Penyisipan Data Diagnosa Pasien Covid-19 Dalam Citra Medis Digital X-Ray

Agus Prihanto[1], Aditya Prapanca[2], Dedy Prehanto[3]

[1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1]agusprihanto@unesa.ac.id

***Abstrak*— Salah satu contoh penggunaan steganografi adalah untuk kepentingan medis yaitu penyisipan pesan diagnosa pasien kedalam citra digital hasil scan *X-Ray*. Kita ketahui bahwa saat ini sudah mulai banyak penggunaan citra digital karena kemudahan dalam pengelohaan data, penyimpanan dan pendistribusiannya. Untuk menjaga kerahasian hasil diagnosa pasien merupakan masalah tersendiri dalam rekam medis karena data tersebut tidak boleh diketahui oleh orang yang tidak berkepentingan. Metode konvensional biasanya menggunakan map berkas rekam medis dan dituliskan kata rahasia. Metode ini sangat rawan sekali untuk masih dapat diketahui orang yang tidak berkepentingan sehingga diperlukan perbaikan pola penyimpanan data rekam medis tersebut. Penelitian ini berfokus pada penyembuyian dan kerahasian informasi diagnosa pasien Covid-19 pada citra medis dengan teknik steganografi PVD (*Pixel Value Differencing*) sehingga data rekam medis pasien tetap aman dari orang-orang yang tidak berkepentingan. Ide dasar adalah citra akan diklasifikasikan dengan Tabel *Contiues Range* yang telah ditentukan dengan tujuan untuk mengetahui tingkat perbedaan nilai antara 2 pixel yang saling berdekatan. Dari nilai tersebut nantinya akan ditentukan seberapa banyak bit informasi yang akan disisipkan. Dengan semakin besar selisih nilai 2 pixel yang berdekatan maka peluang penyisipan informasi tersembuyi akan semakin besar. Untuk lokasi penyisipan akan menggunakan teknik yaitu horisontal scanning.**

Hasil pengujian menunjukkan bahwa 1) Kapasitas metode PVD lebih besar jika dbandingkan dengan metode LSB 1 Bit dengan peningkatan rata-rata 311 % (3,11 kali), 2) Kualitas gambar stego hasil PVD dan LSB 1 Bit tergolong sangat baik dengan ditunjukkan nilai PSNR > 60%, 3) Hasil analisa histogram antara gambar asli, gambar stego PVD dan gambar stego LSB 1 Bit secara kasat mata memiliki kemiripan yang cukup tinggi dan 4) Hasil penyisipan pesan dengan kriptografi memberikan keamanan lebih jika dbandingkan dengan penyisipan tanpa kriptografi.

***Kata Kunci*— Covid-19, Citra Medis, X-Ray, Steganografi PVD**

I. PENDAHULUAN

Internet merupakan salah satu bagian dari teknologi informasi dan telekomunikasi yang sangat penting saat ini. Banyak perusahaan, instansi pemerintahan bahkan individu perorangan yang memanfaatkan media ini untuk bertukar informasi dan kita ketahui bahwa komunikasi data lewat jaringan internet mempunyai peluang besar untuk di lihat (*sniffing*) oleh pihak ketiga karena informasi yang kita kirim tersebut harus melewati jaringan umum sehingga semua orang berhak menggunakannnya.

Untuk menjaga kerahasian informasi telah dikembangkan teknik *kriptografi* yang bersifat mengacak informasi sehingga tidak mudah dimengerti, namun teknik ini dapat menimbulkan kecurigaan. Untuk memperbaiki teknik tersebut telah dikembangkan teknik lain yaitu *Steganografi*.

Steganografi merupakan sebuah seni dan bidang ilmu yang mempelajari tentang komunikasi yang tak tampak (*invisible communication*) dengan menyembunyikan informasi penting di atas media informasi yang lain, sehingga keberadaan informasi yang sesungguhnya tidak nampak keberadaannya.

Steganografi berbeda dengan kriptografi, kriptografi berfokus pada bagaimana melindungi isi informasi agar tetap aman (*secure*), sedangkan steganografi berfokus bagaimana agar isi informasi tidak terlihat keberadaanya (*invisible*). Di lain pihak, steganografi dan kriptografi memiliki persamaan yaitu keduanya berusaha melindungi isi informasi agar tidak diketahui oleh pihak yang tidak diinginkan.

Salah satu contoh penggunaan steganografi adalah untuk kepentingan medis yaitu penyisipan pesan diagnosa pasien kedalam citra digital hasil scan X-Ray. Kita ketahui bahwa saat ini sudah mulai banyak penggunaan citra digital karena kemudahan dalam pengelohaan data, penyimpanan dan pendistribusiannya. Untuk menjaga kerahasian hasil diagnosa pasien merupakan masalah tersendiri dalam rekam medis karena data tersebut tidak boleh diketahui oleh orang yang tidak berkepentingan. Metode konvensional biasanya menggunakan map berkas rekam medis dan dituliskan kata rahasia. Metode ini sangat rawan sekali untuk masih dapat diketahui orang yang tidak berkepentingan sehingga diperlukan perbaikan pola penyimpanan data rekam medis tersebut.

Dari latar belakang permasalahan yang dikemukan sebelumnya, maka tujuan dalam penelitian ini adalah menyisipkan pesan diagnosa pasien covid-19 pada citra digital hasil scan X-Ray dengan menggunakan Teknik Steganografi PVD (*Pixel Value Differencing*) dan penggunaakan kriptografi Triple-DES untuk enkripsi pesan rahasia..

II. KAJIAN PUSTAKA

A. Penelitian Terkait

Ada beberapa penelitian steganografi yang terkait dengan citra medis yaitu :

- Robin **Maulana** yang berjudul *Steganografi Berbasis Citra Menggunakan Prosesor ARM7TDMI dan Algoritma LSB*. Penelitian ini mengimplementasikan steganografi menggunakan prosesor ARM7TDMI dan GSM 900. Dalam penyisipan pesan rahasia kedalam citra medis menggunakan teknik spasial domain LSB (*Least Significant Bit*) 1 bit [2].
- **Meirista Wulandari** dan **Indah Soesanti** yang berjudul *Analisis Kualitas dan Kuantitas Steganografi dengan Interpolasi Citra Medis menggunakan Teknik Interpolasi.* Penelitian ini membagi citra digital menjadi 2 area yaitu

daerah tepi dan non tepi, kemudian pesan tersembunyi disisipkan di pixel interpolasi. Untuk mengekstrak pesan maka pesan tersembunyi tersebut diambil dari pixel interpolasi kemudian citra stego dikembalikan ke citra aslinya [7].

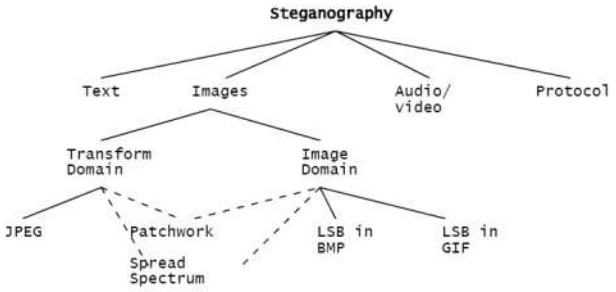
B. Teknik Steganografi

Teknik steganografi pada citra gambar dapat digolongkan menjadi dua bagian: *domain spasial* dan *domain frekuensi*. Pada *domain spasial* informasi dimasukkan ke dalam tiap pixel satu persatu, sedangkan pada *domain frekuensi*, gambar dirubah ke domain frekuensi terlebih dulu baru kemudian pesan di masukkan ke dalam gambar.

Teknik steganografi pada *domain spasial* menggunakan metode *bit-wise* dengan memanipulasi bit bernilai rendah. Format gambar yang paling cocok untuk cara ini adalah tipe *lossless*. Namun, cara ini sangat bergantung kepada format gambarnya [4].

Steganografi pada *domain frekuensi* menggunakan teknik manipulasi algoritma dan transformasi gambar. Metode ini menyembunyikan informasi pada area yang memiliki nilai bit lebih tinggi pada cover image. Kelebihan metode ini cocok untuk berbagai format gambar, karena pesan yang disisipkan juga dapat bertahan walaupun menggunakan teknik kompresi *lossy* maupun *lossless*.

Berikut adalah skema teknik steganografi dan penggolongan berdasarkan domainnya.



Gbr. 1 Skema penggolongan Steganografi berdasarkan domainnya

C. Kreteria Steganografi yang Bagus

Penyembunyian informasi ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah [5] :

- *Fidelity*. Kualitas citra penampung (cover) tidak banyak berubah setelah disisipi informasi tersembunyi, sehingga tidak menimbulkan kecurigaan bagi pengamatnya.
- *Robustness*. Informasi yang disembunyikan harus dapat bertahan terhadap manipulasi yang dilakukan pada citra penampung dan informasi yang tersembunyi tidak rusak.
- *Recovery*. Informasi yang disembunyikan harus dapat diambil kembali (*recovery*) untuk digunakan lebih lanjut.

D. Teknik Steganografi Least Significant Bit Insertion (LSB)

Least Significant Bit Insertion merupakan salah satu metode steganografi yang yang paling sederhana dan mempunyai kapasitas penyisipan informasi tersembuyi yang cukup besar. LSB insertion menggunakan teknik penyisipan pada bit dengan nilai rendah (*Least Siginifacant*) pada data pixel file citra tersebut. Untuk file bitmap 24 bit (*True Color*) tersusun dari tiga warna yaitu: merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit dapat disisipkan 3 bit data [6]

Contoh penyisipan huruf A pada citra dengan format bmp 24 bit pixel dengan data raster biner gambar asli ditunjukkan oleh Gbr. 2 :

```
00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001
```

Gbr. 2 Data raster biner gambar asli

Sedangkan representasi biner ASCII huruf A adalah :

```
01000001
```

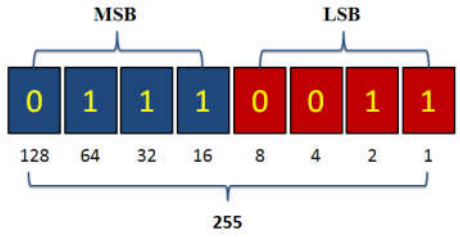
Gbr. 3 Representasi biner ASCII huruf A

Dengan menyisipkannya pada data pixel diatas maka akan dihasilkan :

```
00100110 11101001 11001000
00100110 11001000 11101000
11001000 00100111 11101001
```

Gbr. 4 Data raster biner gambar asli setelah disisipi data biner ASCII huruf A

Terlihat hanya tiga bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Untuk meningkatkan kapasitas maka dapat digunakan bit rendah kedua dan seterusnya, namun sebaiknya tidak melebihi 4 bit LSB [1], karena semakin banyak bit LSB yang digunakan maka gambar akan semakin banyak mengalamai perubahan layaknya sehingga kualitas citra penampung menjadi turun.



Gbr. 5 Representasi Biner 4-LSB

Gambar di atas merupakan representasi biner 1 byte (8 bit), bagian yang berwarna biru merupakan MSB (*Most Significant Bit*) sedangkan yang merah merupakan LSB (*Least Significant Bit*). Kita dapat menyisipkan pada bagian yang berwarna merah. Jika kita rekontruksi ulang contoh sebelumnya dengan menggunakan penyisipan multi LSB 4 bit

E. Teknik Steganografi Pixel Value Differencing (PVD)

PVD merupakan salah satu metode steganografi *domain spasial* dengan memanfaatkan selisih piksel bertetangga untuk menentukan jumlah bit pesan rahasia yang disisipkan pada

kedua piksel tersebut. Dasar pemikiran metode *pixel-value differencing* adalah penglihatan mata manusia tidak sensitif terhadap perubahan piksel dengan nilai kekontrasan tinggi (*edge area*) dan sensitif pada piksel dengan nilai kekontrasan rendah (*smooth area*), sehingga pada *edge area* dapat disisipkan bit pesan rahasia lebih banyak, dan sedikit bit pada *smooth area*. Jumlah bit pesan yang disisipkan bersifat *adaptif*, artinya untuk tiap piksel jumlahnya berbeda-beda tergantung selisih nilai piksel tersebut.

Metode ini dikembangkan oleh Wu & Tsai [8], dilakukan dengan membagi *cover-object* menjadi blok-blok yang tidak *overlap* kemudian dihitung selisih dua piksel bertetangga (p_i,p_{i+1}). Selisih piksel tersebut kemudian digunakan untuk menentukan jumlah bit pesan rahasia yang dapat disisipkan pada blok tersebut yang diklasifikasikan berdasarkan nilai *continuous range* R. Nilai R yang diusulkan oleh Wu & Tsai [8] adalah [0,7], [8-15], [16-31], [32,63], [64,127] dan [128,255].

Nilai R digunakan untuk menentukan lokasi dari selisih dua piksel sehingga dapat tentukan jumlah bit yang disisipkan berdasarkan rentang nilai. Semakin besar selisih piksel, maka nilai R juga semakin besar dan jumlah bit yang disisipkan juga semakin banyak, dan sebaliknya. Misalkan, selisih dua piksel adalah 10, maka berdasarkan nilai R berada pada rentang 8 s.d 15. Berdasarkan nilai rentang tersebut kemudian dapat diketahui jumlah bit yang disisipkan.

F. Kriptografi

Kriptografi adalah ilmu untuk menjaga kerahasiaan informasi. Meskipun begitu, kriptografi juga sering disebut sebagai sebuah seni, karena memang diperlukan kreativitas dalam mencari metode untuk mengamankan informasi. Tujuan utama dari kriptografi tentu saja untuk mengamankan informasi. Pengamanan informasi yang dilakukan mencakup beberapa aspek yang termasuk dalam aspek keamanan informasi [3], yaitu:

- *Kerahasiaan*, menjaga isi informasi dari pihak yang tidak memiliki otoritas.
- *Integritas data*, menjaga data tidak berubah secara tidak sah.
- *Autentikasi*, digunakan untuk identifikasi data.
- *Non-repudiasi*, mencegah penyangkalan oleh pengirim/pembuat.

G. Signal To Noise Ratio

Signal-to-noise ratio didefinisikan sebagai kekuatan rasio antara sinyal (**S** -informasi yang berarti) dan latar belakang noise (**N** - sinyal yang tidak diinginkan):

$$SNR = \frac{Psignal}{Pnoise} \quad (1)$$

Dalam bidang citra digital secara sederhana Psignal merupakan jumlah pixel gambar dan Pnoise merupakan jumlah pixel noise

$$SNR = \frac{Jumlah\ Pixel\ Gambar\ Asli}{jumlah\ Pixel\ Berubah} \quad (2)$$

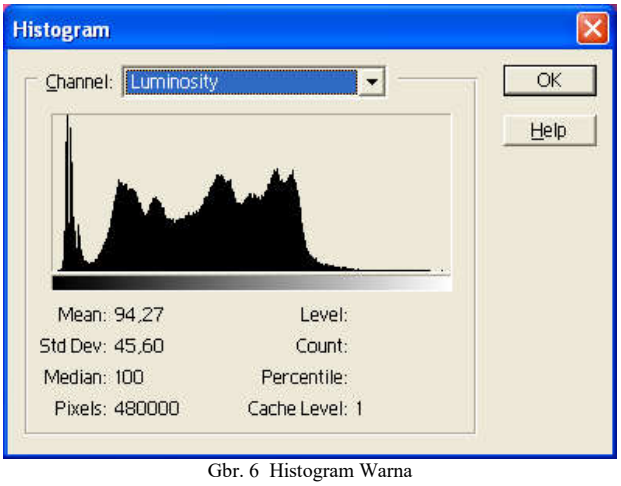
Jika rumus di atas digunakan untuk mengukur tingkat perubahan pixel dalam penyisipan bit pada image steganografi, maka dapat diformulasikan ulang menjadi

$$SNR = \frac{Jumlah\ Pixel\ Gambar}{Jumlah\ Perubahan\ Pixel} \quad (3)$$

Jika SNR semakin besar maka semakin sedikit perubahan bit pixel akibat penyisipan dan begitu sebaliknya.

H. Histogram Warna

Histogram merupakan bentuk representasi grafis untuk distribusi warna dari citra digital yang dinyatakan dalam sumbu X dan Y. Sumbu Y mewakili frekuensi kemunculan warna dan sumbu X mewakili intensitas warna. Intensitas warna untuk gambar bertype RGB 24 bit (*True Color*), setiap warna (R/G/B) diwakili dengan 8 bit (24 bit/3). Ini berarti intensitas warna dapat diwakili angka 0 sampai 255. Kadang dalam analisa kita juga membutuhkan histogram grayscalenya yaitu didapatkan dari nilai rata-rata intensitas warna RGB.

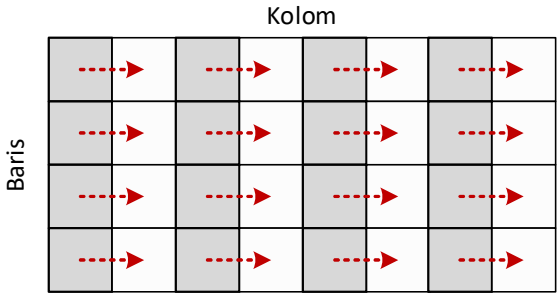


Gbr. 6 Histogram Warna

III. METODE PENELITIAN

Penelitian ini berfokus pada penyembuyian dan kerahasian informasi diagnosa pasien Covid-19 pada citra medis dengan teknik steganografi PVD (*Pixel Value Differencing*) sehingga data rekam medis pasien tetap aman dari orang-orang yang tidak berkepentingan.

Ide dasar adalah citra akan diklasifikasikan dengan Tabel *Contiues Range* yang telah ditentukan dengan tujuan untuk mengetahui tingkat perbedaan nilai antara 2 pixel yang saling redekatan. Dari nilai tersebut nantinya akan ditentukan seberapa banyak bit informasi yang akan disisipkan. Dengan semakin besar selisih nilai 2 pixel yang berdekatan maka peluang penyisipan informasi tersembuyi akan semakin besar. Untuk lokasi penyisipan akan menggunakan teknik *horisontal scanning* yaitu penyisipan dimulai dari pojok kiri atas ke kanan, kemudian diulang kebaris berikutnya sampai semua informasi disisipkan

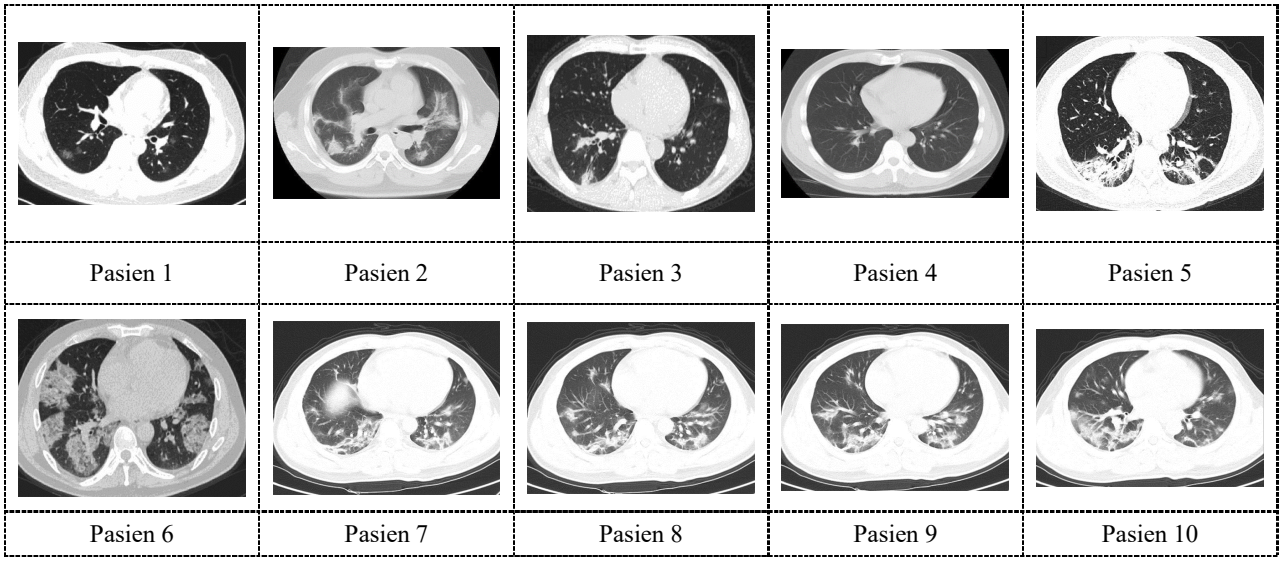


Gbr. 7 Proses penyisipan bit informasi tersembunyi menggunakan Single PVD

IV. HASIL DAN PEMBAHASAN

Uji coba ini dilakukan untuk menguji kebenaran dari tujuan dan manfaat penelitian yang dikemukakan pada bab pendahuluan yaitu mengembangkan teknik Penyisipan Pesan Tersembunyi Data Diagnosa Pasien Covid-19 Dalam Citra Medis Digital X-Ray dengan menggabungan teknik steganografi PVD dan kriptografi Triple-DES agar diperoleh peningkatan kapasitas (daya tampung) penyisipan dan kualitas citra yang serta perlindungan keamanan informasi tersembunyi yang lebih baik.

Dalam pengujian menggunakan data citra COVID-19 yang berjumlah 10 buah dengan format BMP mode grayscale 8 bit dan kemudian dilakukukan pengukuran dan komparasi terhadap metode yang disusulkan dalam hal ini PVD dibandingkan dengan metode LSB 1 bit.



Gbr. 8 Data digital Rontgen X-Ray mode Grayscale.

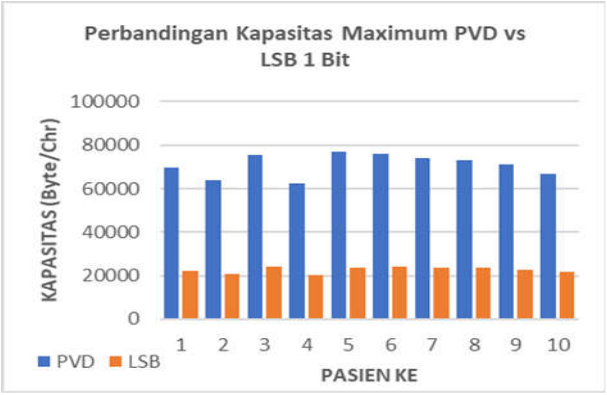
A. Pengujian Pengukuran Kapasitas

Berikut adalah data hasil pengukuran kapasitas maximum terhadap 2 metode yaitu PVD dan LSB 1 bit.

TABEL I
PERBANDINGAN KAPASITAS MAXIMUM METODE PVD VS LSB 1 BIT.

Data	Dimension	Capasity (Byte/Chr)		Compare PVD/LSB %
		PVD	LSB	
Pasien 1	500x358	69.704	22.375	311,5
Pasien 2	500x331	63.669	20.687	307,8
Pasien 3	500x386	75.298	24.125	312,1
Pasien 4	500x325	62.580	20.312	308,1
Pasien 5	500x382	76.955	23.875	322,3
Pasien 6	500x388	75.727	24.250	312,3
Pasien 7	500x380	73.798	23.750	310,7
Pasien 8	500x376	73.171	23.500	311,4
Pasien 9	500x365	71.024	22.812	311,3
Pasien 10	500x344	66.924	21.500	311,3
			Rata-rata	**311,9**

Berikut adalah grafik dari pengolahan data pada Tabel I :



Gbr. 9 Grafik perbandingan kapasitas maximum PVD vs LSB 1 Bit.

Dari Tabel I dan grafik pada Gbr 12 diperoleh informasi bahwa kapasitas maximum metode PVD lebih besar daripada metode LSB 1 bit dengan rata2 peningkatan sekitar 311,9% (3,1 kali).

B. Pengujian Pengukuran PSNR

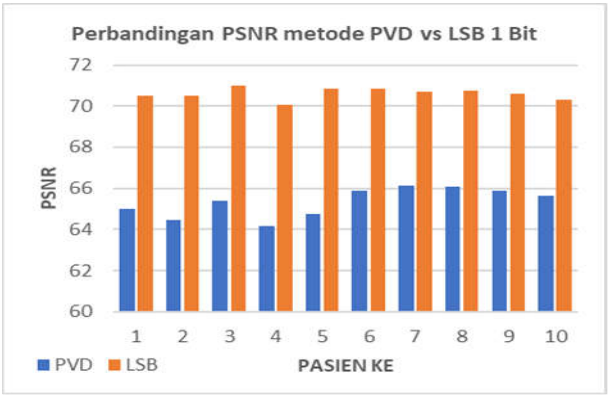
Berikut adalah data hasil pengukuran PSNR terhadap 2 metode yaitu PVD dan LSB 1 bit setelah disisipi pesan Rekam

Medik pasien tanpa menggunakan kriptografi.

TABEL III
PERBANDINGAN PSNR METODE PVD VS LSB 1 BIT.

Data	Dimension	PSNR (dB)		Perbedaan LSB-PVD
		PVD	LSB	
Pasien 1	500x358	65,00	70,50	5,50
Pasien 2	500x331	64,47	70,48	6,01
Pasien 3	500x386	65,39	70,99	5,60
Pasien 4	500x325	64,17	70,08	5,91
Pasien 5	500x382	64,74	70,85	6,11
Pasien 6	500x388	65,89	70,86	4,97
Pasien 7	500x380	66,14	70,71	4,57
Pasien 8	500x376	66,10	70,75	4,65
Pasien 9	500x365	65,87	70,62	4,75
Pasien 10	500x344	65,66	70,32	4,66
			Rata-Rata	**5,27**

Berikut adalah grafik dari pengolahan data pada Tabel II :

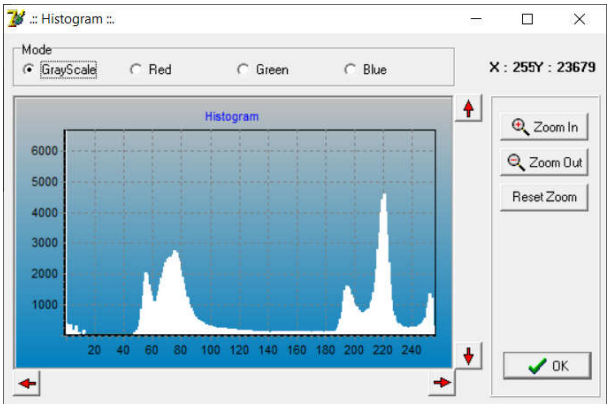


Gbr. 10 Perbandingan PSNR metode PVD vs LSB 1 Bit

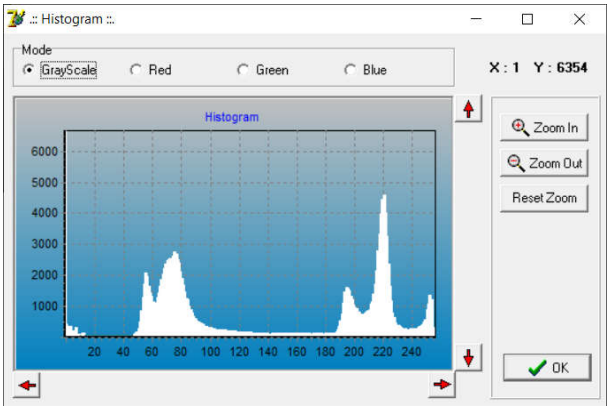
Dari Tabel II dan grafik Gambar 13. diperoleh informasi bahwa PSNR metode PVD lebih kecil daripada metode LSB 1 bit dengan rata-rata selisih mencapai sekitar 5,27 dB. Hal ini menunjukkan bahwa kualitas citra setelah disisipi pesan tersembunyi pada metode LSB 1 Bit lebih baik jika dbandingkan dengan metode PVD. Ini dapat terjadi karena pada metode LSB 1 Bit hanya merubah 1 bit saja dalam setiap pixel gambar sedangkan pada metode PVD menggunakan tabel continues range standar yang mana memiliki aturan minimal penyisipan bit adalah 3 bit pada setiap 2 pixel yang berdekatan. Namun jika dlihat dari nilai PSNR-nya, kedua metode ini masih memiliki nilai di atas 60 dB, sehingga kualitas citra masih dalam kategori sangat baik.

C. Pengujian Pengukuran Histogram

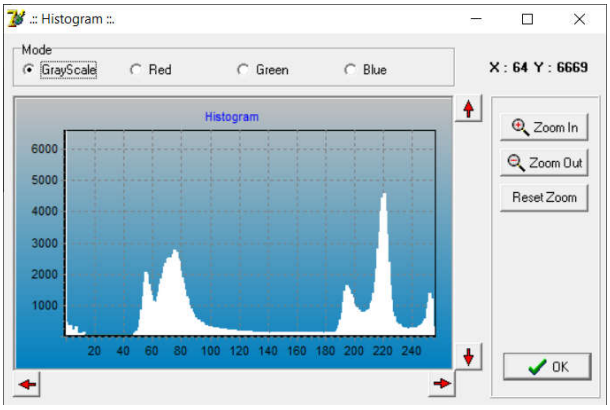
Berikut adalah data sampling hasil pengukuran histogram terhadap 3 gambar yaitu 1) gambar asli, 2) gambar stego hasil penyisipan dengan metode PVD dan 3) gambar stego hasil penyisipan dengan metode LSB 1 Bit pada pasien ke 4.



Gbr. 11 Gambar asli pasien ke 4



Gbr. 12 Gambar stego hasil penyisipan dengan metode PVD Pasien ke 4



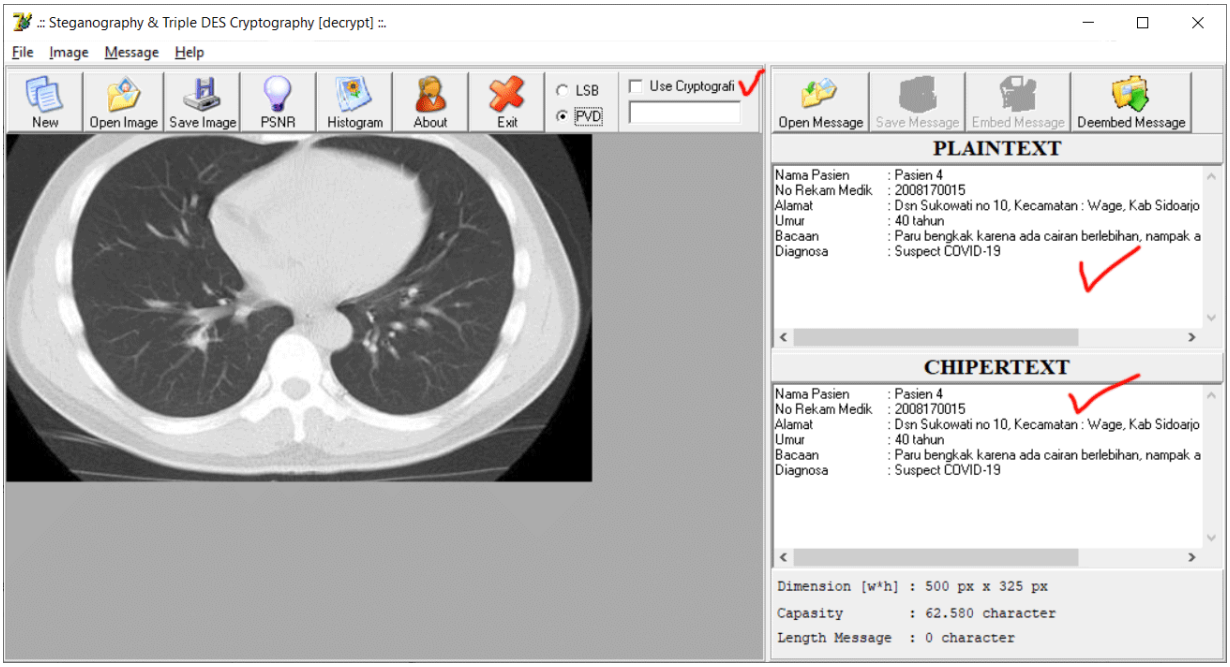
Gbr. 13 Gambar stego hasil penyisipan dengan metode LSB 1 Bit Pasien ke 4

Dari Gbr. 11, Gbr. 12 dan Gbr. 13 diporoleh informasi bahwa secara kasat mata ketiga histogram memiliki bentuk yang hampir sama. Hal ini menunjukkan bahwa ketiga gambar tersebut memiliki kemiripan yang hampir serupa. Kemiripan ini juga sejalan dengan nilai PSNR sebelumnya bahwa metode PVD dan LSB 1 Bit bernilai di atas > 60 dB.

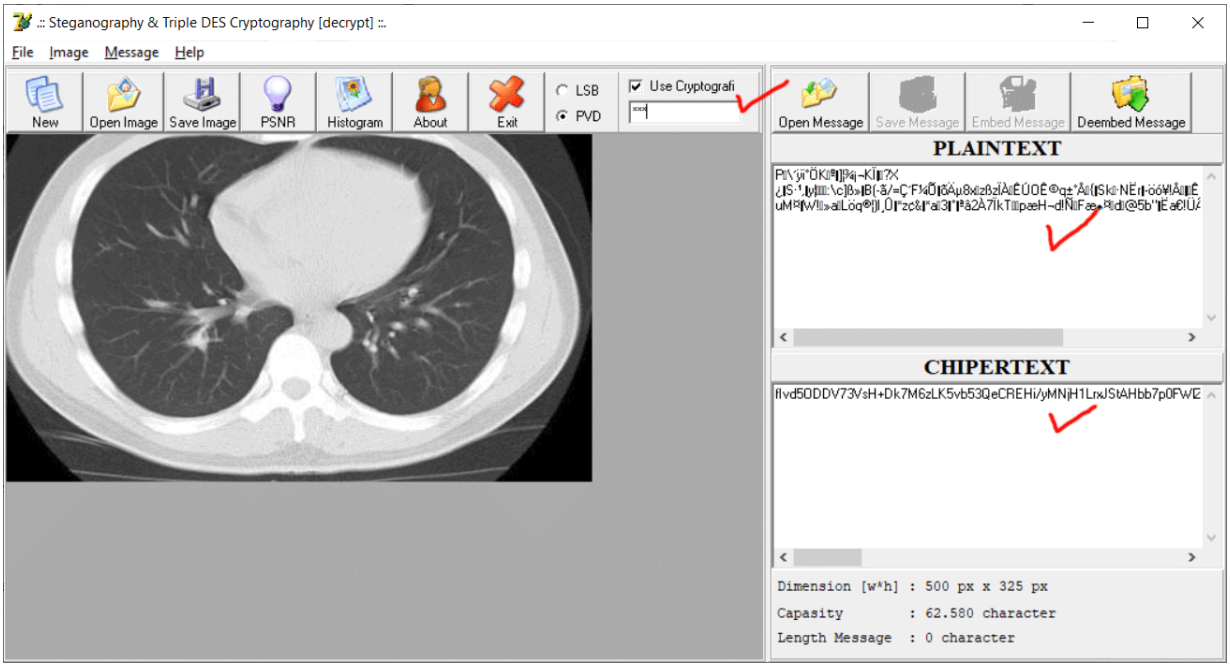
D. Pengujian Penambahan Kriptografi

Pengujian ini bertujuan untuk mengetahui perbedaan hasil extraksi pesan tersembunyi dengan dan tanpa kriptografi Triple-DES. Setelah dilakukan pengujian, maka diperoleh hasil bahwa hasil extraksi pesan tersembuyi tanpa kriptografi diperoleh

pesan plain text atau cleartext yang langsung dapat dibaca seperti ditunjukkan pada Gbr. 14, sedangkan pada extraksi pesan tersembunyi dengan kriptografi Triple-DES, maka diperoleh hasil bahwa pesan tidak langsung dapat dibaca jika password yang dimasukkan tidak sesuai dengan password sebelum penyisipan pesan seperti ditunjukkan pada Gbr. 15.



Gbr. 14 Extraksi pesan tanpa Kriptografi



Gbr. 15 Extraksi pesan dengan Kriptografi

Dari pengujian pada Gbr. 17 dan Gbr. 18 diperoleh informasi bahwa penyisipan pesan dengan kriptografi memberikan keamanan lebih jika dibandingkan dengan penyisipan tanpa kriptografi.

V. KESIMPULAN

Dari hasil pengujian sistem yang dilakukan, maka dapat diambil beberapa kesimpulan antara lain:

- Kapasitas metode PVD lebih besar jika dbandingkan dengan metode LSB 1 Bit dengan peningkatan rata-rata 311 % (3,11 kali).
- Kualitas gambar stego hasil PVD dan LSB 1 Bit tergolong sangat baik dengan ditunjukkan nilai PSNR > 60%.

- Hasil analisa histogram antara gambar asli, gambar stego PVD dan gambar stego LSB 1 Bit secara kasat mata memiliki kemiripan yang cukup tinggi.
- Penyisipan pesan dengan kriptografi memberikan keamanan lebih jika dbandingkan dengan penyisipan tanpa kriptografi.

REFERENSI

[1] Habes, Alkhraisat. (2006), Information Hiding in BMP image Implementation, Analysis and Evaluation, Eletronic Scientific Journal, Saint Petersburg, Russia.

[2] Maulana, Robbin. (2019), Steganografi Berbasis Citra Menggunakan Prosesor ARM7TDMI dan Algoritma LSB, Jurnal ElekFormatika : Vol.1 No.1, 2019

[3] Menezes; P. Van Oorschot and S. Vanstone., (1996), Handbook of Applied Cryptography, CRC Press.

[4] Morkel, T., Eloff dan Olivier, M.S. (2005), An Overview of Image Steganography, Proceedings of the Fifth Annual Information Security South Africa Conference(ISSA2005), Sandton, South Africa, (Published electronically).

[5] Munir, Rinaldi. (2005), Steganografi dan Watermarking, http://www.informatika.org/~rinaldi/Kriptografi/Steganografi%20dan %20Watermarking.pdf, tanggal akses 20 Juni 2010, .

[6] Prihanto, Agus. (2009), Penyembuyian dan Pengacakan Pesan Data Text Menggunakan Steganografi dan Kriptografi Triple DES pada image, Proceding Seminar Nasional Pengaman Jaringan - SNIPER, Banyuwangi.

[7] Wulandari, M., dkk (2015), Analisis Kualitas dan Kuantitas Steganografi dengan Interpolasi pada Citra Medis, Jurnal UGM : Vol.36, No.1, 2015.

[8] Wu, D.-C., & Tsai, W.-H. (2013). A Steganographic method for image by pixel-value differencing. Pattern Recognition Letter 24, 1613-1626