dari data ID (Contoh: no. KTP), Nama, Alamat, Tempat Lahir, Tanggal Lahir), pekerjaan dan keterangan (di isi dengan data-data lain yang terkait dengan keterangan seseorang).

Setelah digabungkan termasuk dengan penanda khusus ("|" untuk pemisah data), password data, panjang masing-masing data, dan penanda akhir "##", data akan menjadi seperti berikut:

Password_data|Hasil_enkripsi_data(|2040|30|10|1|10|2|25|300|45|10|ID_penduduk|nama|alamat|tempat_lahir|Tanggal LAhir|))|##

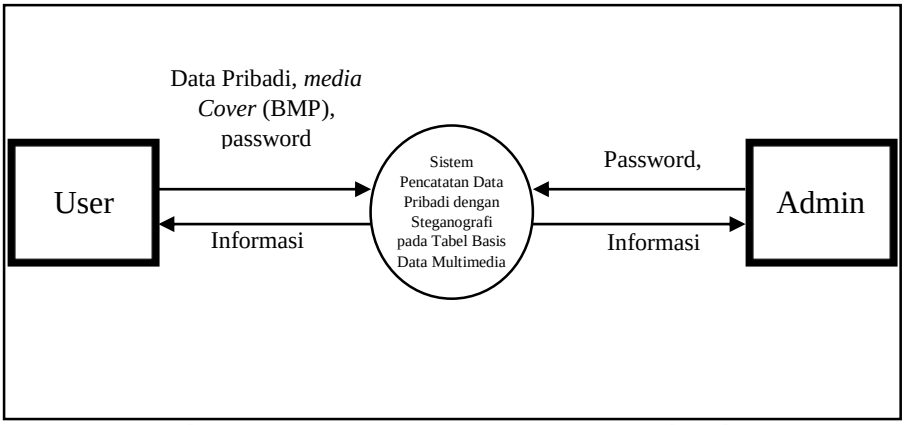
Data-data ini kemudian akan disteganografikan ke *media cover* atau akan diolah oleh sistem yang dibuat.

4. Analisa

4.1 Data Flow Diagram (DFD) Sistem

Perencangan sistem mengunakan DFD berguna untuk mengatahui kebutuhan sistem dan untuk memberikan gambaran yang jelas dan rancang bangun yang lengkap kepada programmer untuk membuat sistem. DFD akan menunjukkan dari mana asal data, kemana tujuan data, dimana data disimpan, proses apa yang dilakukan terhadap suatu data, apa yang dihasilkan dari pengolahan data dan proses-proses yang lainnya.

DFD sistem yang dibuat:



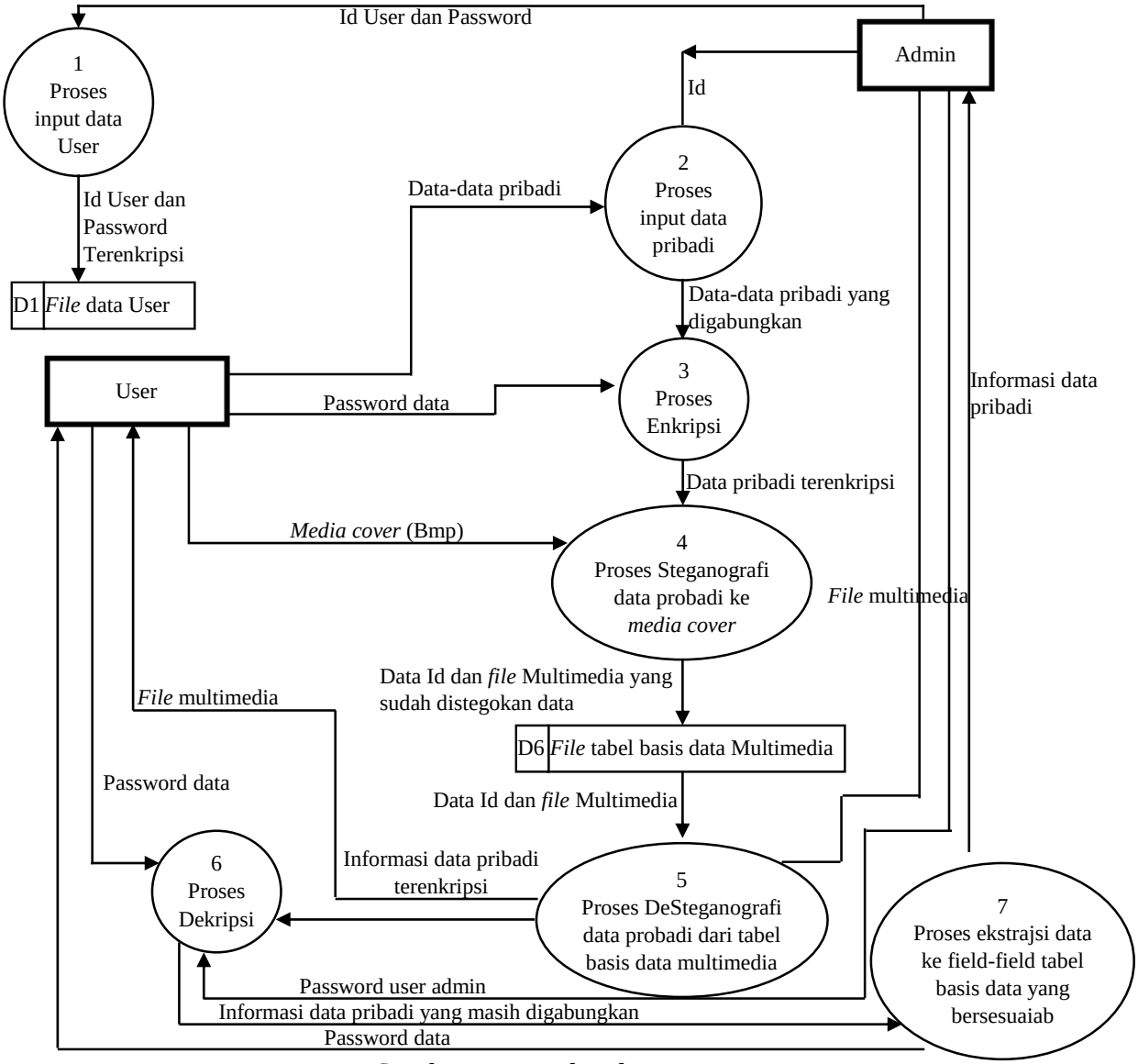
Gambar 1. Diagram *context* system (DFD level 0)

DFD Level 0 (Diagram *context*) dari sistem menunjukkan gambaran umum dari sistem dimana terdapat dua kelompok pemakai sistem yaitu Admin dan User yang masing-masing memiliki hak akses dan tugas yang berbeda.

4.2 DFD Level 1

DFD level I sistem menunjukkan proses-proses yang bekerja pada sistem secara lebih detail termasuk aliran data dan *file-file* yang disimpan oleh sistem.

Pada DFD level I ini dapat dilihat bahwa sistem akan melibatkan 2 buah *file* yang disimpan, yaitu *file* data user, dan *file* tabel data multimedia. Secara umum sistem akan melibatkan 7 (tujuh) buah proses utama yaitu proses input data user, proses input data pribadi, proses enkripsi, proses steganografi, proses desteganografi, proses deskripsi, dan proses ekstraksi.

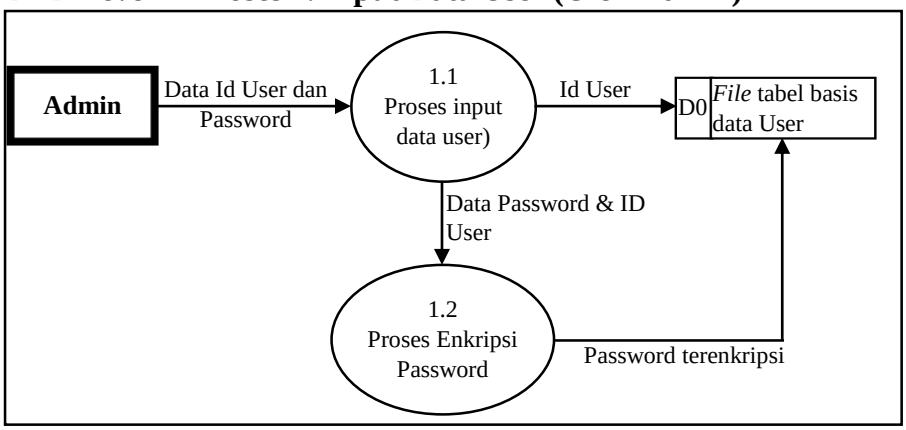


Gambar 2. DFD level 1 sistem

4.3 DFD Level II

DFD level II menunjukkan proses yang lebih detail dari beberapa proses pada DFD level I yang masu besifat umum. Proses-proses pada DFD level I yang masih memiliki sub proses di dalamnya dan akan dirinci dalam DFD level II ini diantaranya yaitu proses no. 1 (Proses input data user) dan proses no. 4 (proses Steganografi data pribadi ke *media cover*) dan proses no. 5 (Proses DeSteganografi data pribadi dari tabel basis data multimedia).

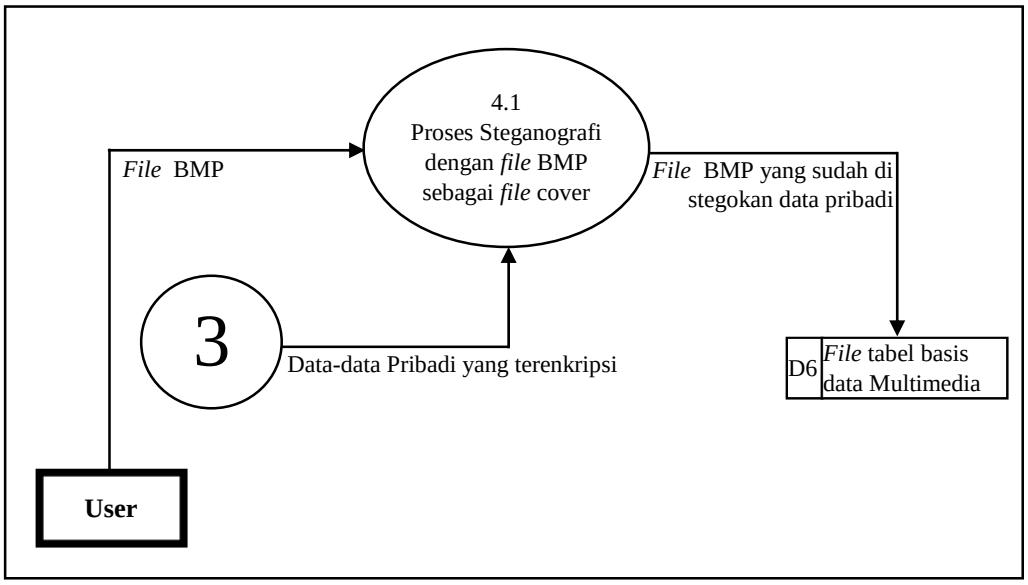
DFD Level II Proses 1. Input Data User (Oleh Admin)



Gambar 3. DFD level II Proses 1. Input Data User

Proses input data user dilakukan oleh Admin, data-data yang diinputkan adalah data ID dan data Password. Setelah data diinputkan, password akan dienkripsi dengan metode enkripsi *vigenere* dimana yang dipakai sebagai kunci untuk mengekripsi adalah nama User (ID User). Data-data tersebut kemudian disimpan ke tabel basis data. Data user berfungsi untuk menentukan hak akses ke sistem, seluruh user yang tercatat memiliki hak yang sama dengan admin.

DFD level II Proses 4. Steganografi Data Pribadi ke *Media cover*

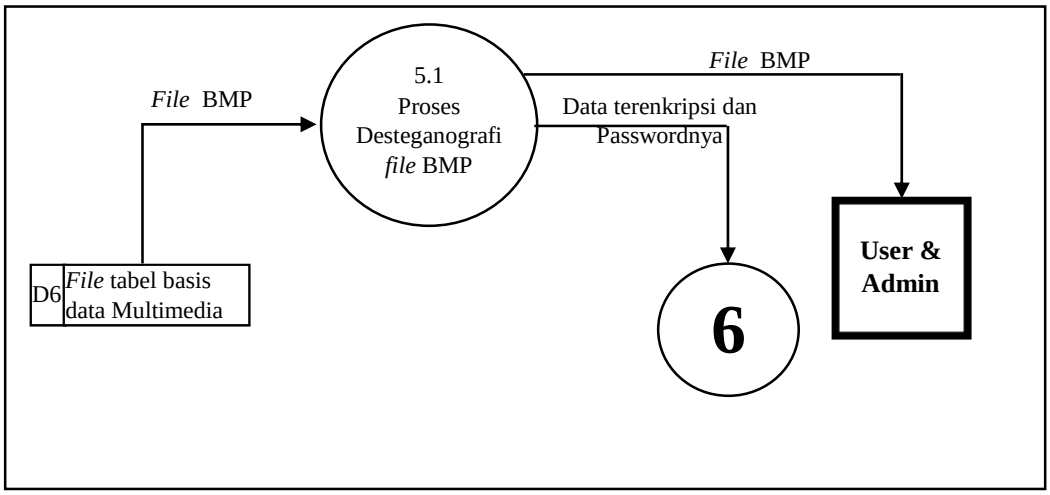


Gambar 4. DFD level II Proses 4. Steganografi Data Pribadi ke *Media cover*

Proses steganografi merupakan inti dari pembahasan penelitian, data-data yang sudah terenkripsi kemudian disteganografikan ke *media cover*. *User* yang akan menyimpan data pribadinya ke dalam sistem harus menginputkan *file* multimedia yang akan dipakai sebagai *media cover*. Proses steganografi dalam sistem ada dua yaitu steganografi dengan *file* BMP sebagai *media cover*.

Setelah proses steganografi, *file* multimedia yang sudah disteganografikan data akan disimpan ke dalam *file* tabel basis data multimedia bersama dengan ID data pribadi tersebut.

DFD level II Proses 5. DeSteganografi Data Pribadi dati Tabel Basis Data Multimedia



Gambar 5. DFD level II Proses 5. DeSteganografi Data Pribadi dari Tabel Basis Data Multimedia

Proses desraganografi adalah kebalikan dari proses steganografi. *File* multimedia dari tabel basis data multimedia akan dikeluarkan dari tabel, jika *file* multimedia tersebut adalah *file* BMP maka akan dilakukan proses desteganografi BMP, Dari proses destaganorafi, *file* BMP yang dihasilkan akan diteruskan sebagai informasi ke *user*, sedangkan data teks hasil desteganografi yang masih terenkripsi akan dilanjutkan ke proses deskripsi (proses nomor 7)

Daru proses desteganografi, data teks yang dihasilkan yang menrupakan *field-field* data pribadi yang digabungkan dan terenkripsi, kemudian data tersebut didekripsikan untuk menghasilkan data yang sebenarnya. Pada proses ini *user* menginputkan data password yang akan dibanfingkan dengan password data, jika password data benar maka data akan dideskripsikan, sedangkan jika data salah maka data tidak akan didekripsikan. Data hasil dekripsi ini (masih berupa data teks yang merupakan gabungan *field-field* data pribadi) kemudian akan diteruskan ke proses ekstraksi untuk mengembalikan *field-field* data kebentuk semua.

Proses ekstraksi merupakan bagian akhir dari proses pengembalian data menjadi informasi. Dari data teks hasil dekripso dimana data ini adalah gabungan dari *field-field* data, kemudian data dikembalikan ke dalam bentuk semula.

Misalnya data teks yang dihasilkan adalah “Password_data|4|4|24|10|10|ID01|Budi|Jln Nagamuda, 293 Gowok|Yogyakarta|12-12-1980|##” setelah diekstrak, data akan menjadi:

ID : ID01,
Nama : Budi,
Alamat : Jln. Nagamuda, 293 Gowok,
Tempat Lahir : Yogyakarta
Tanggal Lahir : 12-12-1980

KESIMPULAN

Pengirim data tidak merasa was-was lagi oleh karena data yang dikirimkan akan sampai ditujuan dengan aman. Pada saat ada serangan dari luar dan mendapatkan data tersebut, maka penyerang akan mendapati sebuah gambar. Yang sebenarnya dalam gambar tersebut apabila diurai akan memberikan sebuah informasi tentang data seseorang.

Terdapat beberapa kelebihan atau keuntungan yang didapat dengan melakukan proses steganografi pada sebuah tabel basis data multimedia, diantaranya:

1. Pada umumnya, proses steganografi dapat dilakukan hampir pada semua file digital yang memiliki bit-bit data yang redundan,
2. Proses steganografi pada sebuah tabel basis data multimedia dapat dikombunasikan dengan sebuah metode enkripsi untuk lebih menjamin keamana data.
3. Selain untuk kepentingan pengamanan data, proses steganografi juga dapat mengurangi (mereduksi) jumlah kolom pada sebuah tabel basis data, meskipun pada saat pengekstrakan data diperlukan sebuah tabel *temporary* untuk menampung kembali data pada *field-field* yang sebenarnya.

Selain sisi positif penerapan steganografi pada tabel basis data multimedia, metode ini juga masih memiliki banyak kelemahan, diantaranya:

1. Proses steganografi menjadi tidak efisien jika data yang disembunyikan berukuran jauh lebih kecil dari ruang yang disediakan oleh *medi over* untuk menyembunyikan data,
2. Ukuran besar *file* tabel basis data hasil steganografi akan menjadi lebih besar karena harus menyertakan sebuah *file* multimedia didalamya. Jika dibandingkan dengan ukuran *file* tabel basis data yang biasa tanpa *file* multimedia, maka hal ini menjadi tidak efisien, tetapi jika tabel basis data harus memuat sebua *file* multimedia (contohnya foto digital seseorang) maka penerapan steganografi menjadi lebih menguntungkan dari sisi ukuran besar *file* tabel basis data.
3. Kerumitan dalam melakukan proses penyimpanan data adalah kelemahan yang nyata dari proses steganografi pada tabel basis data multimedia ini jika dibandingkan dengan penyimpanan data pada tabel basis data biasa atau dengan metode enkripsi saja. Sebelum proses penyimpanan, data harus melalui proses-proses tertentu yang panjang dan rumit demikian pula saat akan mengolah data, diperlukan proses untuk mengekstrak data terlebih dahulu,

Saran-saran yang dapat dilakukan untuk penelitian sejenis yaitu:

1. Peneltian dapat dilakukan pada tabel basis data muultimedia dengan *field-field file* multimedia yang lebih beragam (tidak hanya pada file BMP saja),l
2. Untuk mendapatkan hasil yang lebih baik, penerapan steganografi disarankan hanya dilakukan pada tabel basis data yang harus dan hanya memuat file citra digital saja (file BMP) seperti pada tabel basis data tentang data pribadi yang memat foto pribadi orang bersangkutan, karena akan memberikan efisiensi dalam penyimpanan dan keamanan.
3. Diharapkan penelitian dapat diterapkan pada sistem basis data yang sebenarnya atau pada tabel yang lebih kompleks dalam hal kerelasian antar tabel, untuk menguji kelayakan proses steganografi pada tabel basis data.

DAFTAR PUSTAKA

1. Stalling, William, 2003, *Cryptography and Network Security-Principles and Practice* 3rd edition, Prentice Hall.
2. Budi Sukmawan, http://bdg.ventrin.net.id/~budskman/stegano.htm /articles/ "*Steganografi".*
3. Johnson, Neil F.; Duric, Zoran; Jajodia, Shushil. 2001. *"Information Hiding Steganography and Watermaking-Attacks and Countermeasures",* Advanced in Information Security, Kluwer Academic Publisher, United State.
4. Product – wbStego4, http://www.8ung.at/wbailer/wbstego/pr99cf0.htm /articles/" *Carrier-Files".*
5. TuTran, http://www.cs.sfu.ca/CourseCentral/365/li/material/notes/Chap4/Chap4.2/Chap4.2.html, "*Steganography : The Art of Hiding Data",* Mills College Spring 2002