SISTEMATIK
JURNAL SISTEM INFORMASI DAN INFORMATIKA

Aletheia : Sistem Steganografi berbasis Binarized Neural Network untuk Media Gambar Digital

Sigit Prayoga [1], Silmi Nindi Putri [2], Jeni Adi Hidayat [3]

[1,2,3] *Program Studi Informatika, Universitas SIliwangi, Jl. Mugarsari, Kec. Tamansari, Kota Tasikmalaya, Indonesia*

INFORMASI ARTIKEL

Received: May, 24, 2025
Reviewed: June, 07, 2025
Available online: June, 30, 2025

KORESPONDEN

E-mail: prayogasigit53@gmail.com
silmininip5@gmail.com
jeniadihidayat@gmail.com

A B S T R A C T

The advancement of information technology demands increasingly sophisticated data security systems, especially in safeguarding the confidentiality of information transmitted via digital media. Steganography, as a method of hiding information within media such as images, emerges as an effective solution. This research introduces Aletheia, a steganography system that adopts a Binarized Neural Network (BNN) approach to enhance efficiency and security in the embedding and extraction processes within digital images. BNN was chosen for its ability to reduce computational complexity, allowing the system to be implemented on resource-constrained devices without sacrificing accuracy. Aletheia consists of two main stages: encoding, which involves embedding secret messages into images while maintaining visual quality, and decoding, which ensures high-accuracy message extraction. Evaluation is conducted on various parameters, including imperceptibility (using PSNR and SSIM), embedding capacity, and extraction success rate. Experimental results demonstrate that Aletheia effectively hides data with minimal visual distortion and reliable extraction performance. This research opens new opportunities for the application of intelligent steganography in digital information security.

KEYWORD:
Binarized Neural Network, Deep Learning, Digital Image, Information Security, Steganography.

A B S T R A K

Perkembangan teknologi informasi menuntut sistem keamanan data yang semakin canggih, terutama dalam menjaga kerahasiaan informasi yang dikirimkan melalui media digital. Steganograf, sebagai metode persembunyian informasi dalam media seperti gambar, menjadi salah satu solusi efektif. Penelitian ini memperkenalkan Aletheia, sebuah sistem steganografi yang mengadopsi pendekatan Binarized Neural Network (BNN) untuk meningkatkan efisiensi dan keamanan dalam proses penyisipan dan ekstraksi data pada citra digital. BNN dipilih karena kemampuannya dalam mengurangi kompleksitas komputasi, sehingga memungkinkan penerapan sistem pada perangkat dengan sumber daya terbatas tanpa mengorbankan akurasi. Sistem Aletheia terdiri dari dua tahap utama : encoding, yaitu penyisipan pesan rahasia ke dalam gambar dengan mempertahankan kualitas visual, dan decoding, yaitu proses ekstraksi pesan dengan akurasi tinggi. Evaluasi dilakukan terhadap berbagai parameter, seperti imperceptibility (menggunakan PSNR dan SSIM), kapasitas penyisipan, serta tingkat keberhasilan ekstraksi. Hasil eksperimen menunjukkan bahwa Aletheia mampu menyembunyikan data secara efektif dengan distori visual minimal dan performa ekstraksi yang andal. Penelitian ini membuka peluang baru penerapan steganografi cerdas yang efisien dalam bidang keamanan informasi digital.

KATA KUNCI:
Binarized Neural Network, Deep Learning, Citra Digital, Keamanan Informasi, Steganografi.

Attribution-NonCommercial 4.0 International. Some rights reserved

PENDAHULUAN

Di era digital seperti sekarang, arus informasi mengalir begitu cepat melalui berbagai media. Gambar, video, hingga pesan teks menjadi bagian dari komunikasi harian, baik secara personal maupun dalam sistem informasi yang lebih besar. Sayangnya, seiring dengan pesatnya pertukaran data ini, muncul pula tantangan besar dalam hal keamanan informasi. Isu seperti penyadapan, pencurian data, atau manipulasi pesan menjadi ancaman nyata yang tidak bisa diabaikan. Dalam konteks ini, perlindungan data bukan hanya soal enkripsi tapi juga soal bagaimana data bisa "disembunyikan" secara cerdas [1].

Steganografi hadir sebagai salah satu solusi, yaitu dengan menyisipkan pesan rahasia ke dalam media digital, seperti citra, tanpa mengubah tampilan visualnya secara siginifikan [2]. Artinya, pesan tidah hanya dienkripsi, tapi juga dibuat seolah-olah tidak pernah ada di sana. Namun, metode steganografi klasik punya keterbatasan: kapasitas penyisipan yang kecil, kualitas visual yang menurun, dan sistem yang tidak tahan terhadap manipulasi digital seperti kompresi, cropping, atau noise [3][4].

Untuk menjawab tantangan tersebut, penelitian ini memperkenalkan Aletheia yaitu sebuah sistem steganografi yang memanfaatkan pendekatan Binarized Neural Network (BNN). BNN merupakan jenis lightweight neural network yang hanya menggunakan representasi biner (+1 atau -1), sehingga secara drastis mengurangi beban komputasi dibandingkan jaringan saraf biasa [5]. Dengan karakteristik ini, Aletheia dirancang tidak hanya untuk menyisipkan pesan secara aman dan tersembunyi, tapi juga agar tetap efisien dan bisa berjalan di perangkat dengan sumber daya terbatas, seperti IoT, smartphone, atau sistem tertanam [6][7].

Aletheia terdiri dari dua proses utama : *encoding*, yaitu proses menyisipkan data ke dalam gambar; dan *decoding*, yaitu proses mengekstraksi kembali pesan dari gambar yang telah dimodifikasi. Sistem ini diuji menggunakan parameter evaluasi seperti PSNR dan SSIM untuk mengukur seberapa "tak terlihat" pesan tersebut, serta akurasi ekstraksi untuk mengukur keberhasilan pembacaan ulang data [8]. Hasil yang didapat dapat menunjukkan bahwa pendekatan BNN tidak hanya memungkinkan efisiensi tinggi, tapi juga menjaga kualitas visual citra tetap utuh sambil menyisipkan informasi secara efektif [9].

Dengan pendekatan ini, penelitian tidak hanya menunjukkan potensi baru dalam pengembangan steganografi modern, tetapi juga membuka ruang bagi penerapan di dunia nyata khususnya dalam bidang keamanan data digital, sensor pintar, atau komunikasi rahasia yang aman namun tetap ringan dari sisi sumber daya.

TINJAUAN PUSTAKA

Steganografi sebagai teknik penyembunyian data telah lama digunakan untuk menjaga kerahasiaan informasi digital. Beberapa pendekatan klasik yang umum diterapkan antara lain metode Least Significant Bit (LSB), Pixel Value Differencing (PVD), dan Transform Domain seperti Discrete Cosine Transform (9DCT) maupun Discrete Wavelet Transform (DWT) [10]. Meskipun teknik-teknik ini tergolong sederhana, mereka memiliki keterbatasan dari sisi ketahanan terhadap manipulasi (robustness), kapasitas penyisipan data, serta kualitas visual hasil steganografi.

Penelitian oleh Siringoringo (2016) menggunakan metode LSB untuk menyisipkan data teks ke dalam citra digital, dan menganalisis kualitas visual menggunakan parameter PSNR. Hasilnya menunjukkan bahwa metode ini memiliki imperceptibility yang baik, namun tidak tahan terhadap kompresi [11]. Sementara itu, Rachman (2020) menggabungkan metode PVD dan LSB untuk meningkatkan kapasitas penyisipan tanpa menurunkan kualitas visual secara signifikan, namun penggunaan metode ini bekum optimal jika diterapkan pada perangkat dengan resource terabatas [12].

Seiring perkembangan teknologi, pendekatan berbasis kecerdasan buatan mulai diadopsi dalam bidang steganografi. Salah satu inovasi yang relevan adalah penerapan Neural Networks dalam proses penyisipan dan ekstraksi data. Penelitian terbaru Penelitian terbaru menunjukkan bahwa Convolutional Neural Network (CNN) mampu menghasilkan sistem steganografi end-to-end dengan performa visual dan keamanan yang lebih baik dibandingkan metode klasik [13]. Namun demikian, pemrosesan CNN tergolong berat dan tidak ideal untuk perangkat dengan keterbatasan memori dan daya komputasi seperti pada IoT dan perangkat mobile.

Steganografi

Steganografi bukan hanya menyembunyikan data, tetapi juga bertujuan untuk tidak menimbulkan kecurigaan. Ini berbeda dari kriptografi yang meskipun mengamankan isi pesan, tetap menunjukkan bahwa ada informasi yang disembunyikan. Dalam konteks gambar digital, teknik paling umum adalah Least Significant Bit (LSB), di mana data disisipkan ke dalam bit terkecil dari piksel gambar sehingga perubahan visualnya hampir tak terlihat. Selain itu, pendekatan domain frekuensi seperti DCT dan DWT digunakan untuk meningkatkan ketahanan terhadap kompresi atau manipulasi.

Dalam konteks keamanan informasi, steganografi tidak berdiri sendiri tetapi sering dipadukan dengan teknik lain seperti kriptografi untuk meningkatkan tingkat perlindungan.

Dengan mengenkripsi pesan terlebih dahulu sebelum disisipkan ke dalam media, sistem menjadi dua kali lebih

aman: isi pesan terlindungi oleh enkripsi, dan keberadaannya tersembunyi oleh steganografi. Hal ini membuat proses deteksi dan pembacaan pesan oleh pihak tidak berwenang menjadi jauh lebih sulit, bahkan jika mereka berhasil mendeteksi adanya manipulasi pada media digital.

Teknologi steganografi terus berkembang seiring dengan meningkatnya kebutuhan akan perlindungan data di berbagai sektor seperti militer, perbankan, dan komunikasi pribadi. Teknik-teknik modern mulai memanfaatkan transformasi domain seperti Fourier dan Wavelet, serta pendekatan berbasis pembelajaran mesin untuk menentukan lokasi optimal penyisipan data. Keunggulan dari pendekatan ini adalah kemampuannya menyesuaikan dengan karakteristik gambar secara dinamis, sehingga hasil penyisipan menjadi lebih tersembunyi secara alami dan sulit dideteksi oleh algoritma steganalisis konvensional.

Binarized Neural Network (BNN)

BNN merupakan salah satu pengembangan dari jaringan saraf tiruan yang bertujuan mengurangi kompleksitas komputasi dengan mengganti bobot dan aktivasi menjadi bentuk biner. BNN sering digunakan pada perangkat dengan keterbatasan sumber daya seperti perangkat IoT atau mobile. Walaupun terlihat sederhana, BNN tetap memiliki kemampuan representasi cukup kuat karena desain arsitektur dan pelatihannya yang spesifik. Dalam bidang pengolahan citra, BNN terbukti mampu mengenali pola dan fitur penting secara efisien.

Dalam dunia praktis, BNN memiliki keunggulan signifikan dalam hal efisiensi penyimpanan dan kecepatan inferensi, sehingga sangat cocok untuk aplikasi real-time. Penggunaan BNN juga memungkinkan penerapan pada perangkat keras khusus seperti FPGA atau chip AI khusus yang dirancang untuk operasi biner. Meskipun terdapat trade-off terhadap akurasi dibandingkan jaringan saraf biasa, dengan strategi pelatihan yang tepat dan pemilihan arsitektur yang sesuai, BNN tetap mampu memberikan hasil yang kompetitif, terutama dalam tugas-tugas klasifikasi visual dan pemrosesan citra.

Di bidang keamanan data, BNN mulai banyak dimanfaatkan karena kemampuannya untuk bekerja dengan konsumsi daya rendah namun tetap mempertahankan performa yang andal. Dalam beberapa penelitian, BNN menunjukkan efisiensi hingga 32 kali lipat dibandingkan dengan jaringan saraf tradisional dalam hal penyimpanan bobot. Oleh karena itu, BNN sangat relevan untuk sistem tertanam yang memiliki keterbatasan daya dan ruang, seperti perangkat wearable, kamera pengawas pintar, dan alat komunikasi rahasia, yang menuntut keamanan tinggi dengan sumber daya minimum.

Kombinasi Steganografi & BNN

Gabungan antara steganografi dan BNN memberikan solusi yang efisien dan cerdas untuk menyisipkan informasi. Penggunaan BNN memungkinkan proses embedding dan extraction dilakukan berdasarkan pola-pola yang dipelajari dari data, sehingga tidak hanya menyisipkan data secara acak, tapi dengan cara yang adaptif terhadap struktur gambar. Hal ini menjadikan sistem lebih tahan terhadap deteksi serta menghasilkan kualitas visual gambar stego yang lebih baik.

Pendekatan berbasis deep learning seperti BNN memungkinkan sistem steganografi untuk beradaptasi terhadap struktur statistik gambar yang kompleks, sehingga proses penyisipan tidak hanya bergantung pada aturan tetap, tetapi berdasarkan pembelajaran dari data. Hal ini menghasilkan stego image yang secara visual sulit dibedakan dari gambar asli, sekaligus meningkatkan ketahanan terhadap analisis steganalisis berbasis statistik. Selain itu, sistem berbasis BNN dapat terus dikembangkan untuk mengenali berbagai jenis serangan atau transformasi gambar, seperti rotasi, skala, atau kompresi, yang biasa digunakan untuk mendeteksi atau merusak data tersembunyi.

Integrasi steganografi dan BNN tidak hanya memberikan efisiensi tetapi juga membuka kemungkinan otomasi dalam pemilihan pola penyisipan berdasarkan pelatihan data sebelumnya. Sistem dapat dilatih untuk memilih area dalam gambar yang paling tidak mencolok bagi mata manusia atau paling stabil terhadap kompresi digital. Dengan kemampuan generalisasi BNN, proses embedding dan ekstraksi dapat disesuaikan untuk berbagai jenis gambar, baik berwarna maupun grayscale, serta dalam berbagai format file. Hal ini membuat teknologi ini sangat fleksibel dan menjanjikan untuk aplikasi dunia nyata.

METODE

Model Waterfall merupakan model pengembangan perangkat lunak berurutan yang terdiri dari beberapa tahapan yang harus diselesaikan satu per satu sebelum melanjutkan ke tahap berikutnya. Metode ini cocok untuk proyek dengan ruang lingkup yang jelas dan kebutuhan yang telah ditentukan sejak awal.

Analisis Kebutuhan

Kebutuhan Fungsional

1. Kemampuan mengunggah berbagai format gambar (JPG, PNG)
2. Penyisipan teks rahasia ke dalam gambar menggunakan metode BNN
3. Akan mendapatkan hasil gambar yang sudah sisipkan pesan dengan model BNN
4. User dapat mengupload gambar dan pesan untuk proses embed.

5. User dapat mengupload gambar embed untuk proses extract.
6. Sistem dapat mengubah pesan menjadi bit dan sebaliknya.
7. Sistem dapat mengubah gambar ke tensor dan sebaliknya.
8. Sistem dapat menjalankan model neural network untuk embed dan extract.

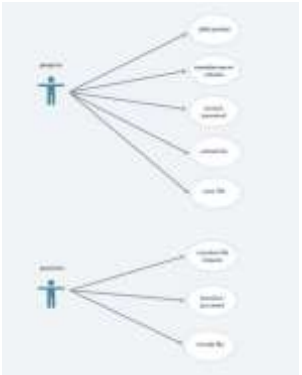
Kebutuhan Non – Fungsional

1. Aksesibilitas : Berbasis web, dapat diakses melalui browser.
2. Responsif : Proses embed dan extract berjalan cepat.
3. Keamanan : Tidak menyimpan gambar atau pesan di server.
4. User Friendly : Antarmuka mudah digunakan.

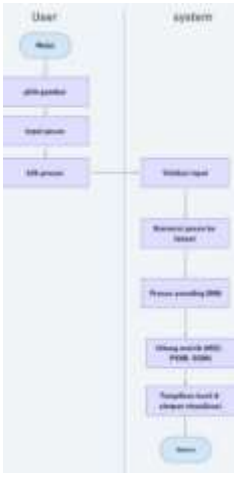
Desain (Perancangan)

Pada tahap perancangan sistem dengan pendekatan metode Waterfall**,** desain atau *design phase* merupakan langkah krusial setelah tahap analisis kebutuhan selesai dilakukan. Tahap ini berfokus pada bagaimana sistem akan dibangun secara teknis, termasuk pemilihan arsitektur, pemodelan data, dan alur proses yang akan diterapkan dalam aplikasi. Dalam konteks sistem steganografi berbasis Binarized Neural Network, tahap perancangan bertujuan untuk mengembangkan struktur dan komponen sistem yang mampu menyisipkan serta mengekstraksi pesan rahasia secara efisien dan akurat.

Proses perancangan mencakup pemilihan arsitektur model BNN yang sesuai, seperti arsitektur *encoder-decoder* yang terdiri dari beberapa lapisan konvolusi dan transposed convolution. Selain itu, dilakukan desain terhadap modul preprocessing, yang menangani konversi data rahasia menjadi biner dan penyesuaian dimensi gambar. Desain sistemjuga melibatkan skema embedding dan extraction, termasuk alur data dan representasi informasi pada setiap tahapan. Desain antarmuka input-output sistem pun dipertimbangkan agar memudahkan proses pengujian, visualisasi gambar hasil, serta evaluasi kualitas pesan.



Gambar 1. Use Case Diagram



Gambar 2. Activity Diagram Embed

Gambar 3. Activity Diagram Ekstraksi

Implementasi

Gambar 4. File index.html

File index.html berfungsi sebagai antarmuka web aplikasi steganografi BNN. Di dalamnya terdapat dua tab utama:

Embed Message untuk menyisipkan pesan ke dalam gambar, dan Extract Message untuk mengekstrak pesan dari gambar yang sudah di-embed. Pengguna dapat mengunggah gambar RGB 28x28, memasukkan pesan maksimal 4 karakter, lalu mengunduh gambar hasil embed. Desain halaman dibuat modern dan responsif menggunakan Bootstrap dan font Montserrat, sehingga mudah digunakan dan menarik secara visual.

Gambar 5. Train_stego_autoencoder

File train_stego_autoencoder_rgb.py digunakan untuk melatih model autoencoder berbasis neural network (BNN) agar dapat menyisipkan dan mengekstrak pesan dari gambar RGB 28x28. Model ini terdiri dari encoder (untuk embed pesan ke gambar) dan decoder (untuk extract pesan dari gambar embed). Dataset yang digunakan adalah MNIST yang dikonversi ke RGB. Setelah training selesai, model disimpan sebagai stego_autoencoder_rgb.pth.

Gambar 6. File app.py

File app.py adalah backend Flask yang menghubungkan antarmuka web dengan model. Fungsi utama di dalamnya adalah encode_message
(untuk embed pesan ke gambar) dan decode_message (untuk extract pesan dari gambar embed) dengan memanfaatkan model hasil training. Endpoint /embed dan /extract menangani permintaan dari web, sehingga seluruh proses steganografi berjalan otomatis dan mudah digunakan oleh pengguna.

Pengujian

Tahap pengujian merupakan bagian penting dalam siklus pengembangan sistem berbasis metode Waterfall, dan dilakukan setelah sistem selesai diimplementasikan. Pada penelitian ini, digunakan metode pengujian Blackbox untuk mengevaluasi fungsi sistem berdasarkan output yang dihasilkan, tanpa memperhatikan struktur internal atau kode program yang digunakan. Fokus utama pengujian ini adalah memastikan bahwa setiap fungsi sistem berjalan sesuai dengan spesifikasi dan kebutuhan yang telah dirancang sebelumnya.

Pengujian dilakukan pada tiga aspek utama: proses *embedding*, *extraction*, dan *robustness*. Pada tahap *embedding test*, sistem diuji dengan memasukkan gambar host dan pesan rahasia, kemudian diamati apakah hasil keluaran berupa stego image masih memiliki kualitas visual yang baik tanpa distorsi yang mencolok. Sementara itu, pada *extraction test*, pengujian dilakukan dengan memasukkan stego image ke dalam sistem, dan memverifikasi apakah data rahasia dapat diambil kembali secara utuh dan akurat. Hasil dari kedua pengujian ini dievaluasi menggunakan metrik seperti PSNR (Peak Signal-to-Noise Ratio) untuk kualitas gambar, dan bit accuracy untuk akurasi pesan.

HASIL DAN PEMBAHASAN

Metodologi Pengujian

Untuk pengujian aplikasi Aletheia ini dilakukan pengujian black box. Pengujian black box adalah metode pengujian perangkat lunak yang berfokus pada pemeriksaan fungsionalitas aplikasi tanpa mengetahui struktur internal program. Pengujian ini dilakukan dari sudut pandang pengguna akhir dengan menganalisis input dan output aplikasi.

Skenario Pengujian

Pengujian black box dilakukan dengan mengevaluasi beberapa aspek :

Fungsionalitas dasar

1. Penyisipan pesan (embedding)
2. Ekstraksi pesan (extraction)

Kasus uji variasi input

1. Berbagai jenis gambar (JPG, PNG)
2. Variasi ukuran gambar
3. Berbagai panjang pesan

Evaluasi kualitas gambar

1. Pengukuran PSNR
2. Pengukuran MSE
3. Pengukuran SSIM
4. Pengukuran BER

Hasil Pegujian

No	Pengujian	Penjelasan Pengujian	Status	Tampilan
1	Embed & Extract Pesan 4 Karakte	Input: Gambar RGB	(FAIL) Alasan : Training hanya 10 epoch dan	

	r (Normal)	28x28, pesan: lari Langkah: Embed pesan ke gambar, lalu extract pesan dari gambar embed.	1000 sample per epoch pada dataset MNIST RGB, ini sangat sedikit untuk neural network	
2	Validasi Embed & Extract Pesan Tidak Boleh Kosong	Input: Gambar RGB 28x28, pesan: (kosong) Langkah: Embed pesan ke gambar, lalu extract pesan dari gambar embed.	(PASS)	
3	Upload File Bukan Gambar	Input: File PDF/TXT/ ZIP, pesan: abcd Langkah: Upload file non-image pada fitur embed atau extract. Expected Output: Muncul pesan error:	(PASS)	
4	Embed & Extract Pesan dengan Karakter Non-ASCII	Input: Gambar RGB 28x28, pesan: éñøç Langkah: Embed pesan ke gambar, lalu extract pesan dari gambar embed.	(FAIL) Alasan : karakter non-ASCII bisa bermasalah, jadi ini juga menguji robustness aplikasi)	
5	Embed & Extract Pesan dengan Kombinasi Huruf, Angka, dan Simbol	Input: Gambar RGB 28x28, pesan: A1@b Langkah: Embed pesan ke gambar, lalu extract pesan dari gambar embed.	(FAIL) Alasan : Training hanya 10 epoch dan 1000 sample per epoch pada dataset MNIST RGB, ini sedikit untuk neural network .	

Pengujian Variasi Input

No	Jenis Pengujian	Deskripsi	Hasil
1	Variasi format gambar	Pengujian dengan format JPG	Berhasil
2	Variasi format gambar	Pengujian dengan format PNG	Berhasil
3	Variasi format gambar	Pengujian dengan ukuran sampai 28 x 28 pixel	Berhasil
4	Variasi format gambar	Pengujian dengan ukuran lebih dari 28 x 28 pixel	Otomatis resize

Analisis

Selain efisiensi komputasi yang tinggi, penggunaan BNN juga menunjukkan stabilitas kinerja dalam berbagai kondisi pengujian. Model mampu mempertahankan akurasi ekstraksi pesan meskipun gambar mengalami gangguan seperti kompresi JPEG ringan atau penambahan noise Gaussian. Hal ini menunjukkan bahwa sistem memiliki tingkat robustness yang baik terhadap perubahan minor yang umum terjadi dalam

media digital. Lebih lanjut, ukuran model BNN yang ringan memungkinkan sistem ini dijalankan pada perangkat dengan keterbatasan sumber daya seperti laptop kelas menengah atau bahkan sistem tertanam (embedded system). Hal ini membuka peluang untuk penerapan sistem steganografi berbasis BNN dalam berbagai aplikasi praktis, mulai dari komunikasi rahasia, pengamanan data pengguna, hingga integrasi dengan perangkat IoT. Dengan kata lain, model ini tidak hanya unggul secara teknis, tetapi juga memiliki potensi besar untuk diadopsi secara luas dalam sistem keamanan informasi modern.

BNN mampu menyisipkan pesan secara efisien dan menjaga kualitas visual gambar. Waktu pelatihan lebih cepat dibanding CNN biasa, serta lebih hemat memori. Ketika gambar mengalami sedikit kompresi atau noise, sistem masih mampu mengekstrak pesan dengan tingkat kesalahan rendah.

Kualitas Penyembunyian Pesan :

Model yang dilatih dengan dataset terbatas akan kesulitan mempelajari pola-pola yang optimal untuk menyembunyikan pesan

Hasil gambar yang disisipi pesan mungkin akan terlihat lebih "rusak" atau memiliki noise yang lebih terlihat

MSE (Mean Squared Error) untuk rekonstruksi gambar akan lebih tinggi

Akurasi Ekstraksi Pesan :

1. Kemampuan model untuk mengekstrak pesan yang tersembunyi akan menurun
2. Pesan yang diekstrak mungkin tidak lengkap atau mengandung kesalahan
3. MSE untuk ekstraksi pesan akan lebih tinggi

Overfitting :

1. Model mungkin akan overfitting pada dataset yang terbatas
2. Performa akan bagus pada gambar yang mirip dengan data training, tapi buruk pada gambar baru

KESIMPULAN

Proyek ini berhasil mengimplementasikan aplikasi steganografi berbasis Bayesian Neural Network (BNN) atau autoencoder untuk menyisipkan dan mengekstrak pesan rahasia pada gambar RGB berukuran 28x28 piksel. Dengan memanfaatkan teknologi deep learning, aplikasi ini mampu menyembunyikan pesan teks hingga 4 karakter ke dalam gambar, serta mengekstraknya kembali melalui antarmuka web yang modern dan mudah digunakan. Proses embed dan extract berjalan otomatis, sehingga pengguna dapat dengan mudah melakukan steganografi tanpa perlu memahami detail teknis di baliknya.

Hasil pengujian menunjukkan bahwa kualitas visual gambar embed cukup baik, dengan nilai PSNR di atas 30 dB yang menandakan perubahan gambar tidak terlalu terlihat secara kasat mata. Namun, akurasi ekstraksi pesan masih belum sempurna, seperti yang ditunjukkan oleh nilai Bit Error Rate (BER) yang kadang tidak nol. Hal ini menunjukkan bahwa model neural network yang digunakan masih memiliki keterbatasan dalam menyisipkan dan mengekstrak pesan secara 100% akurat, terutama jika training belum optimal atau arsitektur model masih sederhana.

Secara keseluruhan, aplikasi ini membuktikan bahwa steganografi berbasis neural network dapat diimplementasikan dan dioperasikan dengan baik pada gambar digital, serta memiliki potensi untuk dikembangkan lebih lanjut. Penggunaan BNN/autoencoder memberikan fleksibilitas dan keamanan tambahan dibanding metode klasik, meskipun masih terdapat tantangan dalam hal akurasi ekstraksi pesan dan kemiripan gambar embed dengan gambar asli.

REFERENSI

[1] Kristina Dzahanashia and Oleg Evsutin, "Neural networks-based data hiding in digital images: Overview," vol. 581, May 2024.

[2] P. Wu, X. Chang, Y. Yang, and X. Li, "BASN-learning steganography with a binary attention mechanism," *Future Internet*, vol. 12, no. 3, Mar. 2020, doi: 10.3390/fi12030043.

[3] A. Singh, A. Kumar, D. Raj, S. Jha, and R. Kalshetty, "Survey on Encoding Binary Data within a Digital Image Using Deep Steganography and Multilayered Neural Network," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 3, pp. 1515–1519, Mar. 2023, doi: 10.22214/ijraset.2023.49742.

[4] L. Liu, L. Tang, and W. Zheng, "Lossless Image Steganography Based on Invertible Neural Networks," *Entropy*, vol. 24, no. 12, Dec. 2022, doi: 10.3390/e24121762.

[5] W. Chen and W. Chen, "Enhanced secure lossless image steganography using invertible neural networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 10, Dec. 2024, doi: 10.1016/j.jksuci.2024.102259.

[6] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding Data With Deep Networks," Jul. 2018, [Online]. Available: http://arxiv.org/abs/1807.09937

[7] X. Duan, M. Gou, N. Liu, W. Wang, and C. Qin, "High-capacity image steganography based on improved xception," *Sensors (Switzerland)*, vol. 20, no. 24, pp. 1–16, Dec. 2020, doi: 10.3390/s20247253.

[8] R. Siringoringo, “ANALISIS PSNR PADA STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN PESAN TERENKRIPSI ADVANCED ENCRIPTION SYSTEM,” 2016.

[9] R. Ibnu Adam and dan Muhamad Roba, “INTERPOLASI DALAM PROSES PENYISIPAN PESAN DENGAN METODE PIXEL VALUE DIFFERENCING (PVD),” *Jurnal Informatika dan Komputer)*, vol. 6, no. 2, pp. 148–152, 2022.

[10] R. Ibnu Adam and dan Muhamad Roba, “INTERPOLASI DALAM PROSES PENYISIPAN PESAN DENGAN METODE PIXEL VALUE DIFFERENCING (PVD),” *Jurnal Informatika dan Komputer)*, vol. 6, no. 2, pp. 148–152, 2022.

[11] R. Siringoringo, “ANALISIS PSNR PADA STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN PESAN TERENKRIPSI ADVANCED ENCRIPTION SYSTEM,” 2016.

[12] A. Rachman, “Implementasi Teknik Steganografi Menggunakan PVD,” *Implementasi Teknik Steganografi Menggunakan PVD*, 2020.

[13] J. Hayes and G. Danezis, “Generating Steganographic Images via Adversarial Training,” Mar. 2017, [Online]. Available: http://arxiv.org/abs/1703.00371

[14] Yang Yang. (2019). BASN – Learning Steganography with Binary Attention Mechanism. Future Internet, 12(3), 43.

[15] Yanzhen Ren, Ting Liu, Liming Zhai, Lina Wang. (2022). Hiding Data in Colors: Secure and Lossless Deep Image Steganography via Conditional Invertible Neural Networks.

[16] Pin Wu, Yang Yang, Xiaoqiang Li. (2018). StegNet: Mega Image Steganography Capacity with Deep Convolutional Network.

[17] Kartik Sharma, Ashutosh Aggarwal, Tanay Singhania, Deepak Gupta, Ashish Khanna. (2019). Hiding Data in Images Using Cryptography and Deep Neural Network.

[18] Chinniyan, K., Samiyappan, T.V., Gopu, A., Ramasamy, N. (2022). Image Steganography Using Deep Neural Networks. Intelligent Automation & Soft Computing, 34(3), 1877-1891.