ISSN : 2356 – 5195
Online ISSN: 2654 - 8704

Perbandingan Metode Steganografi Berdasarkan Waktu, Kualitas dan Ukuran Gambar

Bayu Kumoro Yakti*[1], Ragiel Hadi Prayitno[2], Fauziah[3]
[1]Fakultas Teknologi Industri, Teknik Elektro, Universitas Gunadarma, [2,3]Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma
E-mail: [1*]**Bayuyakti@staff.gunadarma.ac.id**, [2]ragielhp@staff.gunadarma.ac.id, [3]fauziah87@staff.gunadarma.ac.id

Abstrak

Citra digital adalah citra dalam bentuk format digital atau media digital seperti harddisk. Citra digital terdiri dari bit (0 atau 1) yang disebut piksel dan memiliki kapasitas yang tinggi untuk menyimpan data dan informasi. Teknik steganografi berusaha menyembunyikan keberadaan data yang bersifat rahasia. Teknik Steganografi yang sempurna dapat menyisipkan pesan rahasia dalam gambar sampul dengan keamanan tingkat tinggi. Informasi, data atau pesan rahaisa tersebut akan dimanipulasi sehingga tidak dapat dideteksi oleh mata manusia. Least Significant Bit (LSB), Pixel Value Differencing (PVD), dan Chinese Remainder Theorem (CRT) merupakan metode yang dilakukan pada penelitian ini. Penelitian ini membandingkan metode tersebut dengan 3 parameter yaitu: Peak Signal to Noise Ratio (PSNR) untuk melihat nilai perbandingan gambar stego (gambar yang sudah disisipkan) dan gambar sampul, waktu proses pada setiap metode dan ukuran gambar stego dan gambar asli. Setiap metode akan menggunakan gambar yang sama dengan tiga resolusi berbeda yaitu 640x480, 800x600, 1280x720. Ketiga resolusi tersebut, masing-masing metode akan menggunakan PSNR sebagai keluaran dari penelitian ini. Hasil percobaan menunjukkan bahwa metode LSB memiliki hasil terbaik pada tiga resolusi pertama.

Kata Kunci*— Penyembunyian Informasi, PSNR, Resolusi, Steganografi*

Abstract

Digital images are images in digital format or digital media such as hard disks. Digital images consist of bits (0 or 1) called pixels and have a high capacity to store data and information. Steganography techniques try to hide the existence of confidential data. The perfect Steganography technique can insert a secret message in the cover image with a high level of security. The information, data or secret messages will be manipulated so that they cannot be detected by the human eye. Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Chinese Remainder Theorem (CRT) are the methods used in this study. This study compares the method with 3 parameters, namely: Peak Signal to Noise Ratio (PSNR) to see the comparison value of the stego image (pasted image) and the cover image, processing time for each method and the size of the stego image and the original image. Each method will use the same image with three different resolutions namely 640x480, 800x600, 1280x720. The three resolutions, each method will use PSNR as the output of this study. The experimental results show that the LSB method has the best results in the first three resolutions.

Keywords*— Information Hiding, PSNR, Resolution, Steganography*

1. PENDAHULUAN

Gambar digital adalah snapshot elektronik yang diambil dari sebuah adegan atau dipindai dari dokumen, seperti foto, manuskrip, teks tercetak, dan karya seni. Citra digital memiliki kapasitas yang tinggi untuk menyimpan data dan informasi. Citra digital diambil sampelnya dan dipetakan sebagai kisi titik atau elemen gambar (piksel). Setiap piksel diberi nilai (hitam, putih, nuansa abu-abu atau warna), yang direpresentasikan dalam kode biner (nol dan satu). Digit biner ("bit") untuk setiap piksel disimpan secara berurutan oleh komputer dan direduksi menjadi representasi matematis (dikompresi). Bit-bit ini kemudian dibaca dan diterjemahkan oleh komputer untuk menghasilkan versi analog untuk ditampilkan atau dicetak [1]. Resolusi menggambarkan tingkat detail dari gambar sampai resolusi yang lebih tinggi sehingga lebih banyak detail gambar. Dalam pencitraan digital, resolusi sering diukur sebagai jumlah piksel. Piksel (kependekan dari elemen gambar) adalah satu titik atau kotak kecil dalam gambar grafik yang disimpan dalam kotak persegi panjang yang tertata. Semakin banyak piksel yang digunakan untuk merepresentasikan suatu gambar, semakin dekat hasilnya dapat menyerupai analog aslinya [2]. Teknik steganografi berusaha menyembunyikan keberadaan data yang bersifat rahasia. Teknik ini secara sempurna menutup pesan rahasia dalam gambar pembawa dengan keamanan gambar yang tinggi. Dalam steganografi, penggunaan citra digital adalah yang paling umum. Informasi akan dimanipulasi, oleh karena itu, tidak dapat dideteksi oleh mata manusia. Steganografi merupakan salah satu dari sekian banyak teknik yang digunakan untuk menyembunyikan keberadaan informasi rahasia di dalam suatu objek [3].

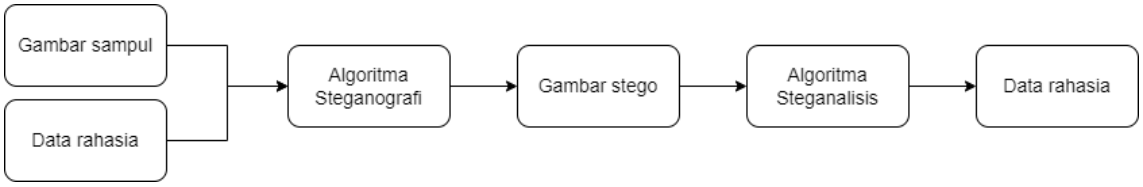
Data berhasil disembunyikan apabila suatu teknik dapat menyematkan data rahasia tanpa mengubah gambar sampul dan mengekstrak informasi tersembunyi dari gambar dengan integritas pengetahuan tingkat tinggi [3]. Menyembunyikan data rahasia dalam gambar digital akan mengubah kualitas gambar. Oleh karena itu, ketika membuat metode pengumpulan pesan, banyak kriteria seperti *fidelity*, *robustness*, dan *recovery* harus diperhitungkan. *Fidelity* mempertahankan tampilan gambar stego setelah pesan tersembunyi ditambahkan, karena memiliki sedikit perbedaan dalam hal kualitas output. Dalam *robustness*, pesan yang disembunyikan harus cukup kokoh untuk mencegah berbagai manipulasi yang dilakukan pada data, karena tujuan utama dari metode steganografi adalah untuk melindungi data yang bersifat rahasia. Setelah pemulihan, data yang disembunyikan harus dapat dibuka kembali karena tujuan steganografi, yaitu menyembunyikan dan mengambil informasi untuk digunakan lebih lanjut [4]. Tiga jenis metode yang digunakan dalam penelitian ini adalah *Least Significant Bit* (LSB), *Pixel Value Differencing* (PVD), dan *Chinese Remainder Theorem* (CRT) [5].

Tujuan dari penelitian ini adalah untuk membandingkan metode steganografi yang diproses untuk mengetahui kelebihan dan kekurangan masing-masing metode. Selama percobaan, gambar dengan pesan tersembunyi akan dibandingkan dengan gambar asli tanpa data yang disematkan. Penelitian ini menggunakan software MATLAB pada Macbook Air MacOS Mojave versi 10.14.6 sebagai alat bantu untuk membandingkan performa dan menghasilkan PSNR, waktu dari awal penyisipan pesan rahasia dan ekstraksi serta ukuran citra pada masing-masing metode.

2. METODE PENELITIAN

2.1. Steganografi

Steganografi bermanfaat di bidang teknologi informasi untuk komunikasi yang aman. Steganografi berlaku untuk bidang berikut: Penyimpanan data rahasia dan komunikasi rahasia yang efisien, Perlindungan perubahan data dan Sistem Basis Data Media [3]. Steganografi menjaga integritas data, artinya tidak akan ada modifikasi konten informasi selama komunikasi. Alur steganografi secara umum ditunjukkan pada gambar 1.



Gambar 1. Alur Steganografi

2.2. Steganografi metode LSB

Metode LSB menggunakan piksel gambar untuk menyembunyikan data rahasia. Setiap bit data rahasia akan menggantikan bit terakhir pada piksel. Gambar sampul digunakan untuk menyembunyikan pesan rahasia. Teknik steganografi yang paling banyak digunakan saat ini adalah LSB [6]. Bit paling kecil dari gambar sampul digantikan dengan data rahasia yang akan disematkan. Metode LSB mempunyai kelebihan dan kekurangan. Kelebihannya adalah mudah diterapkan, Sedikit perubahan pada gambar dan algoritma yang sederhana. Kekurangannya adalah mudah diserang. Untuk mencontohkan teknik LSB, berikut adalah gambar sampul yang sudah dikonversikan ke bit biner:

(00001010 00111010 01110100)

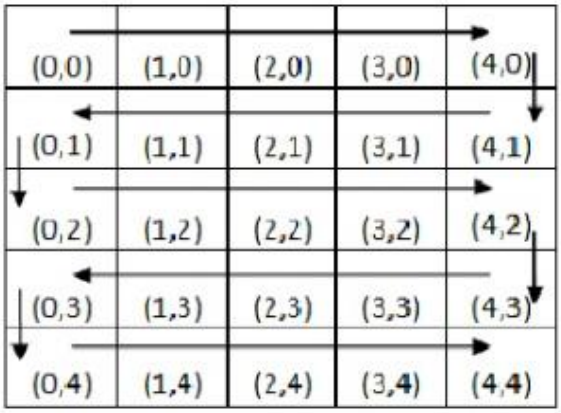
Pesan rahasia (111) akan disisipkan, nilai piksel yang dihasilkan setelah disisipkan adalah:

(00001011 00111011 01110101)

Bit yang digaris bawahi menunjukkan bahwa bit diubah dari nilai aslinya. Hanya ada tiga bit pada gambar sampul yang dimodifikasi dalam proses ini. Metode ini dapat dilakukan steganografi pada bit paling kecil (bit ke-8) sampai dengan bit terbesar (bit ke-1). Metode ini dapat diperluas lebih lanjut untuk menyisipkan data rahasia dalam bit ke-n untuk meningkatkan kapasitas informasi rahasia. Akan tetapi gambar stego dapat menyebabkan banyak distorsi pada jika penyisipan disisipkan pada bit ke-6 sampai bit ke-1 [6].

2.3. Steganografi metode PVD

Teknik PVD merupakan metode steganografi yang didasarkan pada perbedaan nilai piksel dari dua piksel yang berdekatan. Metode ini dikembangkan untuk meningkatkan kapasitas pesan dan mengurangi tingkat distorsi pada steganografi. Metode tersebut menyembunyikan data rahasia di blok yang tidak tumpang tindih dari dua piksel berturut-turut dengan memanipulasi nilai perbedaan. Pada gambar sampul, untuk blok piksel berdekatan, nilai selisih di dapat diperoleh dengan mengurangkan nilai piksel berdekatan dan semua nilai perbedaan terletak diantara -255 dan 255 oleh karena itu $| d_i |$ berkisar dari 0 hingga 255. Oleh karena itu PVD dapat menyisipkan data dalam jumlah besar tanpa banyak degradasi visual [7]. Algoritma PVD merupakan sistem arah pencarian dengan selisih dua piksel terdekat yang ditunjukkan pada gambar 2.



Gambar 2. Alur PVD

Proses penyisipan pada metode ini dilakukan dengan membandingkan dua piksel yang bertetangga pi dan p(i+1) menggunakan persamaan (1)

$$di = | pi - p(i+1) | \quad (1)$$

Hasil perbandingan tersebut digunakan untuk mengetahui berapa banyak bit yang dapat disisipkan ke dalam dua piksel yang dibandingkan. Metode ini menggunakan skema Wu dan Tsai untuk menentukan range perbandingan piksel sebelumnya. Skema Wu dan Tsai yang digunakan adalah R = {[0-7], [8-15], [16-31], [32-63], [64 -127], [128-255]} dan ditunjukkan pada gambar 3.

Range	0-7	8-15	16-31	32-63	64-127	128-255
Hiding Capacity	3	3	4	5	6	7

Gambar 3. Rentang nilai PVD [7]

Skema ini digunakan untuk mengetahui dimana pada range selisih dua piksel, jika diketahui dimana range tersebut maka dapat diketahui batas bawah (li) dan batas atas (ui). Setelah mengetahui batas bawah dan batas atas rentang, kita dapat menghitung lebar rentang optimal (wi) dengan persamaan (2).

$$wi = ui - li + 1 \quad (2)$$

Langkah selanjutnya adalah mencari jumlah bit pesan (ti) yang dapat disisipkan melalui persamaan (3).

$$ti = \left\lfloor \log 2(wi) \right\rfloor \quad (3)$$

Penyisipan pesan dapat dilakukan dengan mengambil sebanyak-banyaknya bit dari pesan yang akan disisipkan. Setelah mengetahui berapa bit pesan yang akan disisipkan, ubah bit pesan yang akan disisipkan menjadi desimal (b). Kemudian nilai baru dari nilai selisih dihitung untuk penyisipan ke dalam citra menggunakan persamaan (4).

$$d'i = b + li \quad (4)$$

Untuk menentukan nilai piksel baru yang telah disisipkan suatu pesan, ada beberapa aturan yang harus dipenuhi, yaitu:

$$(p_i', p_{i+1}') = \begin{cases} p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\, p_i \geq p_i \, and \, d_i' > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\, p_i < p_i \, and \, d_i' > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\, p_i \geq p_i \, and \, d_i' \leq d_i \\ p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\, p_i < p_i \, and \, d_i' \leq d_i \end{cases} \quad (5)$$

Dimana m diperoleh dari selisih d'i dengan di menggunakan persamaan (5)

$$m = d'i - di \quad (6)$$

Ulangi prosedur di atas sampai bit pesan rahasia benar-benar tersembunyi di gambar sampul [7].

2.4. Steganografi metode CRT

Dalam teori bilangan, dasar dari algoritma CRT adalah kemampuannya untuk merekonstruksi bilangan bulat dengan rentang nilai tertentu untuk sisanya dalam bilangan coprima. Metode CRT sebagai berikut: Tentukan lokasi piksel X, ubah nilai piksel menjadi nilai biner 8 bit [0 255]. Ambil 2-MSB X, lalu ubah ke nilai desimal sebagai nilai Y. Ambil 6-LSB dari X, lalu ubah ke desimal [0 63] sebagai nilai Z. Tentukan pasangan bilangan coprima M1 dan M2 (nilai yang dikemukakan oleh Patra dkk adalah 6 dan 11). Hitung R1 = Z mod 6 dan R2 = Z mod 11. Ubah nilai Z untuk bit '0' jika R1 R2 mengembalikan Z, jika tidak tambahkan 1 sampai R1 R2 maka Z menjadi Z'. Ubah nilai bit '1' jika R1 < R2 mengembalikan Z, jika tidak tambahkan 1 hingga R1 < R2 maka Z menjadi Z'. stego pikselnya adalah X' = Z' + Y. [8]

2.5. PSNR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum sinyal yang diukur dengan jumlah noise yang mempengaruhi sinyal. PSNR biasanya diukur dalam desibel (db). PSNR digunakan untuk membandingkan kualitas gambar sampul sebelum dan sesudah pesan disisipkan. Untuk menentukan PSNR, nilai MSE (*Mean Square Error*) harus ditentukan terlebih dahulu. MSE adalah nilai kesalahan rata-rata antara gambar asli dan gambar manipulasi (dalam kasus steganografi MSE adalah nilai kesalahan rata-rata antara gambar sampul dan gambar stego).

Nilai PSNR yang turun di bawah 30 dB menunjukkan kualitas yang relatif rendah, dimana distorsi akibat penyisipan terlihat jelas. Namun, kualitas gambar stego yang tinggi berada pada nilai 40dB ke atas. Secara kasat mata, nilai terbaik pada gambar menunjukkan bahwa mata kita hampir tidak mengenali gambar asli dan gambar steganografi [9]. Nilai PSNR yang lebih tinggi menyiratkan kemiripan yang lebih dekat antara hasil rekonstruksi dan gambar aslinya. PSNR didefinisikan sebagai:

$$PSNR = 10log_{10}\left(\frac{C_{max}^2}{MSE}\right) \quad (7)$$

Dimana MSE dinyatakan sebagai mean square error yang didefinisikan sebagai:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - S_{xy})^2 \quad (8)$$

3. HASIL DAN PEMBAHASAN

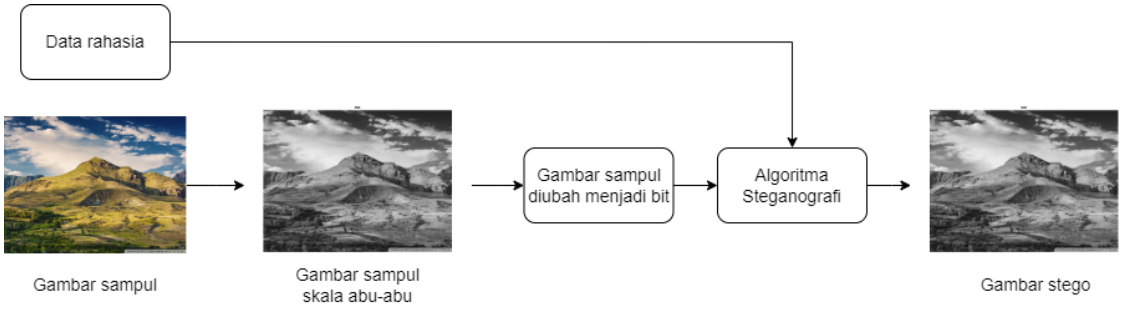
Objek yang akan dibandingkan dalam penelitian ini adalah metode dasar seperti yang dijelaskan pada bagian 2, dengan beberapa batasan sebagai berikut:

- Setiap metode memiliki gambar yang sama dalam resolusi yang berbeda untuk melihat hasil akhir dari percobaan ini
- Pesan rahasia berisi delapan karakter
- Setiap metode menampilkan tiga resolusi berbeda yang banyak digunakan dalam pencitraan digital [10], terdiri dari 640x480 px, 800x600 px, 1280x720 px.
- Gambar akan dianalisis dalam bitmap karena formatnya yang tidak terkompresi, atau, dikompresi dalam proses lossless [11].

3.1. Steganografi

Langkah pertama dari tiga metode yang dijelaskan pada bagian 2 adalah memasukkan pesan rahasia ke dalam gambar sampul untuk menjadi gambar stego. Pesan rahasia yang digunakan dalam penelitian ini adalah "mushroom" yang terdiri dari 8 karakter. Gambar 4 berikut merupakan metode steganografi yang dilakukan pada penelitian. Berikut ini adalah urutan metode steganografi.

1. Membaca pesan rahasianya
2. Pesan rahasia diubah menjadi bit
3. Mengitung jumlah bit pesan rahasia
4. Gambar sampul diubah menjadi gambar skala abu-abu
5. Piksel pada citra abu-abu kemudian diubah menjadi bit
6. Nilai pada piksel pertama citra abu-abu diganti dengan jumlah bit pesan rahasia
7. Pesan rahasia dimasukkan ke dalam piksel ke-2 sampai dengan jumlah bit pesan rahasia, cara pesan rahasia dilakukan penyisipan berdasarkan metode yang dilakukan
8. Setelah proses steganografi, diperoleh gambar stego.

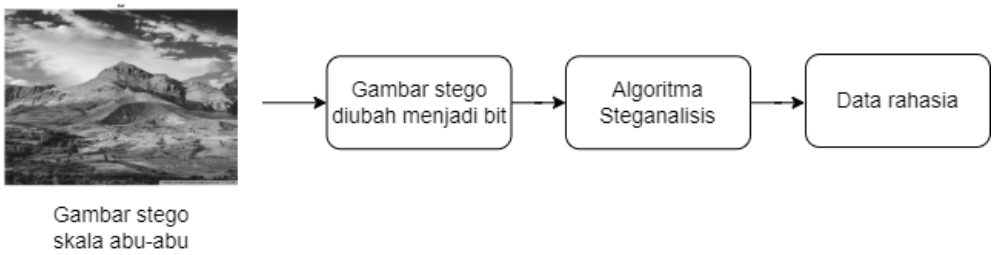


Gambar 4. Metode steganografi

3.2. Steganalisis

Steganalisis adalah bagian dimana pesan rahasia diambil dari gambar stego. Gambar 5 metode steganalisis. Berikut ini adalah urutan metode steganalisis.

1. Gambar stego diubah menjadi bit
2. Membaca piksel pertama gambar stego untuk mendapatkan jumlah bit pesan rahasia
3. Melakukan proses steganalysis berdasarkan metode yang dilakukan
4. Didapatkan pesan rahasia dalam bentuk bit



Gambar 5. Metode steganalisis

3.3. Perbandingan kinerja metode

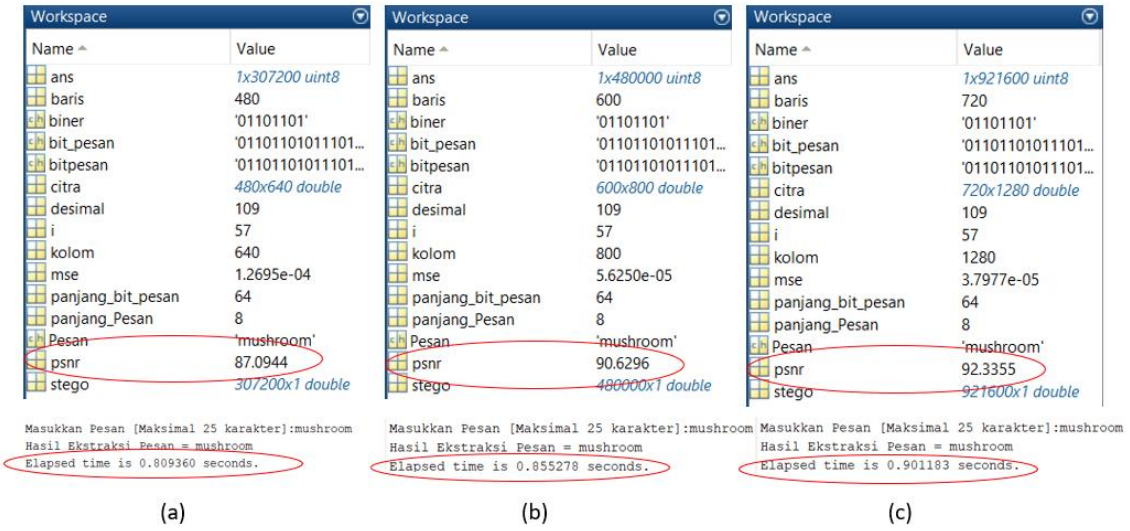
Dalam penelitian ini, PSNR, waktu dari masing-masing metode dan perbedaan ukuran gambar antara gambar sampul dan gambar stego semuanya dibandingkan. Langkah pertama pada penelitian ini adalah menjalankan metode LSB, PVD, dan CRT (dengan data masukan yang sama) menggunakan fungsi tic toc di MATLAB. Langkah terakhir terdiri dari hasil melakukan dokumentasi yang terdiri dari waktu, ukuran gambar gambar sampul dan gambar stego dan PSNR. Data yang diambil adalah proses setelah memasukkan pesan rahasia sampai dengan perhitungan PSNR selesai.

3.4. Hasil Penelitian

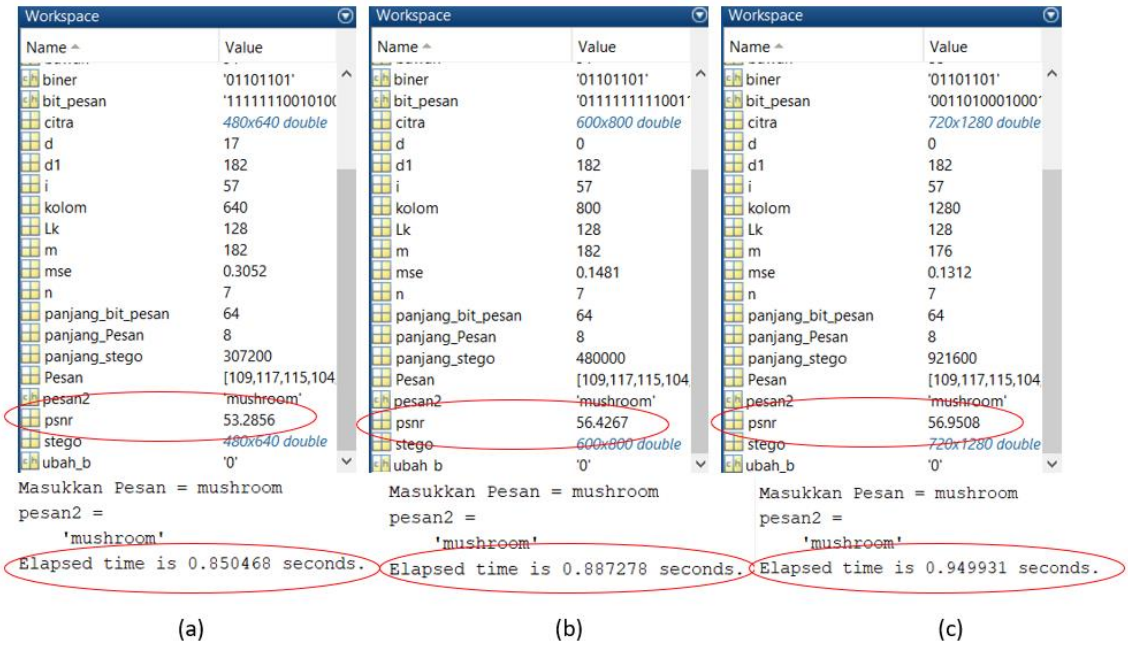
Semua gambar ditempatkan dalam folder yang sama untuk memfasilitasi panggilan program. Pada metode LSB, penulis menjalankan program pertama pada resolusi 640x480. Penelitian dilakukan dengan fungsi tic toc pada MATLAB untuk menghitung waktu program berjalan. Selanjutnya, program akan meminta pesan rahasia untuk disisipkan. Setelah pesan rahasia diketik, peneliti menjalankan program dan hasil yang akan keluar adalah program waktu, gambar sampul, gambar stego dan pesan rahasia yang sudah diekstraksi. Ketika semua data keluaran muncul, hitung penundaan program sesuai dengan metode steganografi yang dilakukan dan simpan gambar sampul dan gambar stego sebagai format .bmp.

Gambar 9 merupakan hasil antara gambar sampul dan gambar stego. Gambar 6a merupakan hasil workspace pada MATLAB dengan metode LSB dan resolusi 640x480. PSNR yang didapat adalah 87,0944 dengan waktu yang membutuhkan proses selama 0,809 detik. Gambar 6b merupakan hasil workspace pada MATLAB dengan metode LSB dan resolusi 800x600. PSNR yang didapat adalah 90,6296 dengan waktu yang membutuhkan proses selama 0,855 detik. Gambar 6c merupakan hasil workspace pada MATLAB dengan metode LSB dan resolusi 1280x720. PSNR yang didapat adalah 92,3355 dengan waktu yang membutuhkan proses selama 0,901 detik. Gambar 7a merupakan hasil workspace pada MATLAB dengan metode PVD dan resolusi 640x480. PSNR yang didapat adalah 53,2856 dengan waktu yang membutuhkan proses selama 0,85 detik. Gambar 7b merupakan hasil workspace pada MATLAB dengan metode PVD dan resolusi 800x600. PSNR yang didapat adalah 56,4267 dengan waktu yang membutuhkan proses selama 0,887 detik. Gambar 7c merupakan hasil workspace pada MATLAB dengan metode PVD dan resolusi 1280x720. PSNR yang didapat adalah 56,9508 dengan waktu yang membutuhkan proses selama 0,949 detik. Gambar 8a merupakan hasil workspace pada MATLAB dengan metode CRT dan resolusi 640x480. PSNR

yang didapat adalah 79,9301 dengan waktu yang membutuhkan proses selama 0,874 detik. Gambar 8b merupakan hasil workspace pada MATLAB dengan metode CRT dan resolusi 800x600. PSNR yang didapat adalah 81,5786 dengan waktu yang membutuhkan proses selama 0,884 detik. Gambar 8c merupakan hasil workspace pada MATLAB dengan metode CRT dan resolusi 1280x720. PSNR yang didapat adalah 85,2477 dengan waktu yang membutuhkan proses selama 0,858 detik.

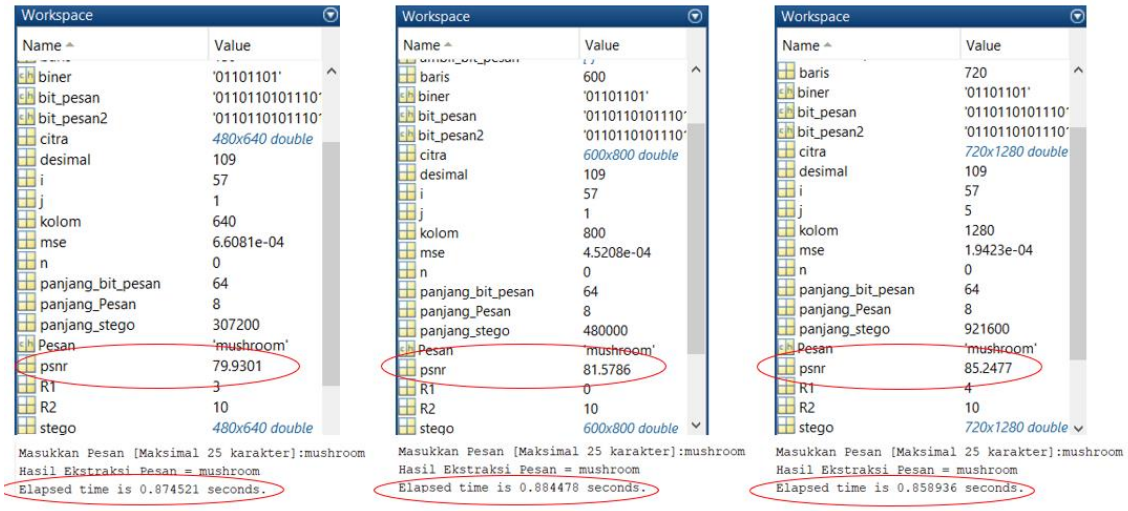


Gambar 6. Hasil metode LSB (a) workspace pada MATLAB dengan resolusi 640x480 (b) workspace pada MATLAB dengan resolusi 800x600 (c) workspace pada MATLAB dengan resolusi 1280x720

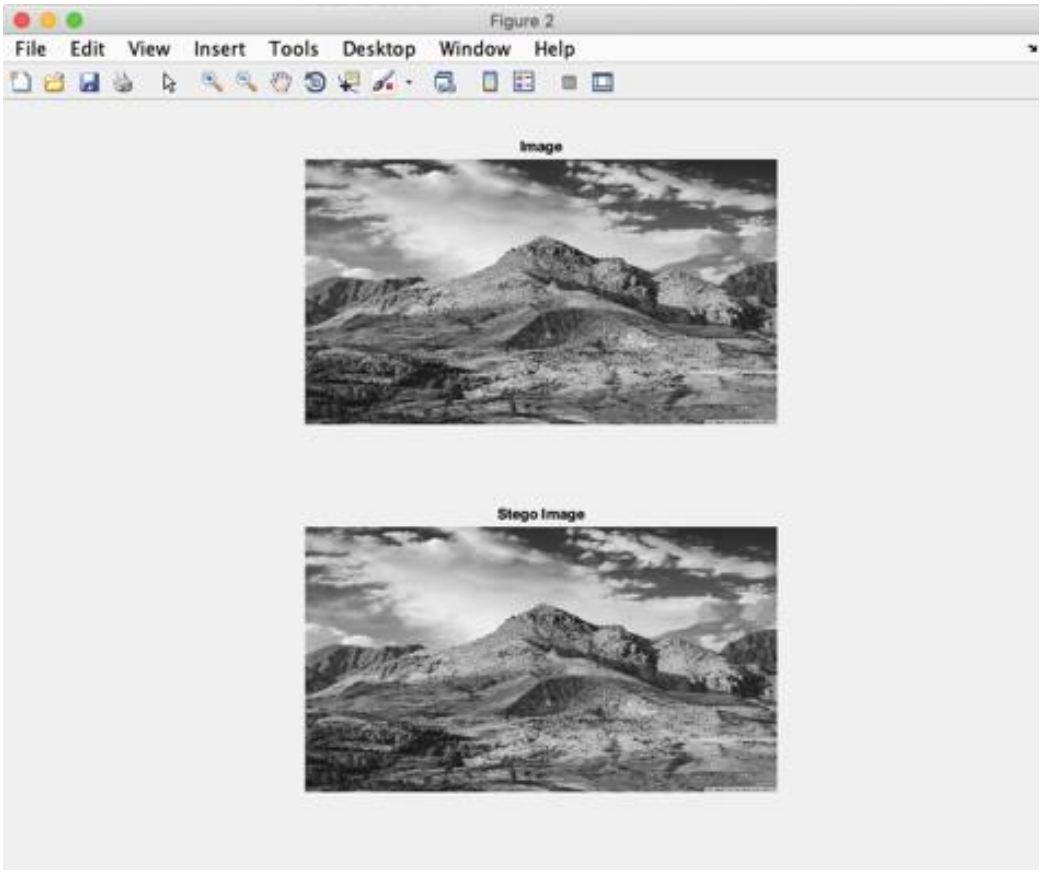


Gambar 7. Hasil metode PVD (a) workspace pada MATLAB dengan resolusi 640x480 (b) workspace pada MATLAB dengan resolusi 800x600 (c) workspace pada MATLAB dengan resolusi 1280x720

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 8. Hasil metode CRT (a) workspace pada MATLAB dengan resolusi 640x480 (b) workspace pada MATLAB dengan resolusi 800x600 (c) workspace pada MATLAB dengan resolusi 1280x720



Gambar 9. Gambar sampul dan gambar stego

Percobaan metode LSB pada tabel 1 menunjukkan bahwa resolusi dari hasil PSNR terkecil hingga tertinggi yang dihasilkan semakin baik. Artinya semakin besar resolusi yang digunakan maka semakin baik pula citra hasil stegonya. Pada percobaan metode PVD, resolusi

dari hasil PSNR terkecil hingga tertinggi yang dihasilkan semakin baik. Namun pada resolusi 800x600 dan 1280x720 PSNR perbedaannya tidak terlalu jauh, yakni hanya 0,5241 dibandingkan resolusi sebelumnya. Berdasarkan ukuran resolusi metode CRT, semakin besar resolusi maka semakin baik hasil PSNR. Namun, hasil PSNR yang diperoleh dari metode ini sedikit lebih buruk daripada metode LSB. Dari segi waktu, berdasarkan ketiga metode yang digunakan semakin besar resolusi maka semakin lama program berjalan. Untuk perbandingan antara gambar sampul dan gambar stego, tidak ada perubahan ukuran gambar. Dalam hal perbandingan ukuran gambar sampul dan gambar stego, tidak ada perubahan ukuran dari semua metode yang diteliti.

Tabel 1. Hasil perbandingan metode

Resolusi	**LSB**			
	PSNR	***Waktu proses***	***Ukuran gambar sampul***	***Ukuran gambar stego***
640x480	87,0944	0,809 detik	1.273.966 bytes	1.273.966 bytes
800x600	90,6296	0,855 detik	1.873.486 bytes	1.873.486 bytes
1280x720	92,3355	0,901 detik	3.064.022 bytes	3.064.022 bytes
Resolusi	**PVD**			
	PSNR	***Waktu proses***	***Ukuran gambar sampul***	***Ukuran gambar stego***
640x480	53,2856	0,850 detik	1.273.966 bytes	1.273.966 bytes
800x600	56,4267	0,887 detik	1.873.486 bytes	1.873.486 bytes
1280x720	56,9508	0,949 detik	3.064.022 bytes	3.064.022 bytes
Resolusi	**CRT**			
	PSNR	***Waktu proses***	***Ukuran gambar sampul***	***Ukuran gambar stego***
640x480	79,9301	0,874 detik	1.273.966 bytes	1.273.966 bytes
800x600	81,5786	0,884 detik	1.873.486 bytes	1.873.486 bytes
1280x720	85,2477	0,858 detik	3.064.022 bytes	3.064.022 bytes

4. KESIMPULAN

Penelitian ini menggunakan tiga metode steganografi yaitu LSB, PVD dan CRT. Ketiga metode tersebut dibandingkan untuk mengetahui metode yang efektif dari segi kualitas citra secara objektif, waktu program yang dijalankan, dan ukuran citra digunakan. Percobaan dilakukan dengan menggunakan *software* matlab dan *hardware* Macbook Air MacOS Mojave versi 10.14.6.

1. Dari segi PSNR, berdasarkan ketiga metode yang digunakan semakin besar resolusi maka semakin baik hasil PSNR yang diperoleh. Semakin besar resolusinya, pesan yang disisipkan tidak akan menggantikan bit gambar yang besar. Resolusi 640x480 metode LSB, PVD, dan CRT memiliki nilai PSNR masing-masing 87,0944, 53,2856 dan 79,9301. Resolusi 800x600 metode LSB, PVD, dan CRT memiliki nilai PSNR sekuensial sebesar 90,6296, 56,4267, 81,5786. Resolusi 1280x720 metode LSB, PVD, dan CRT memiliki nilai PSNR berurutan 92,3355, 56,9508, 85,2477. Metode LSB memiliki hasil PSNR terbaik dari semua resolusi dibandingkan metode lainnya karena pada LSB, pesan rahasia disisipkan pada bit

terendah sehingga tidak banyak mengubah nilai bit gambar. Metode PVD memiliki nilai PSNR paling buruk dibandingkan dengan metode lainnya. Dalam metode PVD, penyisipan pesan dilakukan pada piksel tetangga dan berfokus pada sejumlah besar pesan yang disisipkan. Dengan demikian, penyisipan pesan dapat dilakukan pada bit-bit besar pada citra.

2. Dari segi waktu, berdasarkan ketiga metode yang diteliti semakin besar resolusi maka semakin lama waktu yang didapat. Program mengeluarkan dua keluaran gambar, yaitu gambar sampul dan gambar stego, semakin besar resolusinya, semakin besar ukuran gambarnya, itulah sebabnya kedua keluaran ini menyebabkan penundaan yang lebih lama. Resolusi 640x480 pada metode LSB, PVD, dan CRT memiliki nilai sequential waktu 0,809 detik, 0,85 detik, 0,874 detik. Resolusi 800x600 metode LSB, PVD, dan CRT memiliki nilai sequence waktu sebesar 0,855 detik, 0,887 detik, 0,884 detik. Resolusi 1280x720 metode LSB, PVD, dan CRT memiliki nilai penundaan berurutan 0,901 detik, 0,949 detik, 0,858 detik. Metode PVD memiliki waktu yang paling lama dibandingkan dengan metode lainnya. Dalam PVD, penyisipan pesan rahasia langsung dilakukan pada piksel gambar tetangga tidak seperti metode lain yang harus mengubah gambar dan pesan menjadi bit dan mengubahnya kembali menjadi gambar piksel. Metode LSB memiliki waktu yang lebih cepat dibandingkan dengan metode lainnya. .
3. Dari segi perbandingan ukuran gambar sampul dan fambar stego, berdasarkan ketiga metode yang diteliti tidak ada perubahan ukuran pada kedua image tersebut. Dalam penelitian ini, format .bmp digunakan karena format tersebut memiliki sifat kompresi lossless. Oleh karena itu, karena sifat kompresi lossless tidak ada perubahan ukuran gambar sampul dan gambar stego.
4. Metode CRT mengubah citra menjadi piksel seperti pada metode LSB dan melakukan perhitungan bit tertentu seperti pada metode PVD. Oleh karena itu, pada metode ini aspek waktu dan PSNR tidak lebih baik dan lebih buruk dibandingkan dengan metode lainnya.

5. SARAN

Penelitian ini dapat dilakukan gambar RGB yang berbeda-beda atau ukuran gambar yang lebih besar untuk mendapatkan nilai yang bervariasi juga untuk dianalisa.

DAFTAR PUSTAKA

[1] C. U. Library, "*Digital Imaging tutorial*," Cornell University, http://preservationtutorial.library.cornell.edu/intro/intro-01.html. Diakses tanggal 15 Juli 2019.

[2] A. B. Zhang, "*Resolution Image - an overview*," Elsevier B.V., https://www.sciencedirect.com/topics/computer-science/resolution-image. Diakses tanggal 03 September 2019].

[3] K.Thangadurai, "An analysis of LSB Based Image Steganography Techniques," in *International Conference on Computer Communication and Informatics* , Karur - India.

[4] A. S. Mahajan, "Hardware Implementation of LSB Steganography Using MATLAB and FPGA," in *International Journal of Computer Science Trends and Technology* (IJCST), Maharashtra - India, 2015.

[5] P. N. Andono, *Digital Image Processing*, Semarang: ANDI, 2017.

[6] A. S. Mahajan, "Hardware Implementation of LSB Steganography Using MATLAB and FPGA," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 3, no. 4, pp. 41-44, 2015.

[7] A. Tyagi, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum," in *Second International Conference on Advances in Computing and Communication Engineering*, Durgapur-India, 2015.

[8] J. Chen, "An Information Hiding Scheme Based On Chinese Remainder Theorem," in IEEE *International Conference on Image, Vision and Computing*, Hefei - China, 2018.

[9] V. K. Bhola, "Image Quality Assessment Techniques," in ICFTEM, 2014.

[10] C. A. Rusen, "*What do the 720p, 1080p, 1440p, 2K, 4K resolutions mean? What are the aspect ratio & orientation?*," Digital Citizen, 03 July 2019. https://www.digitalcitizen.life/what-screen-resolution-or-aspect-ratio-what-do-720p-1080i-1080p-mean. Diakses tanggal 26 Augustus 2019.

[11] E. E. A. b. Elgabar, "Comparison of LSB Steganography in BMP and JPEG Images," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, no. 5, pp. 91-95, 2013.

[12] J. Little, "Profile to Improve Performance," Mathworks, 2019. https://www.mathworks.com/help/matlab/matlab_prog/profiling-for-improving-performance.html. Diakses tanggal 27 Augustus 2019].