JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

KOMBINASI PENYISIPAN PESAN DAN WATERMARK DENGAN DISCRETE WAVELET TRANSFORM

Imam Budi Setiawan[1], Ahmad Tri Hidayat[2]

[1,2] Universitas Teknologi Yogyakarta, Sleman 55285
** Email Korespondensi: imamsetiawan110@gmail.com*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl 27/09/2023
Diperbaiki Tgl 06/12/2023
Disetujui Tgl 23/12/2023
Tersedia daring 03/01/2024

e-ISSN 2961-9009
p-ISSN 2963-1289

DOI :
https://doi.org/10.58290/jukomtek.v2i2.168

ABSTRAK

Penyebaran citra digital yang dipermudah dengan internet sehingga dapat menyebabkan kerugian bagi pemilik asil gambar tersebut. Tidak adanya perlindungan terhadap citra tersebut dapat diklaim oleh orang. Dengan memanfaatkan watermark cita digital dapat dilindungi hak ciptanya. Selain melindungi citra dari klaim, pesan rahasia juga dapat disisipkan sebagai media komunikasi. Dengan demikian komunikasi dapat dilakukan secara rahasia. Penyisipan dilakukan dengan metode LSB (*Least Significant Bit*) untuk menyembunyikan pesan rahasia ke dalam gambar, sedangkan metode DWT (*Discrete Wavelet Transform*) dipakai untuk menyisipkan watermark. Pengolahan watermark terlebih dahulu dilakukan dengan membagi watermark menjadi dua bagian. Ekstraksi dilakukan untuk mendapatkan pesan rahasia dan watermark. Hasil penelitian menunjukkan bahwa pesan rahasia dan watermark dapat disisipkan dan diekstraksi. Parameter yang digunakan untuk menghitung perbedaan adalah PSNR dan MSE. Hasil penyisipan rata-rata memiliki nilai PSNR sebesar 29,337 dan MSE sebesar 79,45. Hasil tersebut menunjukkan terdapat sedikit perbedaan gambar asli dengan gambar hasil proses penyisipan. Hasil ekstraksi watermark memiliki nilai PSNR sebesar 40,749 dan MSE sebesar 5,60 yang menunjukkan hasil watermark hampir sama dengan watermark yang asli.

Kata Kunci:
Citra Digital, DWT, LSB, Steganografi, Watermark

PENDAHULUAN

Teknologi yang berkembang menjadikan hampir sebagian informasi didapatkan secara instan. Sama seperti halnya komunikasi yang bisa berjalan secara cepat. Internet mendukung kegiatan komunikasi dan pengambilan informasi yang memiliki fitur unggah dan unduh. Dengan adanya fitur dan jaringan yang global maka sebuah berkas atau *file* seperti citra digital dapat dilihat secara luas.

Penyebaran citra digital memiliki dampak baik maupun buruk. Berfokus pada dampak buruk yang ditimbulkan, citra tersebut dapat merugikan pemilik asli. Hal ini

disebabkan karena ketiadaan perlindungan atas hak cipta atau kepemilikan citra digital tersebut. Berbagai pihak dapat mengklaim sehingga dapat merugikan baik secara materiil maupun non-materiil.

Penanaman watermark dengan citra digital membantu pemilik asli untuk melakukan otentikasi terhadap karyanya. Watermark tersebut digunakan sebagai bukti sehingga dapat dianggap sebagai properti sah. Informasi terkait kepemilikan disisipkan ke dalam citra digital. Penyisipan tersebut menghasilkan citra yang hasilnya mirip dengan aslinya. Dengan demikian, pemilik citra tidak akan dirugikan atas klaim hak cipta yang diajukan oleh orang lain.

Citra digital juga dapat menampung pesan didalamnya. Steganografi membuat pesan rahasia tersembunyi dalam sebuah citra digital yang tidak dapat dilihat oleh indra manusia. Data tersebut memerlukan keamanan sehingga hanya diterima oleh penerima yang sah. Dengan demikian, ancaman keamanan terhadap pesan tersembunyi dapat diatasi. Gambar yang dihasilkan dari proses steganografi kemudian dapat dengan aman didistribusikan karena sulitnya dideteksi. Selanjutnya agar gambar tersebut dapat diklaim atas kepemilikan yang sah maka ditamankan watermark sebagai otentikasi.

Penelitian ini menggabungkan antara penyisipan pesan rahasia dalam gambar dan watermark agar pesan yang disisipkan dapat diklaim atas kepemilikannya dengan watermark. Tujuan dari penelitian ini adalah untuk menyisipkan pesan rahasia dalam gambar yang disertai dengan watermark. Hal ini dilakukan agar integritas kepemilikan gambar dalam dapat terjaga dan pesan terjaga sebagai alat untuk berkomunikasi secara rahasia

Dari latar belakang yang telah dijabarkan, peneliti mengusung judul Implementasi Penyisipan Pesan Dan Invisible Watermark Dengan Teknik Discrete Wavelet Transform yang dibuat menjadi sebuah sistem yang dapat menyisipkan pesan rahasia dan sekaligus watermark dalam sebuah citra gambar.

LANDASAN TEORI

Citra Digital

Citra digital merupakan hasil dari analog dua dimensi berupa gambar yang kontinu menjadi gambar melalui proses sampling. Pembagian pada gambar analog dilakukan dengan membaginya ke dalam N baris dan M kolom. Pembagian tersebut menjadikan gambar bersifat diskrit (Septiani Muzahardin & Fauzi, 2022).

Steganografi

Berasal dari kata steganos yang berarti menyembunyikan dan graptos yang berarti tulisan dalam bahasa Yunani. Secara keseluruhan memiliki arti tulisan yang disembunyikan. Steganografi secara umum memiliki pengertian ilmu atau seni menyembunyikan pesan rahasia sehingga indera manusia tidak dapat mendeteksi keberadaan pesan (Hafiz, 2019).

Watermark

Watermarking merupakan suatu teknik yang digunakan untuk penyembunyian data atau informasi rahasia ke citra digital baik berupa logo, teks ataupun citra lain. Informasi tersebut disisipkan tanpa merusak visual dari citra. Hal ini dilakukan agar orang lain tidak mengetahui data atau informasi yang ada di dalamnya (Fathiha, 2020).

Embedding process (encode) adalah suatu proses penyisipan pesan (*embeded message*) ke dalam sebuah *cover* obyek. Obyek ini bisa berupa gambar, dokumen, dan sebagainya. Proses ini dilakukan dengan menerima *input* atau masukan dari pengguna berupa parameter dari pengguna seperti embedded message (Sina et al., 2022).

Extracting process (decode) merupakan pendeteksian watermark. Algoritma pendeteksian watermark ini dapat menentukan apakah sebuah media digital khususnya citra digital terdeteksi watermark yang sesuai ataupun tidak (Gani & Setiyono, 2018).

Least Significant Bit

Least Significant Bit (LSB) merupakan pendekatan untuk menanamkan informasi pada citra. Menurut Adrian (2012) LSB merupakan cara paling sederhana agar penyisipan data pada citra dapat dilakukan. Pesan rahasia ditamankan ke dalam citra dengan mengubahnya ke dalam bentuk bit. Representasi biner digunakan dalam metode ini. Pada gambar dengan resolusi 800×600 bit yang dapat disimpan adalah 1,400,000 bit atau 180,000 byte (Satria & Antares, 2022).

Discrete Wavelet Transform

Discrete Wavelet Transform (DWT)

e-ISSN 2961-9009
p-ISSN 2963-1289

adalah dekomposisi citra pada frekuensi sub-band citra tersebut yang dihasilkan dengan cara penurunan level komposisi (Ujianto et al., 2020). Dimensi sinyal pada teknik ini dibagi menjadi dua yaitu *highpass* filter dan *lowpass* filter. Watermark disisipkan ke dalam citra digital dengan membandingkan koefisien DWT pada rentang frekuensi hasil dekomposisi citra asli. Rentang frekuensi yang memiliki nilai koefisien DWT terbesar adalah tempat yang paling signifikan untuk menyisipkan watermark (Gani & Setiyono, 2018).

Pemrosesan lanjut adalah dengan menggunakan IDWT. Proses tersebut dilakukan untuk merekonstruksi menjadi sinyal asal yang ditunjukkan pada persamaan tiga. Rekonstruksi merupakan kebalikan dari dekomposisi. Penggabungan koefisien DWT merupakan langkah pertama untuk rekonstruksi yang sebelumnya dengan menggunakan high dan low pass filter (Utami et al., 2022).

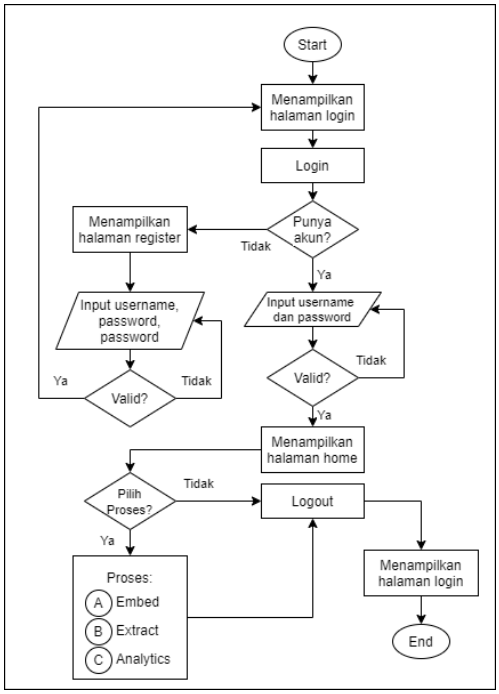
Peak Signal-to-Noise Rasio

PSNR (*Peak Signal-to-Noise Rasio*) bermakna dalam data yang dikodekan pada bit per sampel atau bit per *pixel*. PSNR merupakan ukuran dari puncak kesalahan yang menggunakan desibel. Apabila PSNR memiliki nilai tinggi maka artinya gambar tersebut memiliki kualitas gambar yang mendekati gambar aslinya (Desyani, 2022). Sistem penglihatan manusia sulit untuk mendeteksi perbedaan antara gambar asli dan modifikasi (watermark) pada nilai PSNR lebih dari 30 (Benyoucef Aicha dan Hamadouche, 2022).

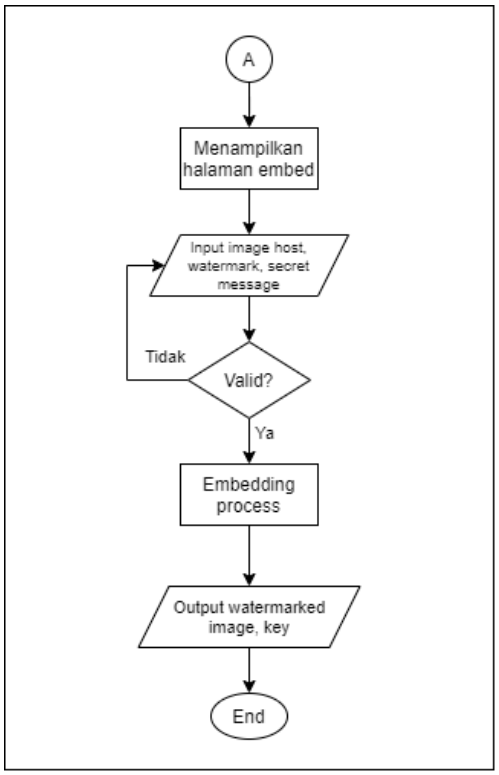
METODE PENELITIAN

Dalam sistem yang dibangun, sistem diusulkan berbasis web. Terdapat proses Sistem watermark yang dibangun memiliki *login*, *embedding*, dan *extracting*. Proses *login* digunakan untuk pengguna sehingga dapat mengakses ke dalam sistem. Gambar di bawah menunjukkan langkah untuk pengguna melakukan *login* baik admin maupun pengguna biasa.

Proses penyisipan dilakukan setelah pengguna melakukan *login* dan menuju ke halaman *embed*. Kemudian pengguna diharuskan untuk mengunggah gambar host, watermark, dan menentukan pesan rahasia. Jika valid maka proses dilakukan dan menghasilkan gambar dengan watermark dan kunci di dalamnya. Gambar 2 menunjukkan *flowchart embedding*.



Gambar 1. Flowchart Login

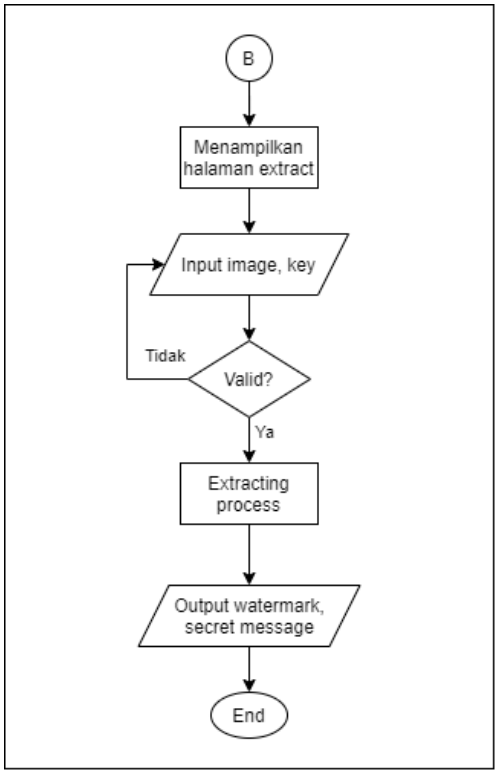


Gambar 2. Proses Penyisipan (*Embedding*)

Proses ekstraksi dapat dilakukan setelah pengguna melakukan login. Proses tersebut membutuhkan gambar yang terdapat watermark dan pesan rahasia dan kunci. Jika valid maka proses ekstraksi akan dimulai dan

e-ISSN 2961-9009
p-ISSN 2963-1289

menghasilkan gambar asli dan watermark. Gambar 3 menunjukkan *flowchart extracting*.



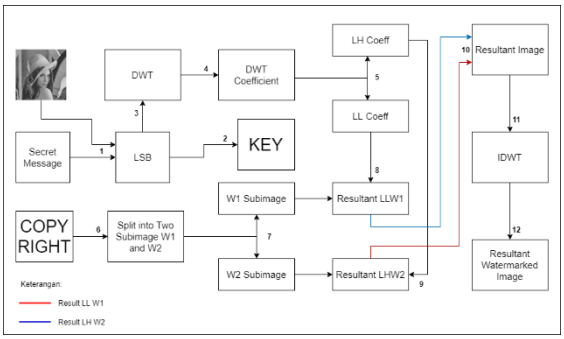
Gambar 3. Proses Ekstraksi (*Extraction*)

Penelitian ini menggunakan metode LSB dan DWT. Penyisipan pesan rahasia dilakukan metode LSB dan penyisipan watermark dengan membagi gambar watermark menjadi dua bagian dan menyisipkannya dalam gambar *host* yang sama. Pembagian tersebut membagi watermark (W) menjadi watermark satu (W1) dan dua (W2). Metode penyisipan pesan rahasia menggunakan metode LSB untuk mengubahnya ke dalam bentuk bit dan metode DWT untuk menyisipkan hasilnya ke dalam gambar.

Data yang digunakan berasal dari dataset Kaggle yang berupa gambar (Pexels 110k 768p JPEG) dan watermark (Large-scale Common Watermark Dataset). Sampel gambar tersebut ditunjukkan pada Gambar 4 di bawah.

Gambar 4. Sampel Data Gambar

Gambar dan watermark yang dipakai diubah menjadi 400×400 piksel dan *grayscale* terlebih dahulu. Penelitian ini juga menggunakan dua proses, yaitu penyisipan dan ekstraksi. Proses penyisipan atau *embedding* ditunjukkan pada Gambar 5 sebagai berikut.



Gambar 5. Proses Penyisipan

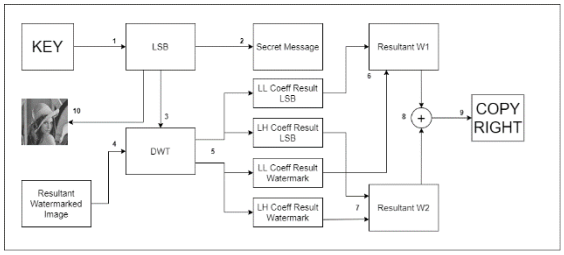
Proses penyisipan yang dilakukan dengan penjabaran sebagai berikut:

1. Menentukan gambar *host* dan pesan rahasia.
2. Gambar host diolah dengan menyisipkan pesan rahasia kemudian ditransformasikan dalam bentuk *file* sehingga menjadi *key* atau kunci.
3. Hasil gambar yang telah disisipkan pesan kemudian diimplementasikan dengan DWT.
4. Proses DWT menghasilkan koefisien, yaitu LL, LH, HL, dan HH.
5. Koefisien yang dipakai adalah LL dan LH.
6. Menentukan gambar watermark kemudian dibagi menjadi dua bagian.
7. Dua bagian gambar tersebut adalah sub-image W1 dan W2.
8. Proses penyisipan dilakukan dengan mengolah koefisien LL dan W1 sehingga hasilnya adalah Resultant LLW1.
9. Proses penyisipan juga dilakukan dengan mengolah koefisien LH dan W2 sehingga hasilnya adalah Resultant LHW2.
10. Proses 9 dan 10 merupakan variabel resultant yang menampung nilai koefisien dari masing-masing proses.
11. Nilai resultant diolah dengan IDWT untuk merekonstruksi gambar yang telah diproses.

e-ISSN 2961-9009
p-ISSN 2963-1289

12. Hasil rekonstruksi gambar memiliki gambar watermark dan pesan rahasia di dalamnya.

Proses ekstraksi atau *extracting* dilakukan untuk menghasilkan *output* berupa gambar asli dan watermark. Gambar 6 menunjukkan proses ekstraksi.



Gambar 6. Proses Ekstraksi

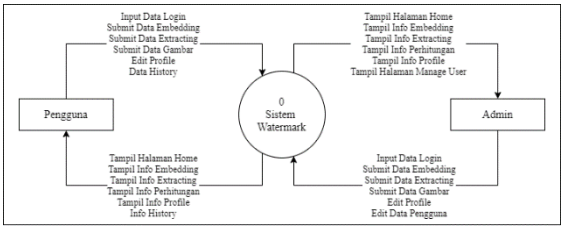
Proses ekstraksi tersebut dijabarkan sebagai berikut:

1. Memilih kunci yang valid kemudian diolah dengan metode LSB.
2. Hasil pengolahan tersebut adalah pesan rahasia.
3. Kunci yang telah diolah dengan DWT.
4. Begitu pula dengan gambar hasil proses penyisipan.
5. Pada kunci yang diterapkan DWT menghasilkan koefisien LL dan LH. Gambar ber-watermark juga menghasilkan LL dan LH.
6. Pengolahan nilai masing-masing koefisien LL menghasilkan nilai W1.
7. Pengolahan nilai masing-masing koefisien LH menghasilkan W2.
8. Hasil nilai yang ditransformasikan menjadi gambar kemudian digabungkan.
9. Setelah penggabungan dilakukan maka didapatkan watermark yang utuh.
10. Pengolahan LSB menghasilkan gambar host.

Secara singkat proses watermark pada penelitian ini adalah sebagai berikut:

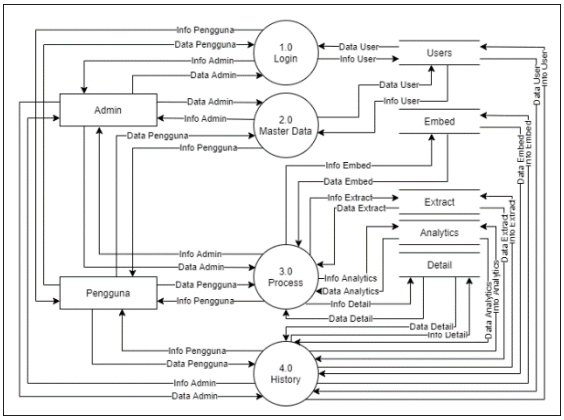
1. Penyisipan dilakukan dengan membagi watermark (W) menjadi dua bagian yaitu watermark bagian pertama (W1) dan watermark bagian kedua W2. Bagian pertama (W1) dan bagian kedua (W2) disisipkan pada transform domain. Pesan yang akan disisipkan pada gambar. Penyisipan menghasilkan kunci dan gambar yang terdapat pesan rahasia dan watermark.
2. Ekstraksi dilakukan dengan memproses kunci sehingga menghasilkan pesan rahasia dan gambar host. Pengolahan pada hasil proses dan gambar ber-watermark menghasilkan W1 dan W2. Penggabungan dilakukan sehingga menjadi watermark yang utuh.

Pembuatan sistem watermark berbasis web menggunakan perancangan sistem dengan Diagram Konteks di bawah.

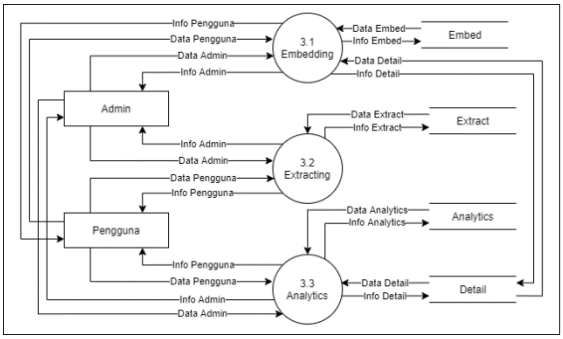


Gambar 7. Diagram Konteks

Diagram Alir Data Level 1 yang menggambarkan penelitian ini memiliki empat proses, yaitu proses *login*¸ manajemen data, proses, dan *history* atau riwayat.



Gambar 8. DAD Level 1 Sistem Watermark

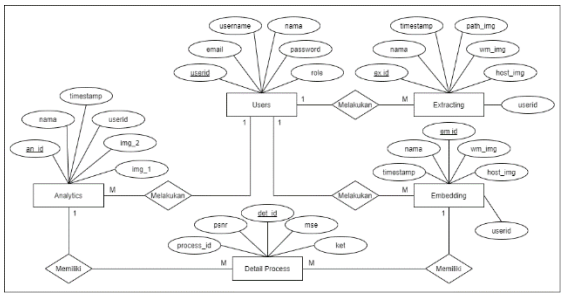


Gambar 9. DAD Level 2

DAD level 2 menggambarkan detail proses yang ada pada proses watermark. Proses tersebut terdiri dari *embedding* dan *extracting*.

e-ISSN 2961-9009
p-ISSN 2963-1289

Penelitian watermark dibangun dengan lima entitas, yaitu *Users*, *Extracting*, *Embedding*, *Analytics*, dan *Detail Process*. ERD yang ditunjukkan pada Gambar 10.

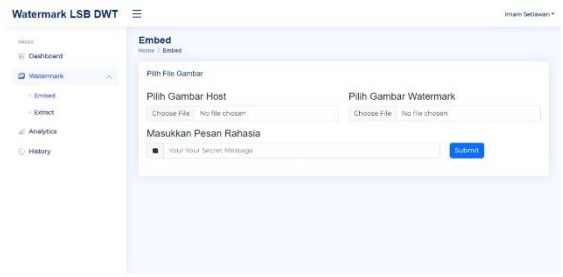


Gambar 10. ERD Sistem Watermark

HASIL DAN PEMBAHASAN

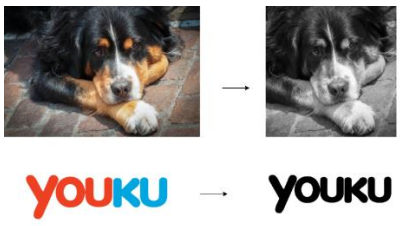
Proses Penyisipan (*Embedding*)

Sistem watermark dibangun berbasis web. Pada proses penyisipan, masukan yang dibutuhkan agar proses dapat berjalan adalah gambar, watermark, dan pesan rahasia. Gambar di bawah menunjukkan tampilan web untuk proses penyisipan.



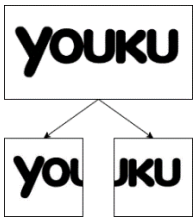
Gambar 11. Halaman Penyisipan

Data sampel gambar dan watermark terlebih dahulu diubah menjadi *grayscale* dan ukurannya ubah menjadi 400×400 piksel.

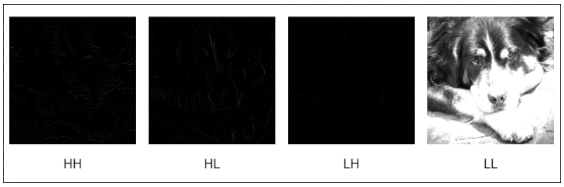


Gambar 12. Transformasi Gambar

Watermark yang telah ditransformasikan menjadi *grayscale* kemudian dibagi menjadi dua bagian (W1 dan W2) seperti yang ditunjukkan di Gambar 13. Terdapat empat hasil koefisien dari DWT yaitu LL, LH, HL, dan HH. Berikut ini merupakan hasil transformasi koefisien menjadi gambar. Gambar hasil transformasi ditunjukkan pada Gambar 14.



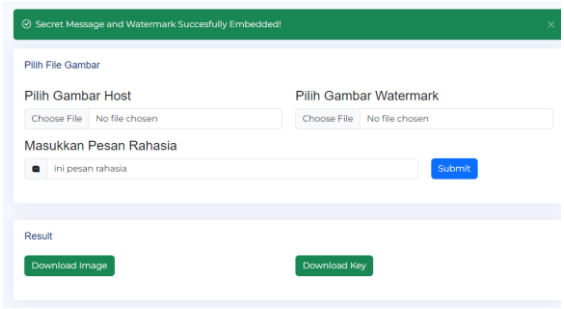
Gambar 13. Membagi Watermark menjadi Dua Bagian



Gambar 14. Transformasi Koefisien menjadi Gambar

Pesan yang dimasukkan ke dalam gambar berbentuk biner. Misal pesan yang disisipkan adalah ‘ini pesan rahasia’ maka hasil binernya adalah 011010010110111001101001000000011100000011001010111001101100001011011100010000001110010011000010110100000110000101110011011010010110000 1. Seluruh hasil proses penyisipan ditunjukkan pada Gambar 15 berikut.

Gambar 15. Hasil Gambar Proses Penyisipan



Gambar 16. Tampilan Web Hasil Proses Penyisipan

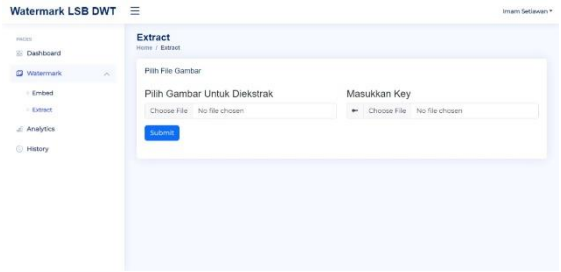
Hasil tampilan saat proses penyisipan ketika sukses akan menampilkan tombol unduh

e-ISSN 2961-9009
p-ISSN 2963-1289

gambar hasil proses penyisipan yang terdapat watermark dan pesan rahasia. Selain itu, terdapat tombol untuk mengunduh kunci yang dibutuhkan ketika proses ekstraksi dilakukan. Tampilan hasil tersebut ditunjukkan pada Gambar 16.

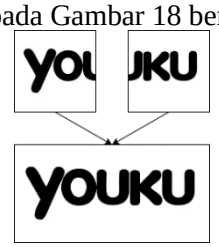
Proses Ekstraksi (*Extraction*)

Terdapat dua input yang dibutukan untuk menghasilkan watermark dan pesan rahasia, yaitu gambar hasil proses penyisipan dan kunci. Gambar 17 menunjukkan halaman untuk proses ekstraksi.



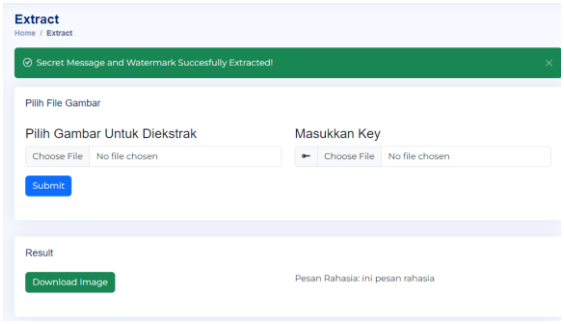
Gambar 17. Halaman Ekstraksi

Gambar hasil proses penyisipan dimasukkan dengan kunci yang sesuai akan menghasilkan watermark dan pesan rahasia. Pada proses ekstraksi terdapat dua bagian watermark. Hasil tersebut kemudian digabung menjadi watermark yang utuh. Proses tersebut dapat dilihat pada Gambar 18 berikut.



Gambar 18. Menggabungkan Watermark Hasil Ekstraksi

Ketika proses penyisipan berhasil dilakukan maka halaman web akan menampilkan tombol untuk mengunduh watermark yang telah disisipkan. Di samping tombol unduh tersebut terdapat pula hasil ekstraksi pesan rahasia. Tampilan hasil penyisipan ditunjukkan pada Gambar 19.



Gambar 19. Tampilan Hasil Proses Ekstraksi

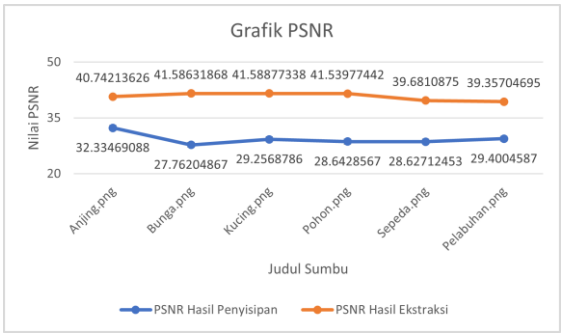
Pengujian

Data sampel gambar yang telah dijelaskan digunakan untuk pengujian. Terdapat enam sampel gambar yang diuji yaitu pesan yang berbeda dengan watermark yang sama. Enam sampel gambar tersebut adalah gambar anjing, bunga, kucing, pohon, sepeda, dan pelabuhan.

Masing-masing sampel disisipkan pesan dan gambar watermark. Proses penyisipan dilakukan untuk mendapatkan gambar yang di dalamnya terdapat watermark dan pesan rahasia serta kunci. Proses ekstraksi dilakukan untuk mendapatkan gambar watermark dan pesan rahasia. Watermark yang disisipkan dalam pengujian ditunjukkan pada Gambar 20 berikut.

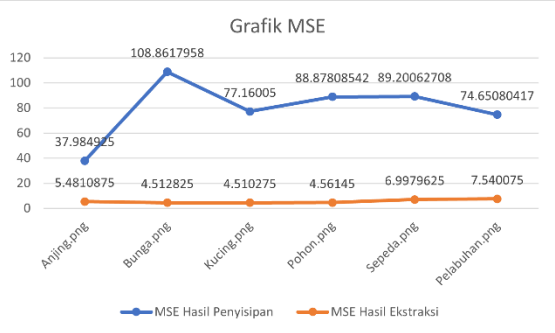
Gambar 20. Watermark yang Disisipkan

Pengujian juga melibatkan PSNR dan MSE. Pengujian dilakukan pada gambar *host* dan gambar hasil proses penyisipan serta pada gambar watermark asli dan watermark hasil proses ekstraksi. Pengujian terhadap enam sampel yang digunakan ditunjukkan pada Tabel 1.



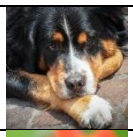
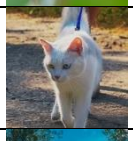
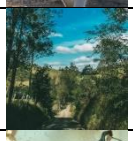
Gambar 21. Grafik PSNR

e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 22. Grafik MSE

Tabel 1. Pengujian Sampel

No	*Host*	Pesan	Hasil *Embed*	MSE	PSNR	Hasil *Extract*	MSE	PSNR	Pesan *Extract*
1		‘ini pesan rahasia pertama’		37.98	32.33		5.481	40.74	‘ini pesan rahasia pertama’
2		‘ini pesan rahasia kedua’		108.8	27.76		4.512	41.58	‘ini pesan rahasia kedua’
3		‘ini pesan rahasia ketiga’		77.16	29.25		4.510	41.58	‘ini pesan rahasia ketiga’
4		‘ini pesan rahasia keempat’		88.87	28.64		4.561	41.53	‘ini pesan rahasia keempat’
5		‘ini pesan rahasia kelima’		89.20	28.62		6.997	39.68	‘ini pesan rahasia kelima’
6		‘ini pesan rahasia keenam’		74.65	29.40		7.540	39.35	‘ini pesan rahasia keenam’

Percobaan hasil penyisipan memiliki nilai PNSR sebesar 29,337 dan MSE sebesar 79,45. Proses ekstraksi memiliki rata-rata nilai MSE sebesar 5,60 dan nilai PSNR sebesar 40,749. Sistem watermark yang dibangun dapat menampung pesan rahasia dan watermark sekaligus. Hasil penyisipan berdasarkan nilai PSNR yang didapat memiliki sedikit perbedaan yang dapat dilihat secara kasat mata. Namun pada hasil ekstraksi diperoleh hasil yang hampir sama dengan watermark asli. Hal tersebut dibuktikan bahwa nilai PSNR hasil ekstraksi memiliki rata-rata 40,749. Nilai PSNR dan MSE dapat dilihat pada Gambar 21 dan Gambar 22.

Di samping itu, hasil ekstraksi yang memiliki hasil PSNR di bawah 40 memiliki *noise* yang terdapat pada hasil ekstraksi. *Noise* tersebut dapat dilihat dengan mata telanjang.

KESIMPULAN

Penelitian yang dilakukan dengan menerapkan metode LSB dan DWT menghasilkan gambar yang menampung pesan rahasia dan watermark. Proses pengujian gambar hasil penyisipan menghasilkan nilai rata-rata PSNR 29,337 dan rata-rata MSE 79,45. Hal ini menunjukkan bahwa gambar hasil proses masih memiliki perbedaan yang dapat dilihat secara kasat mata dengan gambar asli.

Pengujian juga dilakukan dengan watermark hasil ekstraksi yang menghasilkan nilai rata-rata PSNR sebesar 40,749 dan MSE sebesar 5,60. Hal ini menunjukkan bahwa watermark yang dihasilkan mendekati watermark asli. Namun beberapa watermark terdapat *noise* yang dapat dilihat secara kasat mata.

Dengan demikian, penelitian yang telah dilakukan dapat menyisipkan pesan sekaligus menampung watermark. Watermark tersebut

e-ISSN 2961-9009
p-ISSN 2963-1289

digunakan untuk otentikasi kepemilikan sedangkan pesan rahasia dapat dijadikan alat komunikasi secara rahasia

ACKNOWLEDGEMENTS

Paper ini adalah hasil penelitian tugas akhir mahasiswa.

DAFTAR PUSTAKA

Benyoucef Aicha and Hamadouche, M. (2022). RONI-Based Medical Image Watermarking Using DWT and LSB Algorithms. In E. and A. L. Lejdel Brahim and Clementini (Ed.), *Artificial Intelligence and Its Applications* (pp. 468–478). Springer International Publishing.

Desyani, T. (2022). *Pengiriman Data Citra Berbasis Wavelet* (T. Hidayati, Ed.). Pascal Books.

Fathiha, V. A. (2020). Implementasi Teknik Watermarking Menggunakan Metode Discrete Wavelet Transform (DWT) dan Singular Value Decomposition (SVD) pada Citra Digital. *Jurnal Ilmiah Teknologi Informasi Asia*, *14*(2), 125–134.

Gani, S., & Setiyono, B. (2018). Teknik Invisible Watermarking Digital Menggunakan Metode DWT (Discrete Wavelet Transform). *Jurnal Sains Dan Seni ITS*, *7*(2), 24–30. https://doi.org/10.12962/j23373520.v7i2.29845

Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, *17*(1 April), 194–198.

Satria, W., & Antares, J. (2022). Steganografi Metode Least Significant Bit (LSB) Dan End Of File (EoF) Pada Keamanan Data Digital. *Jurnal Teknologi Informasi*, *6*(2).

Septiani Muzahardin, Y., & Fauzi, A. (2022). Perbaikan Citra Digital Pada Foto Dengan Menggunakan Metode Retinex. *Jurnal Teknik Informatika Kaputama (JTIK)*, *6*(1).

Sina, D. R., Kiu, G. A., Djahi, B. S., & Pandie, E. S. Y. (2022). Aplikasi Keamanan Pesan (.TXT) Menggunakan Metode Triple Des Dan Metode Kombinasi LSB Dan BLUM-BLUM-SHUB. *Jurnal Komputer Dan Informatika*, *10*(2), 204–209. https://doi.org/10.35508/jicon.v10i2.8465

Ujianto, E. I. H., Amrulloh, A., Saputro, T. H., Wibisono, G., Setiawati, I., Saifuddin, Mido, A. R., Ikromina, F. I., Waluyo, T., & Hidayati, N. (2020). *Intelligent System and Information Security [an Introduction]* (T. Widodo, Ed.). Universitas Teknologi Yogyakarta. www.uty.ac.id

Utami, M., Rismawan, T., & Ristian, U. (2022). Implementasi Metode Discrete Wavelet Transform (DWT) Pada Watermarking Citra Digital Keaslian Karya Berbasis Web. *Jurnal Komputer Dan Aplikasi*, *10*(1), 124–135.