Jurnal Teknik
Vol. 05 No. 03 Oktober 2025
Page : 1652-1659

S I L I T E K
ISSN 2808-5825 (Online)

PENYEMATAN INFORMASI DIGITAL MENGGUNAKAN SINGULAR VALUE DECOMPOSITION DENGAN PERANGKAT LUNAK SIMULASI

Naufal Faariz Habiibi[1], Ahmad Idlof Dzouqun[2], Herwin Melyanus[3]
[1,2,3]Program Studi Teknik Elektro Universitas Pertahanan Republik Indonesia, naufalf4ariz@gmail.com

ABSTRAK

Perkembangan teknologi informasi menuntut adanya metode yang andal untuk menjaga kerahasiaan, keaslian, dan keamanan data digital. Salah satu pendekatan yang banyak diteliti adalah teknik steganografi dan watermarking berbasis pengolahan citra digital. Penelitian ini membahas penyematan informasi digital menggunakan metode *Singular Value Decomposition* (SVD) dengan bantuan perangkat lunak simulasi. Metode SVD dipilih karena mampu memisahkan citra ke dalam komponen singular yang relatif stabil terhadap berbagai transformasi, sehingga informasi yang disisipkan tetap terjaga kualitas dan integritasnya. Pada tahap implementasi, citra host didekomposisi menggunakan SVD, kemudian informasi digital berupa teks maupun citra disisipkan ke dalam nilai singular tertentu. Proses penyematan dan ekstraksi diuji dengan perangkat lunak simulasi MATLAB, sehingga dapat dianalisis kinerja metode berdasarkan parameter objektif, seperti *Peak Signal-to-Noise Ratio* (PSNR), *Mean Squared Error* (MSE), serta ketahanan terhadap manipulasi citra dasar. Hasil pengujian menunjukkan bahwa metode SVD mampu menyisipkan informasi secara imperseptibel dengan nilai PSNR yang tinggi dan MSE yang rendah, sehingga citra stego hampir tidak dapat dibedakan dari citra asli secara visual. Selain itu, proses ekstraksi berhasil mengembalikan informasi dengan akurasi tinggi. Dengan demikian, metode SVD terbukti efektif untuk penyematan informasi digital, serta berpotensi diterapkan dalam sistem keamanan data dan perlindungan hak cipta digital.

Kata kunci : *Singular Value Decomposition, Steganografi, Watermarking, Penyematan Informasi Digital*

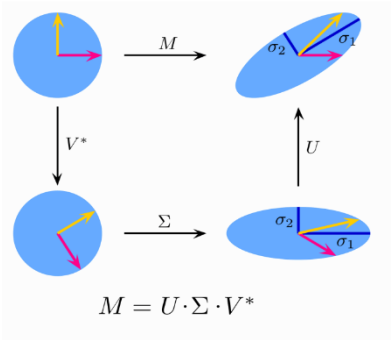
Penerbit : Fakultas Teknik Universitas Pasifik Morotai

1 PENDAHULUAN

Kemajuan teknologi digital yang pesat membawa dampak signifikan pada cara penyimpanan, transmisi, dan perlindungan data digital[1].Di era informasi ini, keamanan data menjadi aspek yang sangat penting, khususnya untuk media digital seperti gambar, audio, dan video[2]. Salah satu teknik yang banyak digunakan untuk menjaga kerahasiaan dan integritas informasi adalah steganografi, yakni metode penyembunyian pesan tersembunyi dalam media digital sehingga pesan tersebut tidak terdeteksi oleh pihak yang tidak berwenang[3]. Steganografi memiliki keunggulan dibandingkan enkripsi biasa karena tidak hanya mengamankan data tetapi juga menyembunyikan keberadaannya[4].

Dalam konteks pengolahan citra digital, teknik Singular Value Decomposition (SVD) menjadi salah satu metode yang menjanjikan untuk implementasi steganografi[5].SVD merupakan teknik matematis yang mampu mendekomposisi matriks citra menjadi tiga matriks komponen: matriks U (left singular vectors), matriks Σ

(singular values), dan matriks V^T(right singular vectors)[6]. Keunggulan SVD terletak pada kemampuannya mempertahankan informasi esensial dari citra dalam singular values, sehingga modifikasi pada nilai singular ini dapat dilakukan dengan tingkat gangguan minimal terhadap kualitas visual citra asli[7].



Gambar 1. Singular Value Decomposition

Menurut Golub dan Van Loan (2013) dalam bukunya "*Matrix Computations*", *Singular Value Decomposition* (SVD) adalah teknik dekomposisi matriks yang paling umum digunakan dalam analisis data. Mereka menjelaskan bahwa SVD memecah matriks menjadi tiga matriks yang lebih sederhana, yaitu matriks *singular value*, matriks *left singular vector*, dan matriks *right singular vector*[8]. Matriks *singular value* berisi nilai-nilai singular value yang menggambarkan besarnya kontribusi setiap vektor singular dalam matriks asli. Sedangkan matriks *left singular vector* dan *right singular vector* berisi vektor-vektor singular yang digunakan untuk merekonstruksi fungsi utama dari SVD adalah untuk mengurangi dimensi data dan mempercepat proses komputasi[9]. SVD juga digunakan dalam berbagai aplikasi seperti analisis data, pengolahan citra, dan pemrosesan sinyal. Dengan menggunakan teknik SVD, kita dapat melakukan reduksi dimensi, kompresi data, dan analisis faktor dalam data mining dan machine learning[10].

2 METODE PENELITIAN

Penelitian ini adalah studi eksperimental yang menggunakan simulasi digital untuk mengeksplorasi implementasi teknik penyisipan informasi, atau steganografi, dengan memanfaatkan Singular Value Decomposition (SVD). Pendekatan ini didasarkan pada karakteristik unik dari nilai singular SVD, yang memungkinkan modifikasi minimal pada citra sambil mempertahankan kualitas visual aslinya. Secara umum, proses penyisipan dan ekstraksi informasi digital melibatkan dekomposisi citra *host*, yaitu citra utama yang berfungsi sebagai media untuk menyembunyikan informasi. Dalam studi ini, informasi yang disisipkan disebut watermark, yang bisa berupa gambar atau teks. Meskipun jenis watermark yang berbeda memiliki karakteristik dan metode penyisipan yang spesifik, keduanya tetap mengandalkan prinsip dasar SVD untuk menyembunyikan data secara efektif.

2.1 Watermark Teks

Watermark berbentuk informasi berupa teks. Dalam penelitian ini, teks yang digunakan mencakup kalimat sederhana, seperti "produk akan dikirim", hingga paragraf panjang berisi deskripsi geografis maupun narasi tertentu. Sebelum dilakukan penyisipan, teks terlebih dahulu diubah ke dalam representasi biner ASCII 8-bit,

sehingga setiap karakter direpresentasikan oleh delapan bit data digital.Proses penyisipan dilakukan pada salah satu kanal warna citra host, biasanya pada kanal biru (blue channel). Kanal ini dipilih karena lebih toleran terhadap perubahan nilai piksel dan perbedaan yang terjadi tidak mudah terlihat secara visual oleh mata manusia. Setiap bit pesan biner kemudian disisipkan pada elemen diagonal matriks singular (Σ) dari kanal tersebut dengan menambahkan nilai kecil (misalnya sebesar 10^{-4}), sehingga perubahan tidak merusak kualitas citra secara kasatmata.Meskipun watermark berbentuk teks tidak dapat dilihat secara langsung setelah proses embedding, informasi yang disisipkan tetap dapat diekstraksi kembali. Ekstraksi dilakukan dengan membandingkan nilai singular yang telah dimodifikasi dengan nilai awal, lalu mengonversi kembali bit biner ke bentuk teks aslinya.Secara garis besar, terdapat empat tahapan utama dalam prosedur penelitian ini, yaitu pra-pemrosesan citra, dekomposisi matriks menggunakan Singular Value Decomposition (SVD), rekonstruksi citra hasil embedding, serta ekstraksi informasi. Seluruh tahapan ini dilaksanakan menggunakan aplikasi simulasi untuk menjamin ketelitian numerik dan kemudahan visualisasi.

a. Pra-pemrosesan

Tahap pertama dalam proses adalah melakukan pra-pemrosesan terhadap citra yang digunakan. Gambar host dan gambar watermark dibaca dari file dengan format JPG atau PNG, lalu dikonversi ke dalam tipe data numerik bertipe double. Konversi ini penting untuk memungkinkan pelaksanaan operasi linear dan dekomposisi matriks yang presisi. Selain itu, dimensi dari gambar watermark disesuaikan agar memiliki ukuran yang sama dengan gambar host, sehingga proses penyisipan dapat dilakukan secara langsung dan proporsional.

Untuk penyisipan teks sebagai watermark, proses pra-pemrosesan juga mencakup ekstraksi kanal warna biru (*blue channel*) dari gambar host. Kanal ini dipilih karena cenderung lebih toleran terhadap perubahan nilai piksel dan memberikan kestabilan visual yang lebih baik dibandingkan kanal merah atau hijau.

b. Penerapan Singular Value Decomposition (SVD)

Setelah proses pra-pemrosesan selesai, langkah berikutnya adalah melakukan dekomposisi matriks menggunakan metode SVD. Fungsi svd() pada aplikasi simulasi digunakan untuk memecah setiap kanal gambar menjadi tiga matriks, yaitu U, Σ, dan VT. Matriks Σ yang mengandung nilai singular menjadi fokus utama dalam proses penyisipan informasi.Sementara itu, untuk watermark dalam bentuk teks, proses penyisipan dilakukan secara langsung pada elemen diagonal matriks Σ dengan menambahkan nilai kecil (≈ 10-4) berdasarkan representasi biner dari pesan teks. Dengan pendekatan ini, teks dapat disisipkan ke dalam gambar tanpa menyebabkan perubahan visual yang mencolok.

c. Rekonstruksi Citra

Setelah matriks singular berhasil dimodifikasi, citra hasil embedding direkonstruksi kembali menggunakan formula:

$A' = U\,\Sigma'\,VT$

Rekonstruksi ini dilakukan untuk masing-masing kanal (R, G, B) jika gambar dalam format RGB, atau hanya pada satu kanal untuk penyisipan teks. Gambar hasil rekonstruksi kemudian dikonversi kembali ke format citra

standar dan disimpan dalam bentuk file berformat PNG, yang dipilih karena mendukung kompresi tanpa kehilangan informasi (*lossless compression*).

d. Ekstraksi Informasi

Tahap terakhir adalah proses ekstraksi informasi dari citra hasil penyisipan. Untuk watermark berbentuk teks, nilai singular dari citra yang telah dimodifikasi dibandingkan dengan nilai singular awal guna memperoleh bit-bit biner dari pesan. Bit-bit ini kemudian direkonstruksi menjadi teks menggunakan metode konversi ASCII.

2.2 Flowchart Sistem

Gambar 2. Flowchart Sistem

Pada skenario ini, pesan teks berupa kalimat (contoh: "semua akses ke daerah tersebut telah ditutup") disisipkan ke dalam citra host. Proses ini secara spesifik berfokus pada penyisipan ke salah satu kanal warna, umumnya kanal biru, karena perubahan pada kanal ini cenderung kurang terlihat secara visual pada citra RGB. Tahapannya meliputi:

1. Konversi Teks ke Biner: Pesan teks diubah menjadi representasi biner.
2. Dekomposisi SVD Kanal Biru: Kanal biru dari citra host didekomposisi menggunakan SVD.
3. Modifikasi Nilai Diagonal Matriks S: Bit-bit biner dari pesan disisipkan ke dalam nilai diagonal matriks Σ (singular values) dari kanal biru. Perubahan yang terjadi sangat kecil, sehingga citra tetap terlihat serupa dengan aslinya.

4. Ekstraksi Pesan: Untuk mengekstraksi pesan, nilai singular hasil penyisipan dibandingkan dengan nilai awal, kemudian dikonversi kembali dari biner ke teks.

3 HASIL DAN PEMBAHASAN

Dalam skenario penyisipan teks, pesan terlebih dahulu dikonversi ke dalam bentuk biner sebelum disisipkan pada kanal biru citra host. Pemilihan kanal biru didasarkan pada rendahnya sensitivitas visual manusia terhadap warna tersebut, sehingga perubahan yang terjadi tidak mudah terdeteksi. Hasil ekstraksi menunjukkan tingkat akurasi yang tinggi, di mana pesan dapat dipulihkan secara utuh dari citra hasil embedding. Temuan ini menegaskan bahwa penerapan metode Singular Value Decomposition (SVD) efektif untuk menyisipkan informasi berbasis teks dengan tingkat robustness yang baik terhadap gangguan visual.

Pengujian lebih lanjut melalui konversi lintas format, baik dari citra berwarna (RGB) ke grayscale maupun sebaliknya, menghasilkan kinerja yang konsisten. Penyesuaian dimensi matriks dalam proses ini mampu menjaga stabilitas embedding, sehingga menunjukkan fleksibilitas metode untuk berbagai skenario praktis. Selain itu, citra hasil steganografi tetap mempertahankan kualitas visual yang menyerupai citra asli tanpa adanya indikasi watermark secara kasatmata.

Secara keseluruhan, metode ini memiliki tiga keunggulan utama, yaitu terjaganya kualitas visual citra, keberhasilan ekstraksi pesan dengan tingkat akurasi tinggi, serta kemampuan adaptasi terhadap berbagai format citra. Dibandingkan dengan metode spasial sederhana seperti Least Significant Bit (LSB), pendekatan berbasis SVD menawarkan kestabilan struktur yang lebih baik serta ketahanan terhadap manipulasi ringan, termasuk kompresi maupun proses filtering.

3.1 Hasil Penyisipan Pesan Dalam Gambar

Gambar yang digunakan pada penelitian kali ini adalah peta Kabupaten Magetan dengan ukuran 1.280 x 1.067 pixel. Gambar diuji dengan menyisipkan pesan yaitu semua akses ke semua daerah tersebut telah ditutup dalam saluran warna biru menggunakan metode SVD (Singular Value Decomposition). Berikut adalah hasil penyisipan pesan pada gambar tersebut.

Gambar 3. Gambar Original

Gambar 3 merupakan gambar original sebelum disisipkan pesan berupa “semua akses ke daerah tersebut telah ditutup”

Gambar 4. Gambar setelah disisipkan pesan

Gambar 4 merupakan gambar setelah disisipkan pesan berupa “semua akses ke daerah tersebut telah ditutup”

```
>> ppp
Extracted Message: semua akses ke daerah tersebut telah ditutup
```

Gambar 5. Hasil Penyisipan Pesan Pada Gambar

Gambar 5 merupakan hasil ekstraksi dari pesan yang telah disisipkan pada gambar setelah disisipkan pesan menggunakan perangkat lunak aplikasi

3.2 Perbedaan Gambar Asli dan Gambar dengan Watermark SVD

1. **Perbedaan Visual**
   - Secara kasat mata, citra hasil penyisipan hampir tidak dapat dibedakan dari citra aslinya. Hal ini menunjukkan bahwa metode SVD berhasil menjaga kualitas visual citra host.
   - Kanal biru yang digunakan sebagai media embedding tidak menimbulkan distorsi signifikan, karena sensitivitas mata manusia terhadap perubahan warna biru relatif rendah.
2. **Perubahan Statistik Piksel**
   - Jika dilakukan analisis kuantitatif (misalnya menggunakan **MSE – Mean Squared Error** atau **PSNR – Peak Signal-to-Noise Ratio**), kemungkinan besar perbedaan nilai cukup kecil (MSE rendah, PSNR tinggi > 40 dB).
   - Histogram citra asli dan citra dengan watermark juga diperkirakan sangat mirip, hanya terdapat sedikit pergeseran distribusi intensitas pada kanal biru.
3. **Ketahanan terhadap Gangguan Visual**
   - Penyisipan melalui modifikasi elemen diagonal matriks singular (Σ) bersifat stabil dan tidak merusak struktur global citra. Oleh karena itu, watermark tidak tampak meskipun gambar diperbesar atau diamati detail.
4. **Keberhasilan Ekstraksi**
   - Melalui proses ekstraksi, pesan biner yang disisipkan dapat dipulihkan kembali ke dalam bentuk teks dengan akurasi tinggi. Hal ini menunjukkan robustness metode SVD terhadap proses embedding dan perbedaan format citra.

4 KESIMPULAN

Berdasarkan rangkaian pengujian yang dilakukan, dapat disimpulkan bahwa metode steganografi berbasis **Singular Value Decomposition (SVD)** memiliki kemampuan yang andal dalam menyisipkan informasi, baik berupa data citra maupun teks, ke dalam citra host dengan tingkat **imperceptibility** yang sangat baik. Proses embedding yang dilakukan melalui kanal RGB, khususnya kanal biru, menghasilkan citra stego yang hampir identik dengan citra asli tanpa menimbulkan distorsi yang berarti pada kualitas visual.

Selain itu, tahap ekstraksi membuktikan efektivitas metode ini dengan tingkat akurasi yang tinggi, di mana data watermark maupun pesan teks dapat dipulihkan kembali secara utuh sesuai dengan bentuk awalnya. Keberhasilan ini menegaskan bahwa metode SVD tidak hanya menjaga kualitas visual citra, tetapi juga menjamin **keandalan dalam retreival informasi**.

Hasil tersebut memperlihatkan bahwa SVD memiliki potensi besar untuk diimplementasikan dalam berbagai aplikasi **keamanan data digital**. Metode ini mampu memberikan keseimbangan antara kualitas citra, kerahasiaan informasi, serta ketahanan terhadap gangguan seperti konversi format, kompresi ringan, maupun filtering. Dengan fleksibilitas yang ditunjukkan dalam beragam skenario praktis, SVD dapat dijadikan salah satu pendekatan unggulan untuk kebutuhan **watermarking, steganografi, dan perlindungan hak cipta digital** pada era pertukaran data yang semakin intensif.

DAFTAR PUSTAKA

[1] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Inf.*, vol. 11, no. 2, 2020, doi: 10.3390/info11020110.

[2] K. M. Hosny, A. Magdi, O. ElKomy, and H. M. Hamza, "Digital image watermarking using deep learning: A survey," *Comput. Sci. Rev.*, vol. 53, p. 100662, 2024, doi: https://doi.org/10.1016/j.cosrev.2024.100662.

[3] Z. Wang *et al.*, "Data Hiding With Deep Learning: A Survey Unifying Digital Watermarking and Steganography," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 6, pp. 2985–2999, 2023, doi: 10.1109/TCSS.2023.3268950.

[4] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali, "An efficient and secure technique for image steganography using a hash function," *PeerJ Comput. Sci.*, vol. 8, no. 2021, pp. 1–18, 2022, doi: 10.7717/PEERJ-CS.1157.

[5] M. Chinnusami, D. Kolli, S. Shreela, R. Anbazhagan, and R. Amirtharajan, "Analysis of hybrid integer wavelet transform and singular value decomposition for image steganography under various noise conditions," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-17020-2.

[6] T. K. Araghi and D. Megías, "Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking," *Multimed. Tools Appl.*, vol. 83, no. 2, pp. 3895–3916, 2024, doi: 10.1007/s11042-023-15554-z.

[7] G. Ye, H. Wu, M. Liu, and X. Huang, "Reversible image-hiding algorithm based on singular value sampling and compressive sensing," *Chaos, Solitons & Fractals*, vol. 171, p. 113469, 2023, doi: https://doi.org/10.1016/j.chaos.2023.113469.

[8] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci. Int.*, vol. 320, p. 110691, 2021, doi: https://doi.org/10.1016/j.forsciint.2021.110691.

[9] B. Kim, "Dimensionality and data size reduction using singular value decomposition," *Issues Inf. Syst.*, vol. 25, no. 3, pp. 231–237, 2024, doi: 10.48009/3_iis_2024_118.

[10] J. A. Tropp and R. J. Webber, "Randomized algorithms for low-rank matrix approximation: Design,

analysis, and applications," vol. 91125, pp. 1–61, 2023, [Online]. Available: http://arxiv.org/abs/2306.12418