Implementasi Steganografi Dengan Metode Pixel Value Differencing (PVD) pada Gambar JPG dan PNG

Yonatan Firdaus[1], I Made Suartana[2],

[1]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]yonatanfirdaus@mhs.unesa.ac.id
[2]madesuartana@unesa.ac.id

***Abstrak*— Informasi dalam bentuk pesan tidak hanya disandikan, namun dapat juga disisipkan ke dalam citra digital. Teknik menyembunyikan atau menyisipkan pesan disebut steganografi. Steganografi merupakan metode yang digunakan untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui pihak yang tidak berhak mengetahuinya. Dalam steganografi terdapat beberapa metode yang dapat digunakan dalam mengamankan informasi dari suatu pihak yang tidak berhak mengetahuinya, salah satunya dengan menggunakan metode PVD (*Pixel Value Differencing*) yang dalam implementasinya memanfaatkan citra digital sebagai media penampung. Penelitian ini bermaksud menghitung kapasitas jumlah bit dan melihat pengaruh format gambar terhadap jumlah kapasitas bit yang dapat disisipi pesan. PVD yang digunakan adalah dengan dua blok piksel untuk mempertahankan kualitas citra hasil steganografi. Hasil dari penelitian ini menunjukkan kapasitas yang didapat pada gambar JPG dan PNG tidak berbeda signifikan. Kemudian juga didapat nilai PSNR (*Peak Signal to Noise Ratio*) dari gambar JPG dan PNG yang relatif sama diatas 40 dB. Namun metode PVD tidak dapat mengantisipasi perhitungan nilai piksel baru yang melebihi nilai maksimal warna 255 dan tidak memiliki ketahanan terhadap modifikasi hasil steganografi.**

***Kata Kunci*— Steganografi, Citra Digital, Pixel Value Differencing, Kapasitas, PSNR.**

I. PENDAHULUAN

Kerahasiaan suatu informasi kini telah menjadi suatu perhatian yang penting. Cara merahasiakan informasi terus dicari sebagai usaha menyembunyikan informasi dari pihak yang tidak berhak mengetahuinya. Salah satunya adalah dengan menggunakan suatu metode yang bertujuan mengacak pesan sebelum dikirimkan kepada penerima. Teknik penyandian ini dikenal dengan istilah kriptografi [1]. Teknik penyandian kriptografi ini terlalu menarik kecurigaan pihak-pihak yang tidak berhak mengaksesnya, dan banyak dari pihak ini lalu mencoba untuk membuka akses penyandian dari data [2]. Oleh karena itu dibutuhkan suatu cara lain yang tidak menimbulkan kecurigaan. Muncullah teknik baru dalam bidang ilmu keamanan data yang dikenal dengan steganografi. Teknik ini menyembunyikan atau menyisipkan data ke dalam sebuah citra digital.

Steganografi merupakan metode untuk menyembunyikan (*embedded*) informasi atau data ke dalam media lain misalnya teks, citra digital, suara dan video [2]. Maka dari itu dalam melakukan proses steganografi dibutuhkan dua properti, yaitu informasi dan media penampung. Citra digital sendiri telah menjadi media penampung yang populer, dengan alasan bahwa mata manusia tidak sensitif terhadap suatu modifikasi pada citra digital. Dalam steganografi terdapat beberapa metode yang dapat digunakan, yaitu *Least Significant Bit (LSB)*, *Redundant Pattern Encoding*, *Spread Spectrum* dan *Transformation*. Salah satu metode yang digunakan dalam penyisipan informasi ke dalam citra digital adalah metode PVD (*Pixel Value Differencing*). Metode ini menyisipkan pesan dengan mencari selisih dua piksel berdekatan dari media penampung [3]. Selisih ini selanjutnya digunakan untuk menentukan jumlah bit pesan yang dapat disisipkan. Metode PVD bekerja dengan cara membagi media penampung (*cover image*) menjadi blok-blok yang tidak saling tumpang tindih. Metode PVD dianggap dapat menyembunyikan lebih banyak jumlah data daripada metode LSB karena jumlah bit data lebih banyak bisa disembunyikan di area tepi daripada area halus. Umumnya, dalam sebuah *image* piksel-piksel menyebar secara berkelompok sehingga pada daerah halus (*smooth area*) didapati selisih antara piksel-piksel yang berdekatan memiliki nilai yang kecil. Namun, sebaliknya pada daerah piksel-piksel yang kontras (*contrast area*) memiliki nilai selisih yang besar [4]. Oleh karena itu, *image* dengan daerah halus yang luas hanya dapat disisipi sedikit pesan dan *image* dengan daerah kontras yang luas dapat disisipi lebih banyak pesan.

Penelitian mengenai steganografi yang menggunakan metode PVD telah banyak dikembangkan oleh para peneliti. Pada tahun 2018 Blerim Rexha dkk. melakukan penelitian dengan membandingkan parameter yang berbeda dari efisiensi metode LSB dan PVD. Hasil penelitian ini dalam menguji kapasitas atau jumlah informasi yang disembunyikan dalam kedua algoritma, menyebutkan bahwa PVD menyembunyikan lebih banyak data 50% lebih daripada LSB. Namun, mereka mengatakan nilai PSNR yang didapat menunjukkan PVD lebih kecil dari LSB [5].

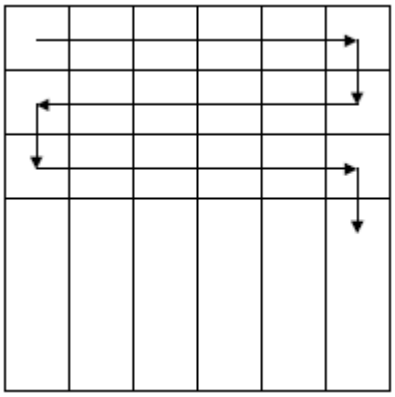
Pada tahun 2015 Tanmoy Halder dkk. melakukan penelitian dengan menggunakan pendekatan baru dari metode PVD. Mereka telah menggunakan tiga blok piksel yang tidak saling tumpang tindih untuk mengetahui lebih banyak selisih sebagai usaha meningkatkan kapasitas PVD. Berdasarkan hasil penelitian mereka berhasil menigkatkan kapasitas karena area tepi yang digunakan lebih banyak. Hal itupun berakibat terhadap kualitas gambar yang menurun, ini dibuktikan dari nilai PSNR yang didapat jauh lebih kecil dari hanya menggunakan dua blok piksel [6].

Pada penelitian ini bertujuan untuk mengetahui pengaruh format gambar terhadap kapasitas pesan yang dapat disisipkan dengan algoritma PVD. PVD yang digunakan adalah dengan dua blok piksel untuk mempertahankan kualitas citra hasil

steganografi yang didapat agar tidak menurun secara signifikan. Format gambar yang dipakai adalah JPG dan PNG, dengan kedua format tersebut memiliki jenis kompresi yang berbeda. Format JPG memiliki jenis kompresi *lossy*, sedangkan format PNG memiliki kompresi *lossless*. Pengujian dalam penelitian ini akan melingkupi pengujian kapasitas jumlah bit, pengujian nilai PSNR, pengujian kapasitas ukuran setelah disisipi untuk membandingkan kapasitas ukuran sebelum dan setelah mengalami proses steganografi. Citra hasil steganografi juga akan dilakukan pengujian modifikasi citra seperti *brightness*, *contrast* dan *resize* untuk melihat ketahanan metode PVD terhadap perubahan yang terjadi.

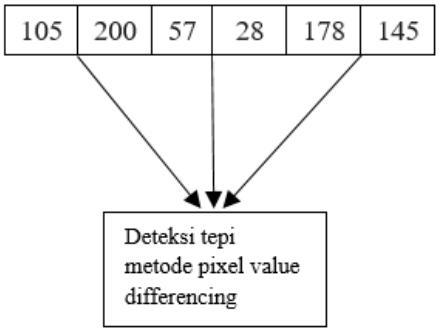
II. METODOLOGI

Penelitian steganografi ini menggunakan metode PVD (*Pixel Value Differencing*) untuk melakukan penyisipan dan pengekstrakan pesan dalam media penampung citra digital. Metode PVD membagi piksel-piksel gambar menjadi dua blok piksel yang tidak saling tumpang tindih. Perbedaan nilai blok-blok piksel ini digunakan untuk menentukan besarnya bit yang akan disisipkan dalam area tepi kedua piksel. PVD menggunakan skema Wu dan Tsai untuk mengetahui letak range selisih kedua piksel. Skema Wu dan Tsai yang dipakai pada penelitian ini yaitu
R={[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}.



Gbr. 1 Proses penyisipan secara zigzag

PVD menyisipkan pesan ke dalam piksel gambar dilakukan secara zigzag seperti ditunjukkan pada Gbr. 1.



Gbr. 2 Deteksi tepi metode PVD

Dari Gbr. 2 dijelaskan dalam enam piksel gambar, piksel-piksel ini kemudian dibagi menjadi dua blok piksel berdekatan sehingga kita dapat menemukan tiga tepi yang dapat disisipi pesan. Metode *Pixel Value Differencing* mengambil dua piksel berdekatan (p dan q) dari gambar, selisih nilai (d) dihitung melalui persamaan (1) berikut.

$$d = \begin{cases} p - q & \text{Jika } p > q \\ q - p & \text{Jika } q > p \end{cases} \quad (1)$$

Nilai (d) berkisar 0 sampai 255. Pada dua piksel gambar yang memiliki perbedaan warna halus akan mendapat (d) kecil, sedangkan perbedaan yang kontras akan mendapat (d) besar. Skema Wu dan Tsai lalu digunakan untuk menentukan *range* dari nilai (d). Skema ini juga mendapatkan batas atas (Ui) dan batas bawah (Li). Selanjutnya mencari rentang nilai (Wi) dengan persamaan (2) dibawah ini.

$$Wi = (Ui - Li + 1) \quad (2)$$

Rentang nilai ini mempengaruhi kapasitas jumlah bit yang akan dapat ditampung dalam blok-blok piksel. Blok piksel dengan perbedaan halus akan dapat menampung sedikit bit pesan. Sedangkan blok piksel yang memiliki kontras tinggi dapat menampung lebih banyak bit pesan. Kapasitas jumlah bit (t) dihitung dalam persamaan (3).

$$t = \log_2 (Wi) \quad (3)$$

Dari persamaan (3) berhasil didapat nilai (t) yang merupakan jumlah bit yang dapat diambil dari pesan. Biner pesan akan diambil sebesar (t) bit lalu diubah ke bentuk desimal (b). Selisih baru (d') dihitung dengan persamaan (4).

$$d' = Li + b \quad (4)$$

Setelah didapatkan selisih baru, nilai piksel baru dapat dihitung dengan menghitung nilai (m) terlebih dahulu melalui persamaan (5). Kemudian hasil ini akan digunakan dalam perhitungan untuk mendapatkan nilai piksel baru yang digunakan untuk menggantikan piksel lama. Sehingga akhirnya didapatkan piksel baru yang membentuk gambar.

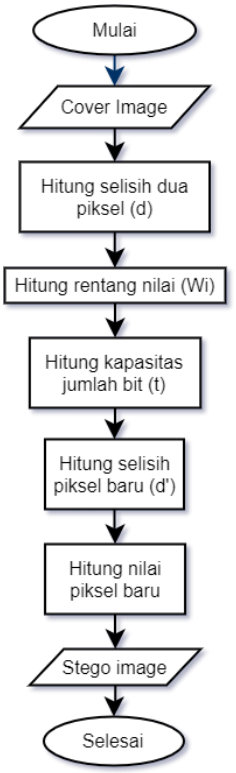
$$m = d' - d \quad (5)$$

Persamaan (6) untuk menghitung piksel baru.

$$p',q' = \begin{cases} \left(p + \left\lceil \frac{m}{2} \right\rceil, q - \left\lfloor \frac{m}{2} \right\rfloor\right) & \text{Jika } p \geq q \text{ dan } d' > d \\ \left(p - \left\lceil \frac{m}{2} \right\rceil, q + \left\lfloor \frac{m}{2} \right\rfloor\right) & \text{Jika } p < q \text{ dan } d' > d \\ \left(p - \left\lceil \frac{m}{2} \right\rceil, q + \left\lfloor \frac{m}{2} \right\rfloor\right) & \text{Jika } p \geq q \text{ dan } d' \leq d \\ \left(p - \left\lceil \frac{m}{2} \right\rceil, q - \left\lfloor \frac{m}{2} \right\rfloor\right) & \text{Jika } p < q \text{ dan } d' \leq d \end{cases} \quad (6)$$

A. *Proses Penyisipan PVD*

Tahap proses penyisipan merupakan proses penyisipan *file* pesan ke dalam gambar.



Gbr. 3 Alur proses penyisipan metode PVD

Berikut ini merupakan langkah-langkah dalam proses penyisipan data ke dalam gambar :

1. Memasukkan *cover image* yang akan disisipi pesan. *Cover image* yang dipakai memiliki format .jpg dan .png.
2. Mambagi piksel-piksel gambar menjadi dua blok yang tidak saling tumpang tindih dan menghitung selisih kedua piksel dengan memakai persamaan (1). Dimisalkan blok piksel pertama dari Gbr. 2 selisihnya dapat dihitung sebagai berikut : d = 200 – 105 = 95.
3. Menentukan batas atas dan batas bawah dengan memakai skema Wu dan Tsai untuk menghitung rentang nilai dari piksel. Dalam skema Wu dan Tsai, nilai d = 95 memiliki batas atas Ui = 127 dan batas bawah Li = 64. Melalui persamaan (2) Wi = 127 - 64 + 1 = 64.
4. Menghitung kapasitas jumlah bit yang akan dapat disisipkan dalam blok piksel. Kapasitas jumlah bit dihitung dalam nilai (t) pada persamaan (3). Dimisalkan t = $\log_2 64$ maka didapat hasil t = 6, yang berarti jumlah bit yang dapat disisipkan dalam area blok piksel sebesar 6 bit data.
5. Menghitung nilai selisih baru dengan perhitungan sesuai persamaan (4). Untuk meghitung selisih baru harus mengambil pesan yang sudah diubah ke bentuk biner sebesar (t) bit dan mengubahnya ke bentuk desimal. Dimisalkan pesan yang akan disisipkan adalah angka 154 lalu diubah ke bentuk biner menjadi 10011010, lalu mengambil sebanyak 6 bit menjadi b = 100110 = 38. Selanjutnya selisih baru yang didapat sebesar d' = 64 + 38 = 102.
6. Menghitung nilai piksel baru dilakukan dengan mencari nilai (m) dengan persamaan (5). Dari hasil nilai d dan d' yang telah didapat, perhitungan m = 102 – 95 = 7. Setelah mendapatkan nilai (m) perhitungan nilai piksel baru dilakukan dengan kondisi yang memenuhi persamaan (6). Perhitungan sebagai berikut :

$$p', q' = 105 - \left\lfloor \frac{7}{2} \right\rfloor, 200 + \left\lceil \frac{7}{2} \right\rceil = (105 - 4), (200 + 3) = 101, 203$$

Nilai piksel baru yang didapat akan menggantikan piksel lama dan menghasilkan *stego image*.

101	203

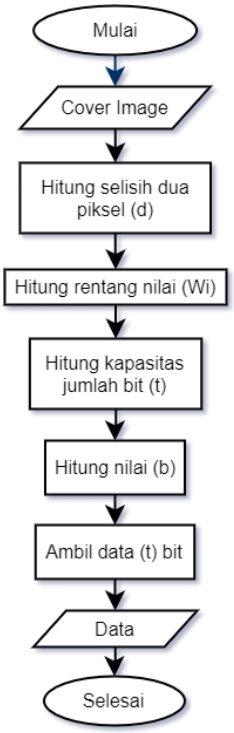
Gbr. 4 Nilai blok piksel baru

Sisa 2 bit pesan akan disisipkan dalam blok piksel selanjutnya.

7. Proses tersebut akan terus diulang sampai semua pesan berhasil disisipkan.

B. Proses Pengekstrakan PVD

Proses pengekstrakan merupakan proses membaca dan mengambil pesan dari dalam gambar.



Gbr. 5 Alur proses pengekstrakan metode PVD

Berikut ini merupakan langkah-langkah dalam proses pengekstrakan data dari gambar :

1. Memasukkan *stego image* yang telah berisi pesan.
2. Mambagi piksel-piksel gambar menjadi dua blok yang tidak saling tumpang tindih dan menghitung selisih kedua piksel dengan memakai persamaan (1). Dimisalkan piksel

yang telah disisipi pesan dari Gbr. 4 dapat dihitung menjadi berikut : d = 203 – 101 = 102.

3. Menentukan batas atas dan batas bawah dengan memakai skema Wu dan Tsai untuk menghitung rentang nilai dari piksel. Dalam skema Wu dan Tsai, nilai d = 102 memiliki batas atas Ui = 127 dan batas bawah Li = 64. Melalui persamaan (2) Wi = 127 - 64 + 1 = 64.
4. Menghitung kapasitas jumlah bit yang akan dapat diambil dari blok piksel. Kapasitas jumlah bit dihitung dalam nilai (t) pada persamaan (3). Dimisalkan t = $\log_2$ 64 maka didapat hasil t = 6, yang berarti jumlah bit yang dapat diambil dari area blok piksel sebesar 6 bit data.
5. Menghitung nilai (b) dengan persamaan (4) maka dapat dihitung dengan b = d – Li = 102 – 64 = 38.
6. Mengubah b menjadi biner dan mengambil (t) bit pesan. b = 38 = 100110.
7. Proses tersebut akan diulang sampai semua pesan berhasil diekstrak.

III. Hasil dan Pembahasan

Penelitian ini dikembangkan/dibuat dengan menggunakan *software* Visual Studio 2019 dengan bahasa pemrograman C#. Berikut merupakan tampilan gambar sebelum dan sesudah melalui proses steganografi metode PVD.

Gbr. 6 Tampilan cover image dan stego image

A. *Data*

Data yang digunakan sebagai media penampung dalam penelitian ini merupakan gambar RGB 24 Bit dengan format yaitu .jpg dan .png. Gambar tersebut memiliki beberapa dimensi seperti ditunjukkan pada Tabel I. Sedangkan untuk pesan yang akan disisipkan menggunakan *file* teks dengan format .txt seperti ditunjukkan Gbr. 7.

Gbr. 7 Pesan yang disisipkan

Gbr. 8 Animal

Gbr. 9 Fruits

Gbr. 10 House

Gbr. 11 Umbrella

Tabel I
Data Gambar Penelitian

No	Nama Cover Image	Dimensi (*Pixel*)	Kapasitas Ukuran
1	Animal.jpg	200 x 200	28 KB
2	Animail.png	200 x 200	113 KB
3	Fruits.jpg	400 x 400	91 KB
4	Fruits.png	400 x 400	503 KB
5	House.jpg	600 x 600	153 KB
6	Huose.png	600 x 600	835 KB
7	Umbrella.jpg	800 x 800	303 KB
8	Umbrella.png	800 x 800	1.66 MB

B. *Hasil Pengujian*

1. Pengujian Kapasitas

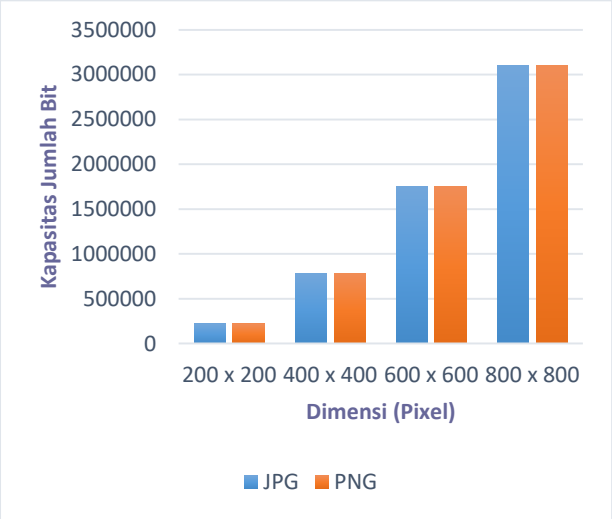
Tahap awal dalam pengujian steganografi dengan metode PVD dalam penelitian ini dimulai dari pengujian kapasitas. Pengujian kapasitas dilakukan pada gambar yang akan dijadikan *cover image* sebelum proses penyisipan pesan. Pengujian kapasitas bertujuan untuk menghitung maksimal kapasitas ruang dalam gambar yang dapat disisipi bit pesan. Dengan demikian, diketahui maksimal kapasitas jumlah bit yang dapat ditampung dan dapat memperkirakan pemilihan ukuran pesan tidak melebihi maksimal kapasitas yang telah didapat. Pengujian

ini juga sebagai alat ukur untuk melihat pengaruh perbedaan format gambar yang dipakai terhadap jumlah kapasitas yang akan didapat. Pengujian ini dilakukan pada gambar JPG dan PNG. Tabel II menunjukkan hasil pengujian kapasitas yang telah dilakukan pada sampel data *cover image* dari Tabel I.

TABEL II
PENGUJIAN KAPASITAS

No	Nama Cover Image	Kapasitas Jumlah Bit
1	Animal.jpg	218167 Bit
2	Animail.png	218912 Bit
3	Fruits.jpg	777688 Bit
4	Fruits.png	784405 Bit
5	House.jpg	1754438 Bit
6	Huose.png	1751800 Bit
7	Umbrella.jpg	3102069 Bit
8	Umbrella.png	3096302 Bit

Dari Tabel II, dapat diketahui bahwa format gambar mempengaruhi kapasitas yang didapat. Dalam cover JPG dan PNG terdapat perbedaan kapasitas jumlah bit. Pengujian pertama pada Gbr. 7 memiliki kapasitas jumlah bit seperti ditunjukkan pada Tabel II sehingga didapat perbedaan sebesar 745 bit, pengujian kedua pada Gbr. 8 memiliki perbedaan 6717 bit, ketiga pada Gbr. 9 didapat perbedaan 2638 bit dan Gbr. 10 didapat perbedaan 5767 bit.



Gbr. 12 Grafik pengujian kapasitas bit

Dalam Gbr.12, secara umum kapasitas yang didapat tidak berbeda signifikan pada kedua format. Kapasitas PNG lebih besar pada resolusi 200 dan 400 piksel sedangkan kapasitas JPG lebih besar pada resolusi 600 dan 800 piksel.

2. Pengujian PSNR

Setelah proses pengujian kapasitas selesai, tahap kedua yaitu penyisipan pesan ke dalam gambar. Pesan yang digunakan merupakan *file* teks berformat .txt. Hasil dari penyisipan dapat dilihat seperti ditunjukkan oleh Tabel III. Kemudian pengujian PSNR dilakukan untuk menghitung tingkat distorsi dari gambar hasil proses steganografi yang telah disisipi pesan terhadap gambar asli. Tujuan dari pengujian ini untuk menganalisa kualitas citra hasil steganografi dengan metode PVD.

PSNR diukur dalam satuan Desibel (dB), semakin besar nilai PSNR maka distorsi dari gambar asli dan gambar hasil steganografi semakin kecil sehingga kualitas gambar masih terjaga, sedangkan semakin kecil nilai PSNR, menandakan distorsi yang terjadi pada kedua gambar semakin besar. Dalam mencari nilai PSNR dibutuhkan nilai MSE (*Mean Square Error*) yang digunakan dalam menyatakan penyimpangan yang terjadi. Persamaan (7) untuk mencari nilai MSE sebagai berikut :

$$MSE = \frac{1}{MxN}\sum_{x=1}^{M}\sum_{y=1}^{N}[I(x,y) - K(x,y)]^2 \quad (7)$$

Keterangan :

I (x, y) = data *cover image*
K (x, y) = data *stego image*
M = lebar *image*
N = tinggi *image*

Persamaan (8) untuk mencari nilai PSNR sebagai berikut :

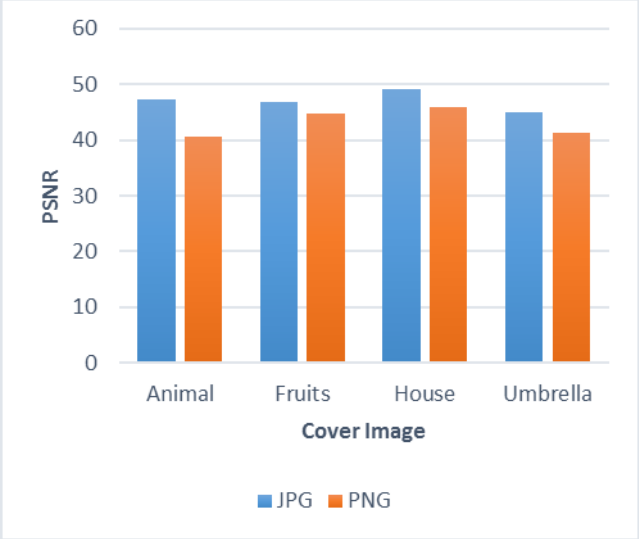
$$PSNR = 10\ Log_{10}(255^2/MSE) \quad (8)$$

Tabel III menunjukkan nilai PSNR yang didapat setelah proses penyisipan pesan. Meski di Tabel II nilai kapasitas pesan yang dapat disisipkan tidak jauh berbeda tetapi rata-rata pesan yang disisipkan pada file PNG lebih besar dari JPG untuk kualitas PSNR yang relatif sama seperti ditunjukkan pada grafik pada Gbr. 13. Dalam pengujian ini pesan berhasil disisipkan dan didapat nilai PSNR dari 40.51 dB sampai 49.27 dB yang menyatakan bahwa tidak ada perbedaan signifikan antara gambar sebelum dan sesudah dilakukan steganografi. Dalam penelitian [7] kualitas dan kemiripan gambar hasil proses steganografi dengan gambar asli masih dapat dikatakan dalam kondisi baik jika nilai PSNR yang didapat berada diatas 40 dB.

TABEL III
PENGUJIAN PSNR

No	Ukuran Pesan	Hasil	PSNR
1	7.24 KB	Berhasil	47.3857630203737 dB

No	Ukuran Pesan	Hasil	PSNR
2	10.8 KB	Berhasil	40.5187233438011 dB
3	19.1 KB	Berhasil	46.831852485013 dB
4	26.9 KB	Berhasil	44.8044277202406 dB
5	42.5 KB	Berhasil	49.2799985772828 dB
6	85 KB	Berhasil	45.9470501734553 dB
7	130 KB	Berhasil	45.0238811054675 dB
8	308 KB	Berhasil	41.3982451392538 dB



Gbr. 13 Grafik PSNR

3. Pengujian Kapasitas Ukuran

Hasil steganografi tersebut lalu disimpan menjadi *file stego image* dalam format PNG agar tidak terkompresi. Hal ini tentu menimbulkan peningkatan ukuran yang terjadi karena gambar telah terisi pesan. Pengujian kapasitas ukuran diperlukan untuk membandingkan ukuran gambar asli dan gambar hasil proses steganografi. Perubahan yang terlalu jauh tentu akan menimbulkan kecurigaan pihak lain.

TABEL IV
PENGUJIAN KAPASITAS UKURAN

No	Ukuran Cover Image	Ukuran Pesan	Ukuran Stego Image
1	28 KB	7.24 KB	103 KB
2	113 KB	10.8 KB	117 KB
3	91 KB	19.1 KB	453 KB
4	503 KB	26.9 KB	505 KB
5	153 KB	42.5 KB	759 KB
6	835 KB	85 KB	888 KB
7	303 KB	130 KB	1.65 MB
8	1.66 MB	308 KB	1.84 MB

Berdasarkan Tabel IV dapat diketahui terjadi peningkatan ukuran. Pada uji coba pertama mengalami peningkatan 75 KB dari 7.24 KB pesan yang disisipkan, uji kedua 4 KB dari 10.8 KB pesan, ketiga 361 KB dari 19.1 KB pesan, keempat 2 KB dari 29.9 KB pesan, kelima 606 KB dari 42.5 KB pesan, keenam 53 KB dari 85 KB pesan, ketujuh 1.35 MB dari 130 KB pesan dan kedelapan 220 KB dari 308 KB pesan. Peningkatan tinggi terjadi pada gambar JPG, sedangkan gambar PNG tidak mengalami peningkatan yang terlalu tinggi.

4. Pengujian Pengekstrakan

Setelah berhasil disisipkan, pesan perlu diekstrak kembali untuk dapat dibaca oleh penerima. Uji coba dalam mengekstrak kembali pesan yang telah disisipkan ditunjukkan pada tabel dibawah ini.

TABEL V
PENGEKSTRAKAN PESAN

No	Nama Stego Image	Hasil
1	Stego1.png	Pesan berhasil diekstrak
2	Stego2.png	Pesan gagal diekstrak
3	Stego3.png	Pesan berhasil diekstrak
4	Stego4.png	Pesan berhasil diekstrak
5	Stego5.png	Pesan berhasil diekstrak
6	Stego6.png	Pesan berhasil diekstrak
7	Stego7.png	Pesan berhasil diekstrak
8	Stego8.png	Pesan gagal diekstrak

Hasil pengekstrakan pesan menggunakan metode PVD dari dalam *stego image* seperti ditunjukkan Tabel V, menyatakan bahwa beberapa pesan berhasil diekstrak. Namun dalam percobaan ke 2 dan 8, pesan tidak dapat diekstrak kembali. Hal ini terjadi karena terdapat kelemahan dalam metode PVD, metode ini tidak dapat mengantisipasi perhitungan nilai piksel baru yang melebihi nilai maksimal warna 255. Penelitian [8] mengatakan hal tersebut terjadi karena nilai-nilai yang berada diluar jangkauan (*out of range*) yaitu berada diluar [0,255] setelah proses penyisipan..

5. Pengujian Modifikasi Hasil Steganografi

Pada *stego image* juga akan dilakukan pengujian modifikasi hasil steganografi yang bertujuan untuk melihat

ketahanan metode PVD terhadap perubahan pada gambar hasil proses steganografi. Modifikasi hasil steganografi ini mencakup pengujian *brightness*, *contrast* dan *resize*. Masing-masing pengujian ini dilakukan pada beberapa peningkatan dan penurunan modifikasi. Pengujian ini dilakukan dengan menggunakan *software* Adobe Photoshop untuk mendapatkan hasil yang akurat.

TABEL VI
PENGUJIAN BRIGHTNESS

No	Nama Stego Image	Tingkat Brigtness	Hasil
1	Stego1.png	150	Pesan tidak dapat diekstrak
2	Stego2.png	100	Pesan tidak dapat diekstrak
3	Stego3.png	50	Pesan tidak dapat diekstrak
4	Stego4.png	25	Pesan tidak dapat diekstrak
5	Stego5.png	-25	Pesan tidak dapat diekstrak
6	Stego6.png	-50	Pesan tidak dapat diekstrak
7	Stego7.png	-100	Pesan tidak dapat diekstrak
8	Stego8.png	-150	Pesan tidak dapat diekstrak

TABEL VII
PENGUJIAN CONTRAST

No	Nama Stego Image	Tingkat Contrast	Hasil
1	Stego1.png	100	Pesan tidak dapat diekstrak
2	Stego2.png	75	Pesan tidak dapat diekstrak
3	Stego3.png	50	Pesan tidak dapat diekstrak
4	Stego4.png	25	Pesan tidak dapat diekstrak
5	Stego5.png	-25	Pesan tidak dapat diekstrak
6	Stego6.png	-50	Pesan tidak dapat diekstrak
7	Stego7.png	-75	Pesan tidak dapat diekstrak
8	Stego8.png	-100	Pesan tidak dapat diekstrak

TABEL VIII
PENGUJIAN RESIZE

No	Ukuran Gambar		Perubahan Ukuran	Hasil
	Sebelum	Sesudah		
1	200 x 200	180 x 180	10%	Gagal diekstrak
2	200 x 200	170 x 170	15%	Gagal diekstrak
3	400 x 400	320 x 320	20%	Gagal diekstrak
4	400 x 400	300 x 300	25%	Gagal diekstrak
5	600 x 600	420 x 420	30%	Gagal diekstrak
6	600 x 600	390 x 390	35%	Gagal diekstrak
7	800 x 800	560 x 560	40%	Gagal diekstrak
8	800 x 800	440 x 440	45%	Gagal diekstrak

Hasil pengujian modifikasi hasil steganografi yang telah dilakukan seperti ditunjukkan pada Tabel VI, *stego image* dilakukan pengujian tingkat *brightness* dengan peningkatan 150 sampai penurunan -150, Lalu dalam Tabel VII dilakukan uji coba peningkatan *contrast* dari 100 sampai -100 dan Tabel VIII pengujian *resize* pada beberapa persen perubahan ukuran. Hasil pengujian ini, pesan tidak dapat diekstrak kembali setelah terjadi perubahan pada *stego image*.

IV. KESIMPULAN

Berdasarkan dari hasil penelitian yang sudah dilakukan oleh peneliti maka dapat diambil kesimpulan bahwa metode PVD digunakan untuk menghitung dan mengukur kapasitas jumlah bit yang dapat disisipi pesan dalam sebuah *cover image*. Format gambar berpengaruh pada jumlah kapasitas yang didapat, sehingga dalam pengujian kapasitas didapat hasil kapasitas PNG lebih besar pada gambar dengan resolusi 200 dan 400 piksel, sedangkan JPG lebih besar pada gambar dengan resolusi 600 dan 800 piksel. Meski kapasitas pesan yang dapat disisipkan tidak jauh berbeda tetapi rata-rata pesan yang disisipkan pada gambar PNG lebih besar dari JPG untuk kualitas PSNR yang relatif sama. Dari beberapa pengujian yang dilakukan, juga berhasil didapat nilai PSNR dari 40.51 dB sampai 49.27 dB yang artinya tidak ada perbedaan signifikan antara gambar sebelum dan sesudah dilakukan steganografi. Kemudian pengujiaan kapasitas ukuran gambar JPG mengalami peningkatan yang tinggi, sedangkan gambar PNG tidak mengalami peningkatan yang tinggi. Namun dalam pengekstrakan pesan, PVD tidak dapat mengantisipasi perhitungan nilai piksel baru yang melebihi nilai warna [0,255].

Metode PVD (*Pixel Value Differencing*) tidak memiliki ketahanan dari modifikasi citra, yang mana dari hasil pengujian *Brightness*, *Contrast* dan *Resize* yang telah dilakukan terhadap gambar hasil steganografi (*stego image*) dengan tingkat yang telah ditentukan, memiliki hasil bahwa

pesan tidak dapat dikembalikan, karena piksel gambar tersebut telah mengalami perubahan tingkat warna dan ukuran.

UCAPAN TERIMA KASIH

Puji syukur penulis ucapkan kepada Tuhan YME yang telah memberikan kasih, hikmat dan penyertaan-Nya sehingga penulis dapat menyelesaikan jurnal ini. Terimakasih juga penulis ucapkan kepada semua pihak yang telah mendukung dalam penyusunan jurnal ini.

REFERENSI

[1] T. E. Tarigan, "Algoritma MEoF (Modifikasi End of File) Untuk Steganografi Pada Citra Bitmap 24 Bit," 2015.

[2] R. Rahim, "Penyisipan Pesan Dengan Algoritma Pixel Value Differencing Dengan Algoritma Caesar Chiper Pada Proses Steganografi," *Journal TIMES,* vol. V, no. 1, pp. 6-11, 2016.

[3] D.-C. Wu dan W.-H. Tsai, "A Steganographic Method For Images by Pixel-Value Differencing," *Elsevier,* pp. 1613-1626, 2003.

[4] R. S. Guritman dan H. T. Natalisa, "Perbaikan Dan Evaluasi Algoritma Pixel Value Differencing (PVD)," *Jurnal Mat Stat,* vol. 9, no. 2, pp. 143-156, 2009.

[5] B. Rexha, P. Rama, B. Krasniqi dan G. Seferi, "Efficiency of LSB and PVD Algorithms Used in Steganography," *International Journal of Computer Engineering and Information Technology,* vol. 10, no. 2, pp. 20-29, 2018.

[6] T. Halder, S. Karforma dan R. Mandal, "A Novel Data Hiding Approach by Pixel-Value-Difference Steganography and Optimal Adjustment to Secure E-Governance Documents," *Indian Journal of Science and Technology,* vol. Vol 8 (16), pp. 1-7, 2015.

[7] M. Hamdani dan G. N. Samosir, "Implementasi Steganografi Untuk Keamanan Pengiriman Citra Digital Menggunakan Merode DCT (Discrete Cosine Transform)," *Sinusoida,* vol. XX, no. 2, pp. 42-52, 2018.

[8] M. Azhari, Pemanfaatan Filterisasi Untuk Meningkatkan Daya Tampung Pesan Pada Steganografi Pixel Value Differences (PVD), Bogor: Institut Pertanian Bogor, 2012.