

ANALISIS FAKTOR ROBUSTNESS DAN FIDELITY PADA METODE LSB, DCT, DAN DWT DALAM IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL

Ardian Tri Kusuma ⁽¹⁾, Juwairiah, S.Si., M.T. ⁽²⁾, Herry Sofyan, S.T., M.Kom. ⁽³⁾
Program Studi Informatika, Fakultas Teknik Industri, UPN "Veteran" Yogyakarta
Jl. Babarsari 2 Yogyakarta 55281 (Kampus Unit II)
e-mail : ¹ ardiantrik@gmail.com, ²juwai_riah@yahoo.com, ³herrysofyan@gmail.com

Abstract

The secret of informations is important. Today, information not only be encrypted, but also can be embedded in digital media. Steganography is an art to hide information so that confidential information cannot be known by others, except the sender and receiver. Several studies have been carried out related to data hiding by implementing several algorithms. In this study, an application was built by applying the method of Least Significant Bit (LSB) steganography, Discrete Cosine Transform (DCT), and Discrete Haar Wavelet Transform (DWT). The message will be inserted to images using the LSB, DCT, DWT, and a combination of those methods. The results will be tested from the aspects of robustness and fidelity and then analyzed and concluded which is the best method to be implemented. The methodology used in this study is prototyping approach. The results showed that based on robustness testing with the Stirmark approach based on geo transform attack, the LSB method received the highest average message extraction percentage of 24.3%, and based on a series of fidelity tests, the LSB method got the best average results such as there was no visual difference, the average file size difference is 3.2 MB, the average PSNR value is 68.2 dB, and the average RGB value difference with Euclidean distance is 339.14.

Keywords : *Steganography, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Haar Wavelet Transform (DWT), Robustness, Fidelity*

Kerahasiaan suatu informasi adalah penting dan menjadi suatu perhatian tersendiri. Zaman sekarang informasi tidak hanya dapat disandikan, tetapi dapat juga disisipkan ke dalam media digital. Steganografi adalah ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima. Beberapa penelitian telah dilakukan berkaitan dengan pengamanan data dengan menerapkan beberapa algoritma. Pada penelitian ini dibangun aplikasi dengan menerapkan metode steganografi *Least Significant Bit (LSB)*, *Discrete Cosine Transform (DCT)*, dan *Discrete Haar Wavelet Transform (DWT)*. Pesan akan disisipkan pada citra digital dengan metode LSB, DCT, DWT, dan kombinasi ketiga metode tersebut. Hasil penyisipan akan diuji dari aspek *robustness* dan *fidelity* dan kemudian akan dianalisis dan disimpulkan manakah metode penyisipan yang paling baik untuk diimplementasikan. Metodologi yang digunakan dalam penelitian ini menggunakan pendekatan metode *prototyping*. Hasil penelitian menunjukkan berdasarkan pengujian *robustness* dengan pendekatan Stirmark berbasis *geo transform attack*, metode LSB mendapat rata-rata persentase keberhasilan ekstraksi pesan tertinggi sebesar 24,3% dan berdasarkan serangkaian pengujian *fidelity*, metode LSB mendapat hasil dengan rata-rata terbaik yaitu tidak nampak perbedaan visual, rata-rata selisih ukuran file terendah sebesar 3,2 MB, nilai PSNR tertinggi sebesar 68,2 dB, dan rata-rata nilai perbedaan RGB dengan jarak *Euclidean* sebesar 339,14.

Kata Kunci : *Steganografi, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Haar Wavelet Transform (DWT), Robustness, Fidelity*

1. PENDAHULUAN

Kerahasiaan suatu informasi adalah penting dan menjadi suatu perhatian tersendiri dari masa ke masa. Manusia berusaha mencari cara bagaimana merahasiakan informasi terhadap pihak yang dianggap tidak berhak untuk mengetahuinya. Berbagai cara telah dilakukan oleh bangsa –

bangsa kuno untuk merahasiakan informasi, karena informasi yang jatuh ke orang yang tidak berhak akan menimbulkan kerugian. (Tarigan, 2015).

Zaman sekarang informasi tidak hanya dapat disandikan, tetapi dapat juga disisipkan ke dalam media digital. Teknik menyisipkan pesan dikenal dengan nama steganografi. Steganografi sebagai ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima (Atoum et al., 2012).

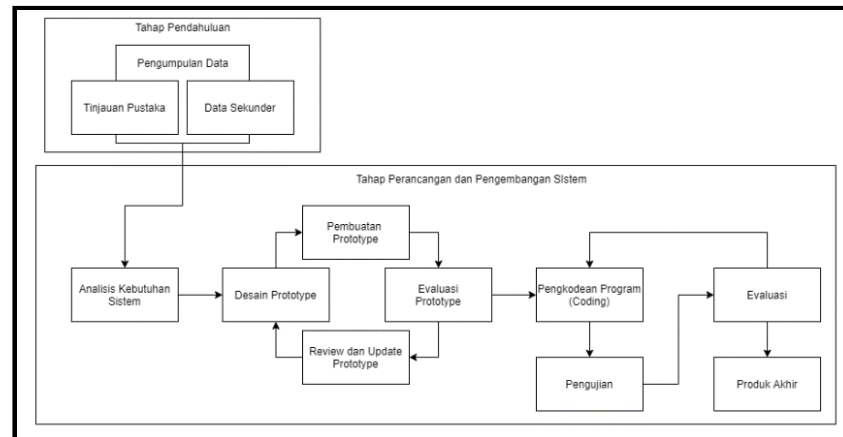
Beberapa penelitian telah dilakukan berkaitan dengan pengamanan data dengan menerapkan beberapa algoritma steganografi seperti algoritma *Least Significant Bit*, *Discrete Cosine Transform*, dan *Discrete Wavelete Transform*. Dalam penelitian Danuputri (2018) menggunakan algoritma *Least Significant Bit* yang diperkuat dengan algoritma *Vignere Key* untuk melakukan enkripsi pada dokumen berekstensi *.doc, *.docx, *.xls, *.xlsx, *.txt, dan *.pdf untuk dihasilkan *plaintext* yang kemudian menggunakan *Least Significant Bit* untuk menyisipkannya ke dalam gambar. Citra stego yang dihasilkan tidak memiliki perbedaan yang signifikan dan data yang disisipkan tidak mengalami perubahan ketika diekstrak. Namun terdapat penambahan ukuran file pada citra stego yang dihasilkan. Penelitian serupa terkait algoritma *Least Significant Bit* juga pernah dilakukan oleh Sanawira dan Purnomo (2016) yang menggunakan algoritma tersebut untuk menyembunyikan pesan ke dalam citra sebagai *cover object* dengan gabungan metode *Redundant Pattern Encoding* dan hasil uji yang didapat tergolong bagus karena citra yang disisipi pesan tidak menunjukkan perbedaan signifikan dari citra aslinya. Selain itu, terdapat juga penelitian oleh Garno dan Solehudin (2017) yang mengkombinasikan metode *Discrete Cosines Transform* dan Interpolasi *Bilinear* untuk menyembunyikan pesan. Pada penelitian tersebut Garno berhasil menyisipkan pesan ke dalam citra digital, namun terjadi distorsi yang cukup signifikan pada *stego object* sehingga nilai hasil uji kurang memuaskan karena rata-rata tingkat PSNR 27,87 dB. Penelitian lain tentang steganografi juga pernah dilakukan dengan metode *Discrete Wavelete Transform* dengan tipe *Haar* oleh Zagade dan Bhosale (2014). Citra stego yang dihasilkan tergolong bagus dengan nilai PSNR yang tinggi dengan hasil rata-rata di atas 70 dB. Metode DWT dan DCT juga pernah dilakukan oleh Faza dkk. (2016) yaitu dengan menggabungkan DCT dan DWT dan citra yang dihasilkan mencapai rata-rata tingkat PSNR 25,72 dB. Namun gabungan tersebut tidak terlalu memuaskan bila dibandingkan dengan metode DWT saja dengan rata-rata tingkat PSNR 38,58 dB.

Penelitian-penelitian tersebut telah menggunakan algoritma-algoritma steganografi yang mempunyai kelemahan masing-masing. Dengan banyaknya metode-metode yang dapat digunakan, maka akan sangat membantu pengguna dalam memilih metode penyembunyian pesan. Namun kelemahan-kelemahan pada masing-masing metode tentu juga harus diperhatikan. Perlu diketahui bahwa *stego object* tidak selamanya aman dan tidak menimbulkan kecurigaan. Ketika *stego object* dikirimkan menggunakan perantara pihak ketiga, ada kemungkinan *hidden object* pada *stego object* tersebut rusak atau *stego object* menimbulkan kecurigaan oleh orang lain. Hal tersebut terjadi karena setiap metode memiliki tingkat *robustness* (ketahanan) dan *fidelity* (ketidakkampakan perbedaan) yang rendah.

Dari permasalahan yang telah dipaparkan, maka diperlukan perbandingan metode-metode tersebut sehingga dapat diketahui metode mana yang memiliki tingkat *robustness* dan *fidelity* yang paling baik untuk digunakan dalam steganografi maupun *watermarking* pada suatu objek. Dalam penelitian ini, metode yang akan diteliti adalah *Least Significant Bit*, *Discrete Cosines Transform*, *Discrete Haar Wavelet Transform*, serta gabungan dari algoritma tersebut yang menghasilkan sebuah *modified algorithm* yang diharapkan dapat meningkatkan tingkat *robustness* dan *fidelity* dari *stego object* yang dibuat. Pemilihan metode-metode tersebut dilandasi oleh beberapa penelitian tentang LSB, DCT, maupun DWT sebelumnya yang hanya menggunakan pengujian kualitas PSNR dan MSE untuk menentukan baik tidaknya metode-metode tersebut untuk diimplementasikan serta pengujian ketahanan yang hanya menyebutkan bisa tidaknya pesan rahasia diekstrak kembali tanpa disebutkan apa yang menyebabkan hal tersebut terjadi.

2. Metodologi Penelitian

Metode penelitian yang digunakan adalah metode kuantitatif dengan serangkaian pengujian *robustness*(ketahanan) dan *fidelity* (ketidakkampakan). Sedangkan metode pengembangan sistem menggunakan pendekatan *prototyping*.

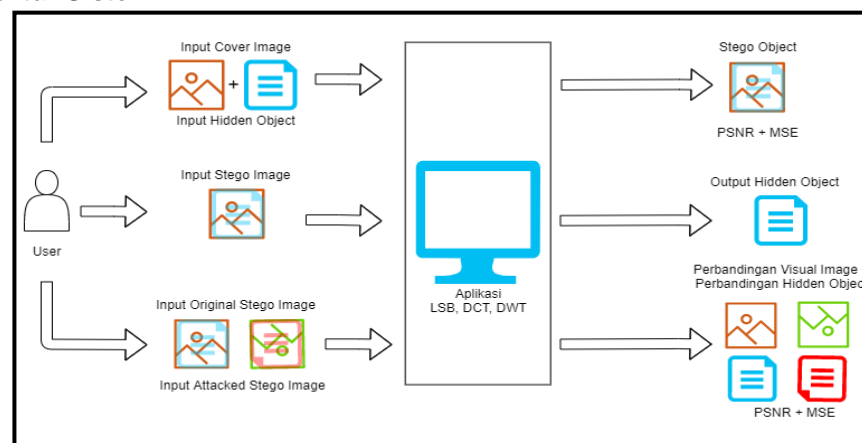


Gambar 1. Metodologi Penelitian

2.1. Pengumpulan Data

Pada tahap ini, pengumpulan data pada aplikasi ini dilakukan dengan studi pustaka untuk mengetahui pengembangan aplikasi yang digunakan untuk teknik steganografi dan gambar yang digunakan untuk proses penyembunyian objek dalam penelitian ini, serta penggunaan data sekunder berupa citra yang didapatkan dari internet dengan format ekstensi *file* yang sudah ditentukan.

2.2. Arsitektur Sistem



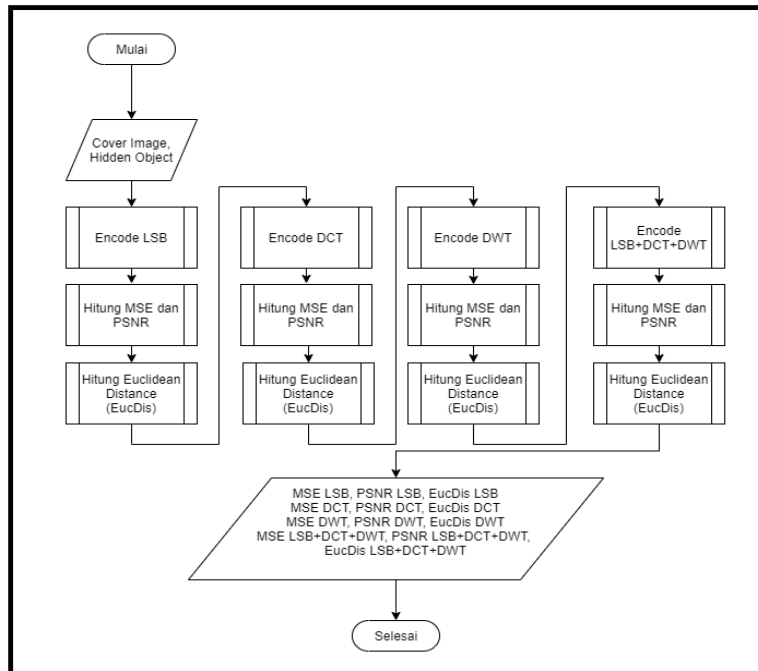
Gambar 2. Arsitektur Sistem

Pada arsitektur di atas, *user* akan memasukkan memiliki tiga pilihan yang dapat dilakukan pada aplikasi. Utamanya *user* akan memasukkan citra yang akan dijadikan citra *cover* dan *hidden object* dengan prosedur *encode*. Kemudian aplikasi akan memproses citra digital tersebut menjadi empat buah citra stego yang merupakan hasil dari penyisipan pesan pada citra menggunakan metode LSB, DCT, DWT, dan kombinasi ketiga metode tersebut. Selanjutnya *user* juga dapat melakukan ekstraksi pesan pada menu *decode*. Proses ini menghasilkan *hidden object* yang didapat dari ekstraksi pesan oleh *stego object* dengan metode yang telah dipilih. Terakhir *user* juga dapat membandingkan dua buah *stego object* yang mana merupakan satu buah *stego object* asli dan *stego object* yang telah diserang. Proses ini terdapat pada menu identifikasi dan akan menghasilkan komparasi kedua citra tersebut secara visual, nilai PSNR antara kedua citra, dan ketahanan pesan yang terdapat dalam kedua citra.

2.3. Perancangan Proses

Perancangan proses meliputi rancangan dari proses algoritma yang terjadi pada aplikasi yang telah dibuat. Terdapat dua proses utama, yaitu proses *encode* dan proses *decode*.

2.3.1. Proses Encode

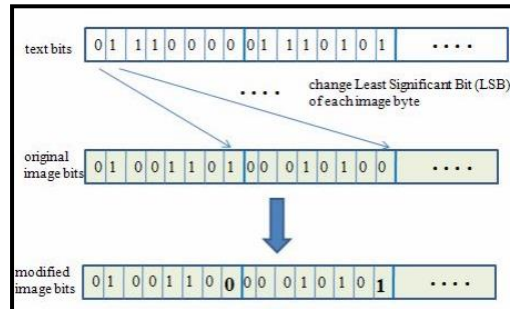


Gambar 3. Flowchart Tahap Encode

Pada tahap *encode* atau penyisipan pesan, proses dilakukan secara *linear* mulai dari penyisipan dengan metode LSB, dilanjutkan DCT, DWT, dan Kombinasi. Masing-masing penyisipan menghasilkan citra stego, nilai MSE, nilai PSNR, dan nilai jarak *euclidean*.

a. Least Significant Bit

Metode LSB dilakukan dengan cara mengubah bit terakhir dari setiap nilai ruang warna RGB dengan bit-bit pesan yang sudah dikonversi menjadi biner ASCII. Ilustrasi penyisipan ditunjukkan pada gambar 4.



Gambar 4. Ilustrasi Penyisipan bit LSB (Joose, 2015)

b. Discrete Cosine Transform

Metode DCT merupakan metode yang mengubah ranah spatial dari citra menjadi ranah frekuensi terlebih dahulu menggunakan persamaan DCT dan IDCT (*Inverse DCT*). Persamaan DCT dapat dilihat pada Persamaan 1 dan persamaan IDCT dapat dilihat pada Persamaan 2.

$$T(i, j) = \frac{2}{\sqrt{N}} C(i) C(j) \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \text{pixel}(x, y) \cos \frac{(2x+1)i\pi}{2N} \cos \frac{(2y+1)j\pi}{2N} \quad (1)$$

$$\text{pixel}(x, y) = \frac{2}{\sqrt{N}} C(i) C(j) \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} T(i, j) \cos \frac{(2x+1)i\pi}{2N} \cos \frac{(2y+1)j\pi}{2N} \quad (2)$$

Dimana :

$T(i, j)$ = Data pada domain frekuensi
 $pixel(x, y)$ = Data pada domain ruang secara pixel

$$C(i) = C(j) = \begin{cases} \sqrt{\frac{1}{n}}, & \text{untuk } i = j = 0 \\ \sqrt{\frac{2}{n}}, & \text{untuk lainnya} \end{cases}$$

Hasil dari persamaan DCT adalah matriks koefisien DCT. Matriks tersebut kemudian akan dilakukan kuantisasi menggunakan matriks kuantisasi. Kuantisasi berfungsi untuk membuat matriks koefisien berukuran 8x8 menjadi 3 *subband*, yaitu *subband* frekuensi rendah, frekuensi sedang, dan frekuensi tinggi. Kuantisasi dilakukan dengan cara membagi nilai matriks koefisien DCT dengan matriks kuantisasi secara *element-wise*. Matriks kuantisasi dapat dilihat pada Persamaan 3.

$$quant = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} \quad (3)$$

Untuk merekonstruksi matriks subband DCT menjadi matriks asal, proses yang dilakukan adalah proses IDCT dengan persamaan 2. Proses IDCT diawali dengan kuantisasi balik dengan cara mengalikan ketiga matriks subband DCT dengan matriks kuantisasi secara *element-wise*, lalu melakukan Persamaan 2.

c. Discrete Wavelet Transform

Metode DWT yang digunakan adalah jenis '*Haar Wavelet*'. DWT juga merupakan metode yang mengubah ranah spatial dari citra menjadi ranah frekuensi terlebih dahulu menggunakan persamaan DWT. Persamaan DWT akan menghasilkan empat ranah yaitu *Low-Low*, *Low-High*, *High-Low*, dan *High-High*. Persamaan dekomposisi DWT dapat dilihat pada Persamaan 4 sampai dengan Persamaan 7.

$${}^J_{LL}W = \int_{x=0}^{M-1} \int_{y=0}^{N-1} g(x)g(y){}^{J-1}_{LL}W(2u-x)(2v-y) \quad (4)$$

$${}^J_{LH}W = \int_{x=0}^{M-1} \int_{y=0}^{N-1} g(x)h(y){}^{J-1}_{LL}W(2u-x)(2v-y) \quad (5)$$

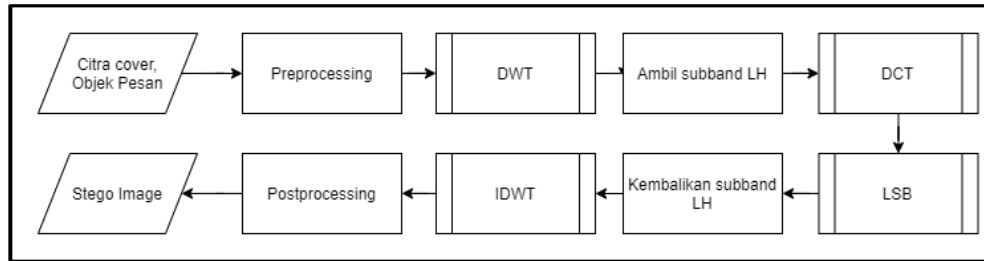
$${}^J_{HL}W = \int_{x=0}^{M-1} \int_{y=0}^{N-1} h(x)g(y){}^{J-1}_{LL}W(2u-x)(2v-y) \quad (6)$$

$${}^J_{HH}W = \int_{x=0}^{M-1} \int_{y=0}^{N-1} h(x)h(y){}^{J-1}_{LL}W(2u-x)(2v-y) \quad (7)$$

Dekomposisi DWT juga bisa dikembalikan seperti semula dengan membalikkan proses dekomposisinya. Hal ini akan merekonstruksi ulang keempat subband menjadi 1 bagian matriks kembali. Proses ini dinamakan IDWT (*Inverse DWT*).

d. Kombinasi

Metode kombinasi merupakan penggabungan metode LSB, DCT, dan DWT menjadi sebuah *modified algorithm*. Proses ini dapat dilihat garis besarnya pada Gambar 5.



Gambar 5. Flowchart garis besar metode Kombinasi

Pada metode kombinasi DCT tidak dilakukan kuantisasi dan IDCT karena matriks *subband* LH berukuran 4x4 dan terlalu banyak proses *rounding* (pembulatan nilai) pada aplikasi menyebabkan nilai ruang warna banyak yang bergeser sehingga hasil penyisipan tidak bisa diekstrak kembali.

e. MSE dan PSNR

Peak Signal to Noise Ratio (PSNR) merupakan sebuah parameter yang penting untuk mengukur kualitas proses pengolahan citra. PSNR adalah rasio antara intensitas maksimum citra dengan *Mean Square Error* (MSE) dari citra. Persamaan untuk menghitung nilai MSE dan nilai PSNR dapat dilihat pada Persamaan 8 dan Persamaan 9.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (8)$$

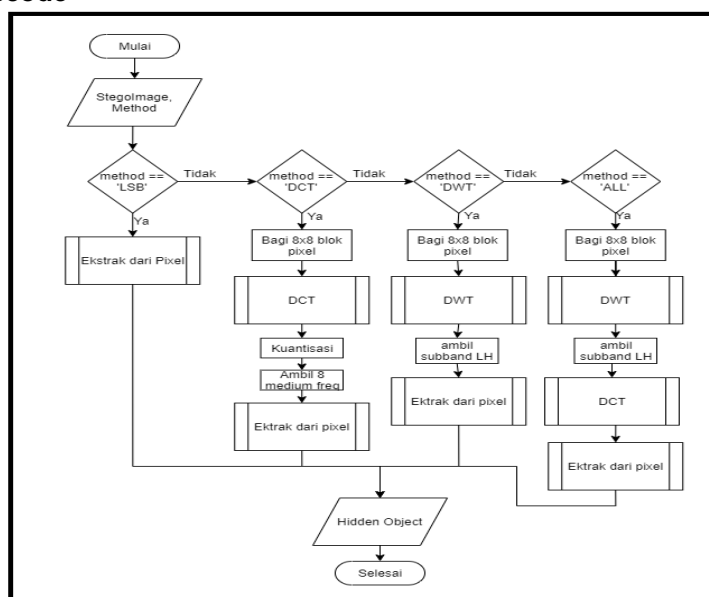
$$PSNR = 20 \times \log_{10} \left(\frac{MAX}{\sqrt{MSE}} \right) \quad (9)$$

f. Euclidean Distance

Proses penghitungan tingkat perbedaan RGB dapat dilakukan dengan penghitungan jarak Euclidean. Persamaan *Euclidean Distance* dapat dilihat pada Persamaan 10.

$$EucDist = \sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ((R1(i,j) - R2(i,j))^2 + (G1(i,j) - G2(i,j))^2 + (B1(i,j) - B2(i,j))^2)} \quad (10)$$

2.3.2. Proses Decode



Gambar 6. Flowchart Tahap Decode

Pada tahap ini proses *decode* akan mengekstrak kembali pesan yang disisipkan. Proses yang terjadi pada proses *decode* hampir sama dengan proses *encode*, yang membedakan hanyalah proses ekstraksi pada setiap metode. Apabila pada proses *encode* dilakukan penyisipan pada bit-bit yang ada dengan cara mengubah LSB setiap nilai ruang warna menjadi bit-bit pesan, maka proses *decode* akan mengambil nilai LSB tersebut dan direkonstruksi untuk dikonversi kembali menjadi karakter yang dapat ditampilkan. Proses *decode* dapat dilihat pada Gambar 6.

3. Hasil dan Pembahasan

3.1. Hasil Penelitian

Hasil penelitian ini mencakup implementasi sistem berupa halaman home, halaman *encode*, halaman hasil *encode*, halaman *decode*, dan halaman identifikasi. Proses yang terjadi pada halaman *encode* adalah proses penyisipan pesan ke dalam citra dengan metode LSB, DCT, DWT dan Kombinasi yang selanjutnya semua hasil akan ditampilkan pada halaman hasil *encode*. Halaman identifikasi digunakan membandingkan citra stego asli dan citra stego yang telah diserang. Aplikasi dibuat dalam bentuk *web app* menggunakan *micro-framework* Flask dengan bahasa *python*.

3.2. User Interface

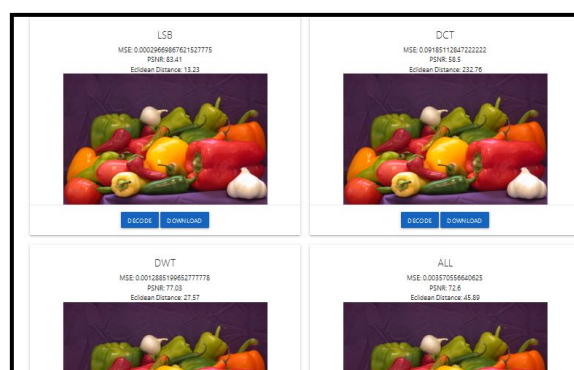
Halaman *home* merupakan halaman awal ketika aplikasi diakses. Pada halaman ini pengguna akan memilih menu selanjutnya yaitu menu *encode*, menu *decode*, atau menu identifikasi.

Halaman *encode* merupakan halaman untuk memilih citra yang akan disisipkan objek. Objek yang disisipkan dapat berupa teks atau citra. Pengguna akan ditunjukkan *preview* dari citra yang akan disisipi, ukuran dari citra tersebut, kapasitas penyisipan, dan objek yang akan dimasukkan.



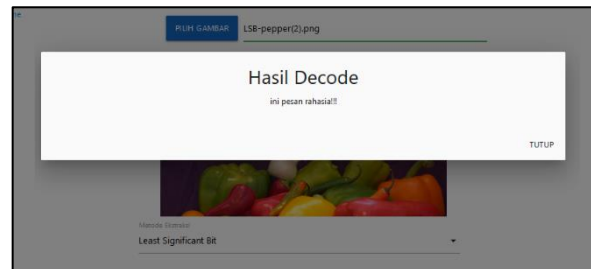
Gambar 7. Tampilan Halaman *Encode*

Halaman hasil *encode* berisikan hasil dari proses penyisipan pesan ke dalam citra dengan metode LSB, DCT, DWT, dan Kombinasi. Halaman ini juga menampilkan nilai PSNR, MSE, dan jarak *Euclidean* masing-masing hasil penyisipan. Pengguna dapat langsung melihat isi yang disisipkan dengan tombol *decode* atau juga dapat mengunduh citra hasil penyisipan dengan tombol *download*.



Gambar 8. Tampilan Halaman Hasil *Encode*

Halaman *decode* merupakan halaman untuk mengekstrak pesan atau menampilkan isi dari pesan yang telah disisipkan. Pengguna dapat memasukkan citra stego dan memilih metode apa yang digunakan untuk ekstraksi pesan. Apabila pengguna menekan tombol *decode* setelah memasukkan citra stego dan memilih metode ekstraksi, maka hasil ekstraksi akan muncul dalam bentuk *pop-up modal* pada *browser*.

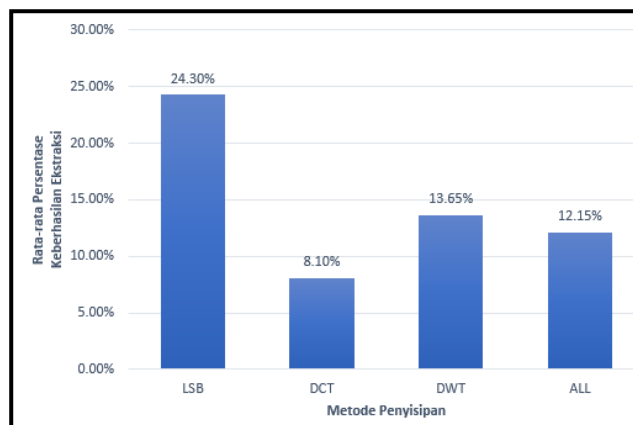


Gambar 9. Tampilan Halaman *Decode*

Halaman identifikasi merupakan halaman untuk membandingkan hasil ekstraksi dua citra, yaitu citra stego yang belum diserang dan citra stego yang sudah diserang. Hasil tersebut akan ditampilkan pada tabel yang sudah tersedia berupa bentuk citranya dan hasil ekstraksinya.

3.3. Pengujian Robustness

Pengujian *robustness* dilakukan dengan menerapkan Stirmark *geometric transform attack* dengan 22 skenario pengujian yang mencakup tidak diserang, *cropping*, *rotate*, *flip*, *resize*, dan penggunaan aplikasi pengiriman pesan seperti WhatsApp, Telegram, LINE, dan Gmail. Hasil dari pengujian ini disajikan pada gambar 10.



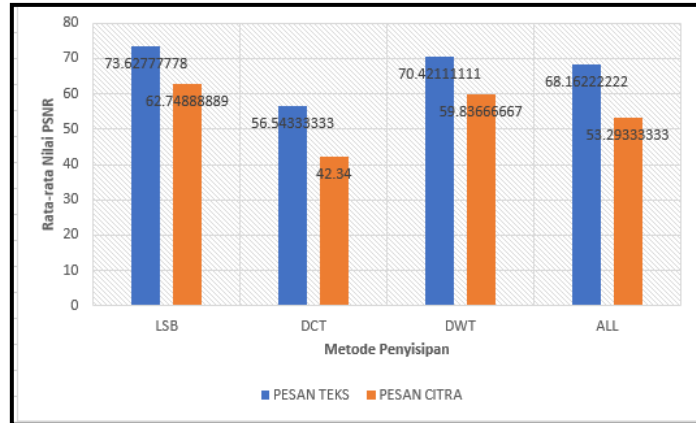
Gambar 10. Grafik rata-rata persentase keberhasilan ekstraksi

3.4. Pengujian Fidelity

Pengujian *fidelity* dilakukan dengan menerapkan beberapa perhitungan seperti PSNR, selisih ukuran *file*, dan jarak *Euclidean*.

a. Peak Signal to Noise Ratio

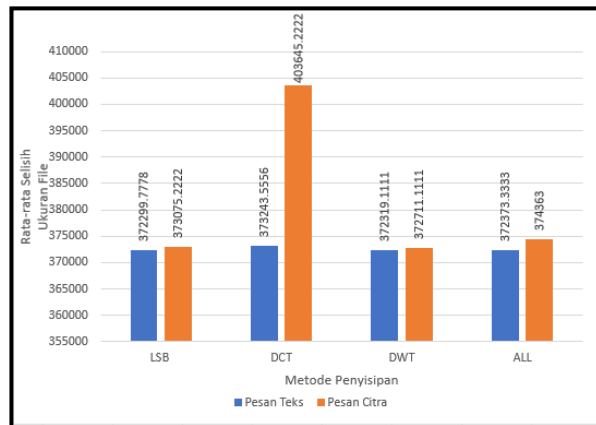
Pengujian PSNR dibagi menjadi dua bagian grafik yaitu grafik PSNR untuk pesan berupa teks dan grafik PSNR untuk pesan berupa citra. Berikut grafik rata-rata PSNR disajikan pada Gambar 11.



Gambar 11. Grafik rata-rata PSNR

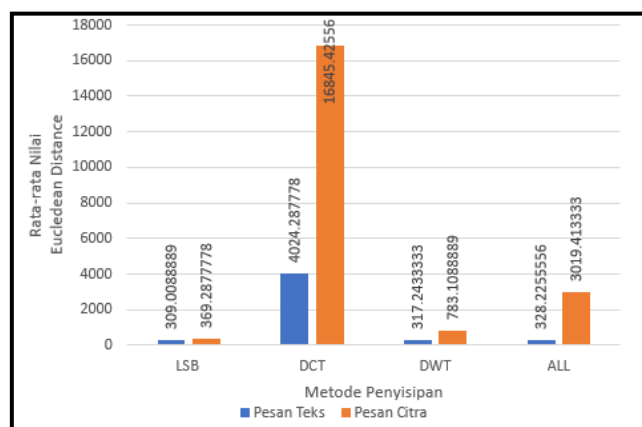
b. Selisih Ukuran File

Pengujian selisih ukuran *file* dibagi juga menjadi dua bagian grafik yaitu grafik untuk pesan berupa teks dan grafik untuk pesan berupa citra. Berikut grafik rata-rata selisih ukuran *file* disajikan pada Gambar 12.

Gambar 12. Grafik rata-rata selisih ukuran *file*

c. Euclidean Distance

Pengujian jarak *Euclidean* dibagi juga menjadi dua bagian grafik yaitu grafik untuk pesan berupa teks dan grafik untuk pesan berupa citra. Berikut grafik rata-rata jarak *Euclidean* disajikan pada Gambar 13.

Gambar 13. Grafik rata-rata jarak *Euclidean*

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan, dan pembahasan yang telah dilakukan, maka dapat diperoleh kesimpulan sebagai berikut:

1. Berdasarkan pengujian faktor *robustness* pada *hidden object* dengan 22 pengujian, metode penyisipan *Least Significant Bit* paling baik untuk diimplementasikan dalam steganografi dengan persentase keberhasilan ekstraksi 24,3%, diikuti metode DWT dengan persentase keberhasilan sebesar 13,65%, metode Kombinasi sebesar 12,15%, dan DCT sebesar 8,1%.
2. Berdasarkan pengujian faktor *fidelity* antara citra *cover* dan citra *stego*, metode penyisipan *Least Significant Bit* paling baik untuk diimplementasikan dalam steganografi dengan rata-rata selisih ukuran file sebesar 3,72 MB, rata-rata PSNR sebesar 68,2 dB, dan rata-rata *euclidean distance* 339,14, diikuti metode DWT dengan rata-rata selisih ukuran file sebesar 3,72 MB, rata-rata PSNR sebesar 65,12 dB, dan rata-rata *euclidean distance* 550,17, lalu metode Kombinasi dengan rata-rata selisih ukuran file sebesar 3,73 MB, rata-rata PSNR sebesar 60,72 dB, dan rata-rata *euclidean distance* 1673,8, dan terakhir metode DCT dengan rata-rata selisih ukuran file sebesar 3,88 MB, rata-rata PSNR sebesar 49,4 dB, dan rata-rata *euclidean distance* 10434,86.
3. Format ekstensi *file* juga mempengaruhi hasil akhir dari penyisipan pesan. PNG dan BMP paling baik untuk implementasi steganografi karena bersifat *lossless compression* sehingga data yang disisipkan tidak rusak, sedangkan JPG kurang baik untuk implementasi karena bersifat *lossy compression* yang memiliki kemungkinan besar data yang disisipkan akan rusak oleh kompresi. Selain itu, ekstensi BMP juga memiliki keunggulan yaitu ukuran file tidak berubah jika proses penyisipan masih dalam satu *channel* warna.

DAFTAR PUSTAKA

- Atoum, M. S., Ibrahim, S., & M. Ahmad, A. (2012). MP3 Steganography: Review. *International Journal of Computer Science Issues*, 236-244.
- Danuputri, C. (2018). Pengamanan Data melalui Cloud Computing dengan Integrasi Steganografi Least Significant Bit dan Kriptografi Vigenere Key Berbasis Android
- Faza, A. M., Slamet, C., & Nursantika, D. (2016). Analisis Kinerja Kompresi Citra Digital dengan Komparasi DWT, DCT, dan Hybrid(DCT-DWT).
- Garno, & Solehudin, A. (2017). TEKNIK STEGANOGRAFI DENGAN METODE DISCRETE COSINES TRANSFORM (DCT) PADA CITRA INTERPOLASI BILINEAR UNTUK PENGAMANAN PESAN. *JURNAL INFORMATIKA UPGRIS Vol. 3, No. 2*.
- Joose, A. (2015). *Steganography Programming*. Retrieved September 30, 2019, from <http://josea1.weebly.com/results/trial-and-error-steganography-programming>
- Munir, R. (2019). *Kriptografi : Edisi Kedua*. Bandung: Penerbit Informatika Bandung.
- Sannawira, R. F., & Purnomo, A. S. (2016). Penyisipan Citra Pesan Ke Dalam Citra Berwarna Menggunakan Metode Least Significant Bit dan Redundant Pattern Encoding.
- Tarigan, T. E. (2015). Algoritma MEoF (Modifikasi End of File) untuk Steganografi pada Citra Bitmap 24 Bit.
- Zagade, S., & Bhosale, S. (2014). Scret Data Hiding in Images by Using DWT Techniques. *International Journal of Engineering and Advanced Technology(IJEAT)*, 230-235.

Pernyataan

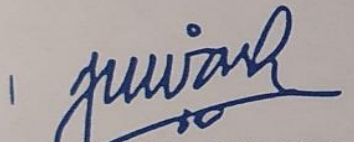
Dengan ini kami menyatakan bahwa judul karya ilmiah “Analisis Faktor *Robustness* dan *Fidelity* pada Metode *Least Significant Bit*, *Discrete Cosine Transform*, dan *Discrete Haar Wavelet Transform* dalam Implementasi Steganografi pada Citra Digital”

Merupakan naskah karya ilmiah dari Skripsi/Tugas akhir mahasiswa :

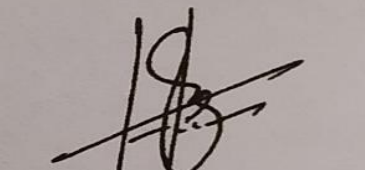
Nama	: Ardian Tri Kusuma
Nim	: 123160035
Judul Skripsi/Tugas Akhir	: Analisis Faktor <i>Robustness</i> dan <i>Fidelity</i> pada Metode <i>Least Significant Bit</i> , <i>Discrete Cosine Transform</i> , dan <i>Discrete Haar Wavelet Transform</i> dalam Implementasi Steganografi pada Citra Digital

Telah kami periksa dengan benar dan memenuhi kaedah penulisan ilmiah serta bebas dari plagiat kecuali cuplikan serta ringkasan yang terdapat didalamnya serta telah dijelaskan sumbernya(Sitasi) dengan jelas. Apabila pernyataan ini terbukti tidak benar maka saya bersedia menerima sanksi sesuai peraturan perundang-undangan yang berlaku.


Pembimbing I


Jiwairiah, S.Si., M.T.
NIK. 2 7607 00 0230 1

Pembimbing II


Herry Sofyan, S.T., M.Kom.
NIK. 2 6404 96 0139 1

Mengetahui
Koordinator Program Studi


Dr. Heriyanto, A.Md., S.Kom., M.Cs.
NIK. 2 7706 11 0301 1