Coding : Jurnal Komputer dan Aplikasi
Volume 08, No. 01 (2020), hal 175-184 ISSN: 2338-493X

PENGAMANAN DATA RIWAYAT PENYAKIT PADA PASIEN MENGGUNAKAN STEGANOGRAFI *MOST SIGNIFICANT BIT* (MSB) (Studi Kasus: Penyakit Hiv/Aids Rumah Sakit Soedarso Pontianak)

Risma Maharani[1], Sampe Hotlan Sitorus[2], Dian Prawira[3]
[1,2]Jurusan Rekayasa Sistem Komputer dan [3]Jurusan Sistem Informasi, Fakultas MIPA
Universitas Tanjungpura
Jalan Prof Dr. H. Hadari Nawawi Pontianak
Telp./Fax. : (0561) 577963
e-mail: [1]rismamaharani@student.untan.ac.id, [2]sitorus.hotland@gmail.com,
[3]dian.prawira@sisfo.untan.ac.id

ABSTRAK

Perkembangaan teknologi pada sistem pengamanan data dalam menjaga keamanan informasi telah berkembang dengan pesat. Dalam menjaga keamanan data terdapat cabang ilmu dalam pengembangannya seperti steganografi. Saat ini pengamanan data riwayat penyakit pasien di Rumah Sakit Soedarso masih secara manual dengan ditulis dikertas dan disimpan di *filling cabinet*, untuk menjaga data medis terkait riwayat penyakit pasien di rumah sakit maka dibutuhkan sistem pengamanan data yang lebih kuat agar data yang jatuh ke tangan seseorang tidak dapat diketahui begitu saja. Penelitian tentang pengamanan data riwayat penyakit pasien menggunakan steganografi bertujuan agar data tidak dapat diketahui oleh orang yang tidak berkepentingan, serta bagaimana kinerja MSB pada pengamanan data riwayat penyakit pasien. Penelitian ini mengimplementasikan steganografi menggunakan metode *Most Significant Bit* (MSB) yaitu dengan menyisipkan bit pada bit awal dalam satu *byte* data dengan menggunakan citra sebagai media penampung. Hasil penelitian menunjukkan bahwa aplikasi berhasil melakukan penyisipan dan melakukan pemanggilan kembali pesan yang telah disisipkan. Hasil ekstraksi pesan memiliki tingkat kesesuaian karakter pesan terhadap isi pesan asli, pada gambar asli dan gambar stego terdapat perubahan yang nampak secara visual.

Kata kunci: Steganografi, *Most Significant Bit*, Pengamanan Data, Rekam Medis.

1. PENDAHULUAN

Seiring perkembangan teknologi yang pesat akses informasi dilakukan dengan mudah dari mana dan kapanpun. Kemudahan pengaksesan data dengan menggunakan teknologi melalui internet yang mengakibatkan orang yang tidak berkepentingan pun dapat memanfaatkan dan menyalah gunakannya. Disisi lain, beberapa data atau informasi selayaknya tidak jatuh ketangan orang lain, seperti data privasi, rahasia perusahaan, dan lain-lain.Pada bidang medis penggunaan informasi sangatlah penting untuk menunjang proses pelayanan agar lancar, cepat, dan efektif. Namun demikian, di sisi lain informasi yang terkait dengan hal-hal data medis tidak seluruhnnya dapat diakses oleh semua orang, seperti data riwayat penyakit pasien. Perlindungan terhadap data riwayat penyakit pasien telah diatur didalam Peraturan Menteri Kesehatan Republik Indonesia No.269/ Menkes/Per/III/2008 tentang Rekam Medik/*Medical Records*. Pasal 10 ayat 1, yang menegaskan "Informasi Tentang Identitas, Diagnosis, Riwayat Penyakit, Riwayat Pemeriksaan dan Riwayat Pengobatan Pasien harus Dijaga Kerahasiannya oleh Dokter, Dokter Gigi, Tenaga Kesehatan Tertentu, Petugas Pengelola Dan Pimpinan Sarana Pelayanan Kesehatan". Saat ini pengamanan data riwayat penyakit pasien di rumah sakit Soedarso masih secara manual dengan ditulis dikertas dan disimpan di *filing cabinet*. Oleh karena itu untuk menjaga data medis terkait

riwayat penyakit pasien di rumah sakit maka dibutuhkan sistem pengamanan data yang lebih kuat agar data yang jatuh ke tangan seseorang tidak dapat diketahui begitu saja. Adapun teknik pengamanan data riwayat penyakit yang akan dilakukan adalah meng-*encode* data tersebut dengan metode steganografi *Most Significant Bit* (MSB).

Penelitian tentang pengamanan data dilakukan oleh [1] yang berjudul Implementasi Steganografi Dalam Menyembunyikan Pesan Teks Dengan Metode MSB (*Most Significant Bit*)" menggunakan metode yang digunakan untuk melakukan penyisipan pesan kedalam *file* citra adalah metode MSB. Metode ini akan mengganti bit pertama dari piksel citra dengan bit-bit penyisip. Untuk melakukan penyisipan pesan kedalam citra warna, maka citra dan pesan penyisip harus diubah menjadi biner, dengan mengunakan format gambar Bitmap.

Penelitian lainnya tentang pengamanan data dilakukan oleh [2] yang berjudul Pengamanan Pesan dengan Steganografi MSB Berbasis Pencocokan Bit" menggunakan metode MSB bertujuan untuk Proses pencocokan dilakukan secara *divide* dan *conque*. Masukan data berupa pesan teks, citra, output yang dihasilkan berupa indeks posisi bit yang dapat digunakan sebagai kunci untuk merahasiakan data.

Penelitian lainya tentang pengamanan data [3] yang berjudul Penyembunyian Informasi (*steganography*) Gambar Menggunakan Metode LSB *(Least Significant Bit)*" penelitian tersebut menggunakan metode LSB untuk penggunaan media gambar sebagai data masukan media pembawa pesan rahasia berupa gambar dengan format BMP.

Dengan adanya masalah tersebut maka penelitian ini akan mengambil judul "Pengamanan Data Riwayat Penyakit Pada Pasien Menggunakan Steganografi Most Significant". Diharapkan penelitian ini akan dapat mengamankan data riwayat penyakit pada pasien di Rumah Sakit Soedarso Kota Pontianak.

2. LANDASAN TEORI

2.1 Pengolahan citra

Pengolahan citra adalah pemrosesan citra, khususnya dengan mengunakan komputer, menjadi citra yang kualitasnya lebih baik. Pengolahan citra bertujuan memperbaiki kualitas citra agar mudah di interprestasi oleh manusia atau mesin (dalam hal ini komputer).

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut piksel (piksel = *picture element*), element terkecil dari sebuah citra. Piksel merupakan elemen penyusun warna terkecil yang menyusun suatu citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Untuk menunjukkan lokasi piksel, koordinat (0,0) berfungsi untuk menunjukkan posisi sudut kiri atas pada citra, indeks x bergerak ke kanan dan indeks y bergerak ke bawah. Sebuah citra diubah ke bentuk digital agar dapat disimpan dalam memori komputer atau media lain.

Bila citra sudah diubah dalam bentuk digital, maka dengan berbagai proses pengolahan citra dapat dilkukan pada citra tersebut. Agar dapat diolah dengan komputer digital, maka suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Repersentasi citra dari fungsi kontinyu menjadi nilai-nilai diskrit disebut digitalisasi citra. Citra yang dihasilkan inilah yang disebut citra digital (*digital image*).

Pada umumnya citra digital berbentuk empat persegi panjang, dan dimensi ukurannya dinyatakan sebagai tinggi x lebar. Masing-masing elemen pada citra digital (berarti elemen matriks) disebut *image element, picture element* atau piksel atau pel. Jadi citra yang berukuran N × M mempunyai NM buah piksel. Citra biner hanya dikuantisasi pada dua level yaitu 0 dan 1. Tiap piksel pada citra biner cukup direpresentasikan dengan 1 bit, yang mana 0 berarti hitam dan bit 1 berarti putih [4] Berikut ini adalah perhitungan untuk mencari jumlah daya tampung dari gambar, dimana daya tampung harus lebih besar dari pada pesan yang ditampung, menggunakan persamaan 1.

$$DT = N \times M \quad (1)$$

Dimana DT adalah daya tampung, N adalah jumlah baris, dan M adalah jumlah kolom. Karena RGB mempunyai 3 lapisan *red,green*, dan *blue*, maka persamaan menjadi: Persamaan 2.

$$DT = N \times M \times 3 \quad (2)$$

Jumlah karakter bergantung pada kata yang akan disisipkan, kemudian untuk mengubah karakter menjadi biner maka jumlah karakter dikalikan 8. Adapun persamaan 3.

$$BT = K \times 8 \quad (3)$$

Dimana BT adalah bit tampung, K adalah jumlah karakter

Untuk mengetahui sisa bit tertampung yang telah digunakan, maka daya tampung dapat dikurang dengan bit tertampung, adapun persamaan 4:

$$SB = DT - BT \quad (4)$$

Dimana SB adalah sisa bit, DT adalah daya tampung, dan BT adalah bit tertampung.

2.1 *Steganografi*

Steganografi berasal dari bahasa Yunani, yaitu *"steganos"* yang artinya "tulisan tersembunyi *(covered writing)*". Steganografi membutuhkan dua properti yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program, atau pesan lain.

Saat ini steganografi sudah banyak diimplementasikan pada media digital. Steganografi digital mengunakan media digital sebagai penampung, seperti citra digital. Informasi yang disembunyikan juga berbentuk digital seperti teks. Steganografi digital dapat dipakai di negara-negara yang menerapkan sensor ketat terhadap informasi atau di negara di mana enkripsi pesan terlarang [5].

2.2 Most Significant Bit (MSB)

Sistem steganografi akan menyembunyikan sejumlah informasi dalam suatu berkas dan akan mengembalikan informasi tersebut kepada pengguna yang berhak. Terdapat dua langkah dalam sistem Steganografi yaitu proses penyembunyian dan *recovery* data dari berkas penampung. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode modifikasi *MSB* dari setiap sample pada citra. Pada susunan bit di dalam sebuah *byte (1byte = 8 bit)*, ada bit yang paling berarti *MSB* dan bit yang paling kurang berarti *LSB* [2].

Sebagai contoh akan disisipakan A ke dalam sebuah citra nilai A dalam ASCII adalah 65 kemudian nilai ASCII A diubah menjadi biner yaitu 0100 0001. Piksel citra yang akan disisipakan teks dari salah satu nilai warna foto memiliki nilai RGB pada koordiat 1,1 yaitu R(11111110) ,G(11111110), B(11111110), koordinat 1,2 yaitu R(11111110) ,G(11111110), B(11111110), koordinat 1,3 yaitu R(11111110) ,G(11111110), B(11111110), dan sisa biner dari RGB yang tidak berisi sisipkan biner teks, tetap megikuti nilai RGB asli. Tabel.1 menunjukkan hasil dari penyisipan.

Tabel.1 Proses Penyisipan

Biner Piksel Citra	Biner Huruf R	Piksel Citra Berubah
R : 11111110	0	01111110
G : 11111110	1	11111110
B : 11111110	0	01111110
R : 11111110	0	01111110
G : 11111110	0	01111110
B : 11111110	0	01111110
R : 11111110	0	01111110
G : 11111110	1	11111110
B : 11111110	-	11111110

2.3 Perlindungan Data Medis

Dalam penjelasan Peraturan Menteri Kesehatan Republik Indonesia No.269/ Menkes/Per/III/2008 tentang Rekam Medik/ Medical Records. Pasal 10 ayat 1, yang menegaskan "Informasi Tentang Identitas, Diagnosis, Riwayat Penyakit, Riwayat Pemeriksaan dan Riwayat Pengobatan Pasien Harus Dijaga Kerahasiannya oleh Dokter, Dokter Gigi, Tenaga Kesehatan Tertentu, Petugas Pengelola dan Pimpinan Sarana Pelayanan Kesehatan". Pasal 10 menjelaskan bahwa:

1. Informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan pasien harus dijaga kerahasiannya oleh dokter, dokter gigi, tenaga kesehatan tertentu, petugas pengolahan dan pimpinan sarana pelayanan kesehatan.
2. Informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan dapat dibuka dalam hal:
   a. Untuk kepentingan kesehatan pasien;

b. Memenuhi permintaan apatur penegak hukum dalam rangka penegakan hukum atas perintah pengadilan;
c. Permintaan dan/atau persetujuan pasien sendiri;
d. Permintaan institusi/ lembaga berdasarkan ketentuan perundang-undang; dan
e. Untuk kepentingan penelitian, pendidikan, dan audit medis, sepanjang tidak menyebutkan identitas pasien.

3. Permintaan rekam medis untuk tujuan sebagaimana dimaksud pada ayat (2) harus dilakukan secara tertulis kepada pimpinan sarana pelayanan kesehatan.

Dimana sudah tertera diundang-undang kesehatan bahwa data riwayat penyakit pasien wajib dilindungi, maka dari itu peneliti membuat suatu aplikasi pengamanan data riwayat penyakit pasien agar data tidak jatuh ke tangan orang yang tidak berkepentingan.

2.4 Hyper Text Markup Language (HTML)

Hyper Text Markup Language atau dikenal dengan istilah HTML. HTML merupakan sebuah bahasa pemrograman terstruktur yang dikembangkan untuk membuat sebuah halaman *website* yang dapat diakses atau ditampilkan pada *Web Browser* [6]. HTML tidak hanya mampu menampilkan teks tapi juga dapat menampilkan format-format lain dari teks tersebut, misalnya tabel, list, form, frame serta dapat digabungkan dengan obyek suara, gambar, video maupun Java. Dokumen yang berisi script HTML merupakan dokumen yang disajikan dalam bentuk website. Dokumen HTML disebut markup language karena mengandung tanda-tanda tertentu yang digunakan untuk menentukan tampilan suatu teks dan tingkat kepentingan dari teks tersebut dalam suatu document [7]. Dokumen dibagi menjadi dua bagian besar, yaitu *HEADER* (bagian atas) dan bagian *BODY* (tubuh dokumen). Masing-masing ditandai oleh pasangan tag <HEAD> dan <BODY>. Bagian HEAD berisikan judul dokument dan informasi-informasi dasar lain, sedangkan bagian BODY adalah data documennya[8].

2.5 M*ySQL*

MySQL termasuk dalam kategori database *management system*, yaitu suatu database yang terstruktur dalam pengolahan dan penampilan datanya. Mysql merupakan database yang bersifat *client server*, dimana data diletakkan diserver yang bisa diakses melalui komputer *client*. Pengaksesan dapat dilakukan apabila komputer telah terhubung dengan *server*. Berbeda dengan database desktop, dimana segala pemrosesan data harus dilakukan pada komputer yang bersangkutan [9]. *MySQL* merupakan suatu aplikasi yang bersifat gratis serta server basis data *MySQL* memiliki kinerja sangat cepat, reliable, dan mudah untuk digunakan. *SQL (Structured Query Language)* adalah sebuah konsep pengoperasian basis data, terutama untuk pemilihan *(SELECT)*, pemasukan *(INSERT)*, dan penghapusan *(DELETE)* serta pembaruan data *(UPDATE)*, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis [10].

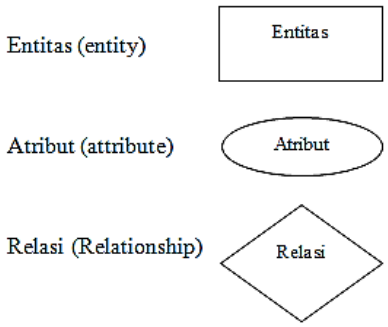
2.8 ERD

ERD adalah suatu diagram untuk menggambarkan *Desain* konseptual dari model konseptual suatu basis data relasional. ERD juga merupakan gambaran yang merelasikan antara objek yang satu dengan objek yang lain dari objek di dunia nyata yang sering dikenal dengan hubungan antar entitas. ERD terdiri dari 3 komponen utama [11]

a. Entitas (*Entity*). Adalah objek yang dapat dibedakan dalam dunia nyata. Sedangkan *entity set* adalah kumpulan dari *entity* yang sejenis. *Entity set* dapat berupa objek secara fisik (rumah, kendaraan, peralatan) atau objek secara konsep (pekerjaan, perusahaan). *Entity* disimbolkan dengan persegi panjang.
b. Relasi (*Relationship*). Adalah hubungan yang terjadi antara satu atau lebih *entity*. Sedangkan *relationship set* adalah kumpulan *relationship* yang sejenis. *Relationship* disimbolkan dengan jajar genjang.

Atribut (*Attribute*). Adalah karakteristik dari setiap *entity* atau *relationship* yang menyediakan penjelasan detail mengenai entity atau relationship tersebut. Nilai *attribute* adalah data aktual atau informasi yang disimpan pada suatu *attribute* di dalam *entity*

atau *relationship*, dimana *attribute* memiliki *domain* (*value set*) tersendiri. *Domain* (*value set*) adalah batas-batas nilai yang diperbolehkan bagi suatu *attribute*. Attribute disimbolkan dengan lingkaran.

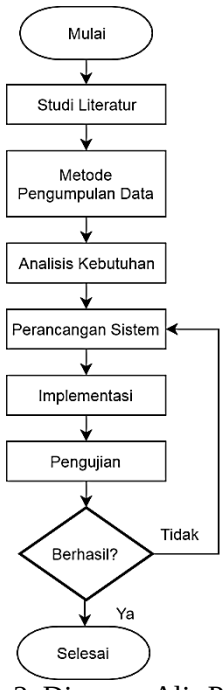


Gambar 1.Komponen Entity Relationship Diagram

3. METODE PENELITIAN

Dalam penelitian ini, penulis akan menggunakan metode *stegonografi* MSB. Penelitian ini akan di fokuskan dalam pembuatan suatu aplikasi dalam implementasi pengamanan data riwayat penyakit pasien yang akan di sisipkan pada gambar, sehingga akan mengurangi pencurian data oleh oknum yang tidak bertanggung jawab. Terdapat enam metodologi penelitian, yaitu studi literatur, metode pengumpulan data, analisis kebutuhan, perancangan sistem, implementasi, dan pengujian, seperti pada Gambar 2. Pada penelitian ini, studi literatur bertujuan untuk mencari referensi teori-teori yang terkait dengan penelitian. Referensi dapat berupa buku, jurnal atau sumber internet. Referensi juga bisa didapat dari wawancara terhadap pihak yang terkait dengan penelitian. Pada penelitian pengaman data riwayat pasien, referensi yang dibutuhkan antara lain tentang pengertian *steganografi*, algoritma MSB.

Pengumpulan data dilakukan pengumpulan data-data yang terkait dengan penelitian. Pada penelitian ini data yang dibutuhkan adalah riwayat penyakit pasien HIV/AIDS dan citra sebagai medianya. Data riwayat penyakit pasien berupa data sekunder yang di peroleh dari Rumah Sakit Dr. Soedarso, dan citra berupa pas gambar binatang. Analisis kebutuhan merupakan analisi yang dibutuhkan pada penelitian, seperti analisis data, analisis masalah, analisis solusi, dan analisis kebutuhan. Analisis kebutuhan digunakan dalam pembuatan sebuah aplikasi pengamanan data riwayat penyakit pasien analisis data, analisis masalah, analisis solusi, dan analisis kebutuhan.



Gambar 2. Diagram Alir Penelitian

Tahap perancangan sistem membahas perancangan sistem pengaman data riwayat penyakit pasien perancangan *software*, perancangan *interface*, dan simulasi sistem keamanan. Sistem kerja ini meliputi keseluruhan cara kerja aplikasi yang dibuat, yaitu merancang aplikasi untuk dapat melakukan encode dan decode. Aplikasi yang dirancang ini berbasis web dan dibangun dengan bahasa pemograman php. Implementasi sistem pada tahap ini peneliti menerapkan sistem yang sudah diuji sebelumnya sesuai dengan rancangan yang telah dibuat.

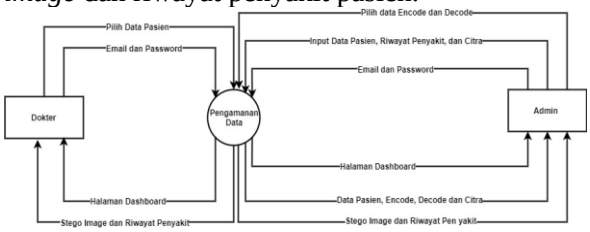
Pengujian sistem dilakukan menguji metode MSB, dimana pengujian yang dilakukan adalah dengan membandingkan inputan diagnosa dengan hasil yang telah disisipan mengunakan metode MSB, selain itu dilakukan pengujian parameter daya tampung citra, perubahan ukuran citra yang telah disisipkan, perubahan fisik pada citra, daya tampung, bit tertampung, dan sisa bit. Hasil

pengujian akan dianalisa sebelum dilakukan penarikan kesimpulan.

4. PERANCANGAN

Bagian ini menggambarkan rancangan sistem yang akan dibangun. Salah satu rancangan yang perlu dibuat adalah *Data Flow Diagram (DFD)*. *Data Flow Diagram (DFD)* adalah sebuah gambaran secara grafis tentang sistem yang menggunakan beberapa bentuk simbol untuk menggambarkan aliran data melalui suatu prosec yang saling berkaitan. *Data Flow Diagram (DFD)* menggambarkan *input*, *process*, dan *output* yang terjadi dalam suatu sistem.

Pada *DFD level 0* seperti pada Gambar 2dapat dilihat bahwa dalam aplikasi pengamanan data terdiri dari dua entitas yaitu *admin* dan dokter dimana masing-masing entitas tersebut memiliki fungsi yang berbeda. Dimana *admin* berfungsi untuk mengolah data riwayat penyakit pasien, dan dokter berfungsi untuk mengecek riwayat penyakit pasien yang telah di input. Admin dapat melakukan login terlebih dahulu, kemudian pengguna dapat input data pasien, riwayat penyakit, citra, *encode* dan *decode*. Hasil yang didapat berupa halaman *dashboard*, data pasien, riwayat pasien, citra, *stego image*, serta hasil *decode*. Dokter dapat melakukan login dengan memasukkan *email* dan password, dan dokter dapat melihat data pasien, kemudian hasil yang didapat berupa halaman *dashboard*, *stego image* dan riwayat penyakit pasien.



Gambar 3. *DFD Level 0*

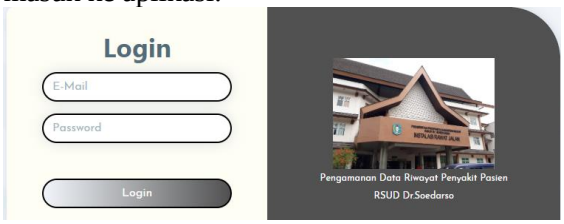
5. HASIL DAN PEMBAHASAN

5.1 Tampilan Aplikasi

Berikut merupakan tampilan dari masing-masing antarmuka dalam aplikasi pengamanan data.

1. Halaman *Login*

Halaman *login* sistem seperti yang terlihat pada Gambar 4, pada halaman ini terdapat teks input berupa email dan password, serta memiliki tombol untuk melakukan konfirmasi proses yaitu tombol "*login"* untuk masuk ke aplikasi.



Gambar 4 Halaman *Login* Sistem

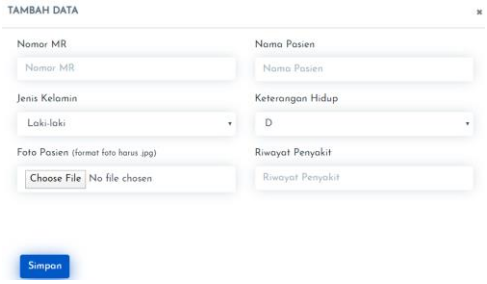
2. Halaman Kelola Data Pasien

Halaman kelola data pasien seperti yang terlihat pada Gambar 5, menampilkan tabel data pasien yang sudah diinput dan menampilkan beberapa fungsi seperti menambah, menghapus, dan dapat melihat secara detail dari data pasien tersebut.

Gambar 5.Halaman Kelola Data Pasien

3. Halaman Tambah data pasien

Halaman tambah data pasien seperti yang terlihat pada Gambar 6, admin dapat masukkan nomer MR, nama pasien, jenis kelamin, keterangan hidup, diagnosa penyakit serta upload gambar yang akan digunakan pasien tersebut untuk menyisipkan riwayat penyakitnya, kemudian terdapat tombol simpan jika data tersebut sudah benar, tombol batal jika ingin membatalkan

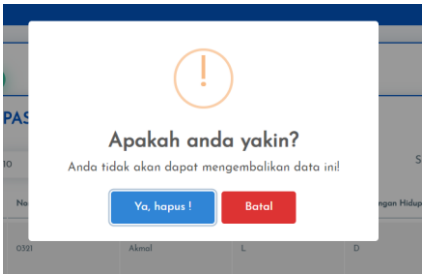


Gambar 6.Halaman Tambah Data

4. Halaman Hapus Data Pasien

Halaman hapus data pasien seperti yang terlihat pada Gambar 7 admin dapat menghapus data pasien yang tidak digunakan

lagi. Pada saat admin ingin menghapus data maka akan timbul modal konfirmasi.



Gambar 7.Halaman Hapus Data

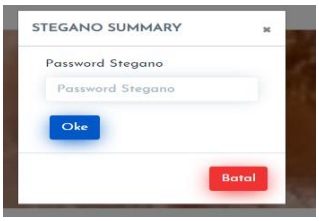
5. Halaman Detail Data Pasien

Halaman detail data pasien seperti yang terlihat pada Gambar 8 admin dapat melihat data pasien secara detail, terdapat tombol *stegano summary* untuk pengguna menampilkan hasil *encode* dan *decode.* Tombol *stegano summary* untuk pengguna memasuki *password* yang telah diberikan agar dapat melihat hasil *encode* dan *decode*.

Gambar 8.Halaman Detail Data Pasien

6. Halaman Password *Stegano Summary*

Halaman Password *Stegano Summary* seperti yang terlihat pada Gambar 9, admin terlebih dahulu harus memasuki password untuk hasil *encode* dan *decode.*



Gambar 9.Halaman Password *Stegano Summary*

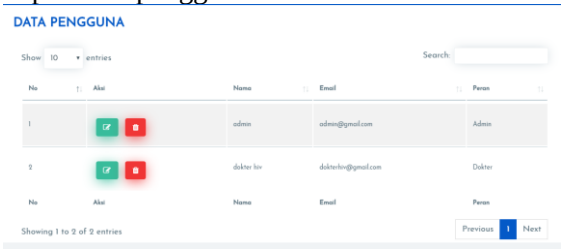
7. Halaman *Stegano Summary*

Halaman *Stegano Summary* seperti yang terlihat pada Gambar 10, dimana pada halaman ini menampilkan hasil *encode*, *decode*, serta pengujian lainnya.

Gambar 10.Halaman *Stegano Summary*

8. Halaman Kelola Pengguna

Halaman kelola pengguna seperti yang terlihat pada Gambar 11, dimana pada halaman ini dibuat untuk admin melihat pengguna lain yang menggunakan sistem. Pada halaman ini admin dapat melakukan tambah, edit, dan hapus data pengguna.



Gambar 11.Halaman Kelola Pengguna

9. Halaman Ganti Password

Halaman ganti password seperti yang terlihat pada Gambar 12, berfungsi untuk dokter mengganti password akunnya untuk masuk ke sistem.

Gambar 12.Halaman Ganti *Password*

5.2 Pengujian

Pengujian sistem dilakukan dengan menguji daya tampung citra, perubahan ukuran citra yang telah disisipkan, perubahan fisik pada citra, bit tertampung, dan sisa bit. Pada pengujian ini dilakukan menggunakan 30data riwayat penyakit pasien, dimana diambil 1 data dengan menggunakan foto binatang dengan ukuran file sebesar 100x100pixel, dan riwayat penyakit pasien yang disisipkan berupa ‘Sepsis, HIV/AIDS’, semua citra

menggunakan pada penelitian ini berukuran 100x100pixel agar perubahan antar citra asli dan *stego image*. Pada pengujian daya tampung dimana besar daya tampung harus lebih besar dari pada bit yang akan ditampung, perhitungan manual memiliki 30000pixel, dan sama pada sistem.

Pengujian perubahan ukuran citra memiliki perubahan yang sangat besar, perubahan terjadi dikarenakan perubahan format citra. Pengujian bit tertampung dan sisa bit hasil dari perhitungan manual memiliki kesamaan dengan sistem, dimana bit tertampung muat disisipkan pada citra yang telah tersedia, dan masih memiliki beberapa sisa bit dari daya tampung yang tidak digunakan. Perubahan pada citra terdapat perubahan secara visual antara citra asli dan *stego image*, terdapat pada kiri gambar, dapat dilihat pada Gambar 5.13.

Citra asli Stegano Image

Gambar 5.13 Pengujian

5.3 Pembahasan

Aplikasi yang telah dibangun mampu mengamankan data riwayat penyakit pada pasien dengan baik. Dalam proses mengamankan data digunakan metode MSB untuk proses *encode* dan *decode* riwayat penyakit pada pasien. Pertama admin menambahkan data pasien beserta foto, data pasien yang di input berupa nomer mr, nama pasien, jenis kelamin, keterangan hidup, dan riwayat penyakit pasien, dan foto yang di input akan di-*resize* oleh sistem berukuran 100x100 pixel. Ukuran tersebut dipilih agar foto yang digunakan ukurannya tidak terlalu besar dan masih terlihat dengan baik. Teks riwayat penyakit pada pasien yang diinputkan diubah ke ASCII kemudian ubah lagi ke desimal. Foto yang telah di *resize* maka diektrak dan diambil nilai RGBnya dari desimal diubah ke biner.

Masing–masing nilai biner dari teks riwayat penyakit pada pasien disisipkan pada bit awal atau paling kiri dari nilai biner RGB gambar. Misalnya huruf A mempunyai biner 01000001, kemudian salah satu nilai warna foto memiliki nilai R(11111110) ,G(11111110), B(11111110) maka bit pertama huruf A disisipkan ke R, sehingga R berubah menjadi (01111110), kemudian bit kedua disisipkan ke G, sehingga G menjadi(11111110), sehingga bit ketiga disisipkan ke B sehingga B berubah menjadi (01111110). Sisa 5 bit dari huruf A akan disisipkan ke RGB pada kolom selanjutnya. Disetiap akhir kata riwayat penyakit pada pasien diberikan tanda pembatas berupa tanda (#). RGB yang telah disisipkan akan di rekonstruksi kembali menjadi gambar yang utuh. Gambar tersebut kemudian akan disimpan. Untuk mengetahui informasi riwayat penyakit pada pasien yang telah disisipkan pada gambar maka admin perlu melakukan decode.

Pada proses ini citra hasil *encode (stego image)* diekstrak untuk mengambil nilai RGBnya. Nilai RGB tersebut diubah menjadi biner. Sistem mengambil bit pertama dari masing- masing nilai RGB. Bit yang telah diambil akan dipisah menjadi beberapa blok dengan isi 1 blok sebanyak 8 bit. Masing-masing blok tersebut akan dikembalikan ke desimal untuk mendapatkan nilai ASCII, sehingga diketahui huruf-hurufnya.

Pada saat melakukan penyisipan teks, ukuran daya tampung harus lebih besar daripada teks yang akan disisipkan ke dalam citra, agar teks yang akan disisipkan dapat tertampung pada citra. Perubahan *size* citra asli dan *stego image* terjadi dikarenakan adanya perubahan format citra, dimana ekstensi dari citra sebelum proses penyisipan teks adalah JPG, sedangkan ekstensi setelah proses penyisipan teks adalah PNG, dimana format JPG menggunakan teknik kompresi yang menyebabkan kualitas gambar menjadi turun *(lossy compression).* Citra dengan format JPG biasanya ukuran gambarnya lebih kecil, dan kualitasnya lebih rendah, sedangkan format PNG menggunakan teknik kompresi yang tidak menghilangkan data *(lossles compression)*. Teknik ini mengkompresi gambar dari proses fotografi tanpa banyak mengurangi kualitas gambarnya sehingga ukuran gambar yang dihasilkan lebih besar daripada citra dengan format JPG. Pada citra

asli dan *stego image* terdapat perubahan yang nampak secara visual, dimana perubahan terletak pada bagian atas kiri dari citra, perubahan ini dikarenakan pesan yang telah disisipkan menggunakan metode MSB, dimana pesan yang telah disisipkan diletakkan pada awal bit yang membuat pengaruh perubahan yang besar terhadap RGB citra, sehingga menghasilkan perubahan secara visual.

Hasil pengujian sistem yang telah dilakukan oleh peneliti menunjukkan sistem yang dibangun dapat melakukan pengamanan data dengan baik. Pengujian menggunakan 30 data riwayat penyakit pada pasien, data tersebut diuji dengan cara membandingkan inputan riwayat penyakit pada pasien dengan hasil yang telah disisipkan mengunakan metode MSB, dimana *encode* dan *decode* tidak memiliki perbedaan, selain itu dilakukan juga pengujian parameter perubahan ukuran citra, dimana perubahan terjadi karena adanya perubahan format pada citra, perubahan fisik pada citra yang telah disisipkan terdapat perubahan secara visual pada bagian kiri citra, daya tampung, bit tertampung, dan sisa bit, dimana pengujian ini dilakukan dengan membandingkan hasil perhitungan manual dan sistem memiiki kesamaan.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

1. Kinerja MSB dalam mengamankan data riwayat penyakit pasien diukur dari daya tampung citra, perubahan ukuran citra yang telah disisipkan, perubahan fisik pada citra, bit tertampung, dan sisa bit serta perhitungan manual, pada ukuran citra awal dan citra stegano memiliki perubahan ukuran, terdapat perubahan fisik pada citra asli dan citra *stegano* dimana pada atas kiri gambar stegano terdapat perubahan ,pada *encode* dan *decode* mengeluarkan teks yang sama.
2. Berdasarkan pengujian dari 30 data yang telah dilakukan dalam parameter daya tampung citra ukuran daya tampung harus lebih besar daripada teks yang akan disisipkan ke dalam citra,maka dipilih citra berukuran 100x100 piksel, ukuran dipilih agar foto yang digunakan ukurannya tidak terlalu besar dan masih terlihat dengan baik. Perubahan ukuran citra yang telah disisipkan rata-rata sebesar 21,53 dikarenakan adanya perubahan format citra, dimana ekstensi dari citra sebelum proses penyisipan teks adalah JPG, sedangkan ekstensi setelah proses penyisipan teks adalah PNG. Perubahan fisik pada citra asli dan *stego image* ini dikarenakan pesan yang telah disisipkan menggunakan metode MSB, dimana pesan yang telah disisipkan diletakkan pada awal bit yang membuat pengaruh perubahan yang besar terhadap RGB citra, sehingga menghasilkan perubahan secara visual, bit tertampung, dan sisa bit, dimana pengujian ini dilakukan dengan membandingkan hasil perhitungan manual dan sistem memiliki kesamaan.

6.2 Saran

Adapun saran yang dapat peneliti berikan untuk penelitian selanjutnya, yaitu memperbaharui data yang disisipkan berupa *file*, gambar, audio dan video.

DAFTAR PUSTAKA

[1] Wahyuni, M. S. (2017). Implementasi Steganografi Dalam Menyembunyikan Pesan Teks Dengan Metode Msb(Most Significant Bit). *Jurnal Nasional Informatika dan Teknik Jaringan*, 121.

[2] B.Prasetiyo, R.Gernowo, dan B.Noranita. (2013). Pengamanan Pesan deangan Steganorafi MSB Berbasis Pencocokan Bit. *ISBN 978-602-14724-4-6*, 143.

[3] Irfan. (2013). Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB(LEAST SIGNIFICANT BIT). *Rekayasa Teknologi Vol.5, No. 1*, 1

[4] Putra, D. (2010). *Pengolahan Citra Digital*. Yogyakarta: ANDI.

[5] Munir, R. (2006). *Kriptografi*. Oktober: Informatika Bandung.

[6] Setiawan, D. (2017). *Buku Sakti Pemrograman Web*. Yogyakarta: START UP.

[7] Asih Winantu dan Wahyu T.Saputro. (2010). *Pemograman Web dengan HTM L, XHTML, CSS, JavaScript*. Yogyakarta:

Explore.

[8] Taryana Suryana dan Jonathan Sarwono. (2007). *E-commerce menggunakan PHP dan MySQL*. Yogyakarta: Graha Ilmu.

[9] Sugiri, Dan Haris Saputro. (2008). *Pengolahan Database MySQL dengan PhpMyAdmin*. Yogyakarta: Graha Ilmu.

[10] Yuliansyah, H. (2014). Pera ncan ga n Replikasi Basis Data MySQL dengan Mekanisme Pengamanan Menggunakan SSL Encryption. *Jurnal Infor atika*, 826-836.

[11] Enterprise, J. (2015). *Mengenal PHP Menggunakan Framework Laravel*. Jakarta: PT Elex Media Komputindo.

[12] Yanto, R. (2016). *Manajemen Basis Data Menggunakan MySQL*. Yogyakarta: Deepublish