

Pendekatan Pembelajaran Mesin Berbasis Model Campuran Gaussian untuk Deteksi Steganografi Pada Citra JPEG

Indrawan Ady Saputro^{1*}, Febrianta Surya Nugraha², Lilik Sugiarto³

^{1,2,3} Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Surakarta
Sukoharjo, Jawa Tengah, Indonesia 57163
indrawanadys@dosen.amikomsolo.ac.id

Abstrak

Perkembangan keamanan digital terus mengalami kemajuan pesat, khususnya di bidang steganografi. Steganografi adalah teknik menyembunyikan data agar tidak mudah terdeteksi. Salah satu teknik populer pada citra JPEG adalah Least Significant Bit (LSB). Namun, teknik ini sering disalahgunakan, sehingga meningkatkan risiko terhadap keamanan data dan menuntut adanya metode deteksi yang andal. Tujuan penelitian ini adalah mengembangkan metode deteksi steganografi yang efektif dengan menggunakan *Gaussian Mixture Models* (GMM). Metodologi yang digunakan melibatkan pengolahan dataset yang terdiri dari dua kelas: citra asli dan citra yang telah disisipkan pesan tersembunyi menggunakan teknik LSB. Dataset ini kemudian dianalisis menggunakan model GMM untuk mendeteksi pola-pola steganografi. Hasil evaluasi menunjukkan bahwa GMM mencapai akurasi 78,67%, presisi 89,15%, dan recall 69,70%. Selain itu, nilai AUC-ROC sebesar 86,59% menunjukkan kemampuan yang baik dalam membedakan citra asli dan steganografi. Kesimpulannya, GMM merupakan metode yang efektif dan efisien untuk deteksi steganografi adaptif, menawarkan tingkat akurasi tinggi dengan kebutuhan sumber daya yang lebih ringan dibandingkan metode lain.

Kata kunci: Deteksi, GMM, Keamanan Digital, LSB, Steganografi

Abstract

The development of digital security continues to experience rapid progress, especially in the field of steganography. Steganography is a technique of hiding data so that it is not easily detected. One popular technique in JPEG images is Least Significant Bit (LSB). However, these techniques are often abused, increasing the risk to data security and demanding reliable detection methods. The purpose of this study is to develop an effective steganography detection method using Gaussian Mixture Models (GMM). The methodology used involves processing a dataset consisting of two classes: the original image and the image that has been inserted with hidden messages using the LSB technique. This dataset was then analyzed using the GMM model to detect steganography patterns. The evaluation results showed that GMM achieved 78.67% accuracy, 89.15% precision, and 69.70% recall. In addition, the AUC-ROC value of 86.59% showed good ability in distinguishing original images and steganography. In conclusion, GMM is an effective and efficient method for adaptive steganography detection, offering a high level of accuracy with less resource requirements than other methods.

Keywords: Detection, Digital Security, GMM, LSB, Steganography

I. PENDAHULUAN

Dalam era digital, kebutuhan akan keamanan informasi menjadi semakin penting, terutama dengan berkembangnya teknik steganografi yang memungkinkan penyembunyian data dalam media digital seperti gambar, suara, dan video [1][2].

Steganografi pada citra digital, khususnya pada format JPEG, menjadi salah satu teknik yang banyak digunakan karena mampu menyembunyikan informasi secara visual tanpa mengurangi kualitas gambar secara signifikan [3][4]. Namun, berkembangnya teknik steganografi diikuti oleh meningkatnya ancaman penyalahgunaan teknologi

ini untuk tujuan ilegal seperti penyebaran informasi rahasia atau penyamaran malware. Oleh karena itu, dibutuhkan metode deteksi yang dapat mengidentifikasi keberadaan pesan tersembunyi dalam gambar secara efektif [5] [6]. Sistem deteksi steganografi tradisional sering kali bergantung pada analisis statistik konvensional, yang meskipun memiliki ketelitian yang baik, cenderung memiliki keterbatasan dalam mengidentifikasi steganografi kompleks yang dihasilkan oleh metode modern [7][8]. Sebagai contoh, teknik deteksi konvensional sering kali gagal ketika berhadapan dengan steganografi adaptif yang dapat menyamarkan pola-pola penyisipan data secara dinamis [9]. Oleh karena itu, metode berbasis pembelajaran mesin mulai diperkenalkan sebagai solusi alternatif untuk mengatasi kelemahan sistem deteksi tradisional [10]. Dengan kemampuannya dalam mempelajari pola kompleks dan mengklasifikasikan data dengan akurasi tinggi, pembelajaran mesin memberikan peluang baru dalam meningkatkan efektivitas deteksi steganografi.

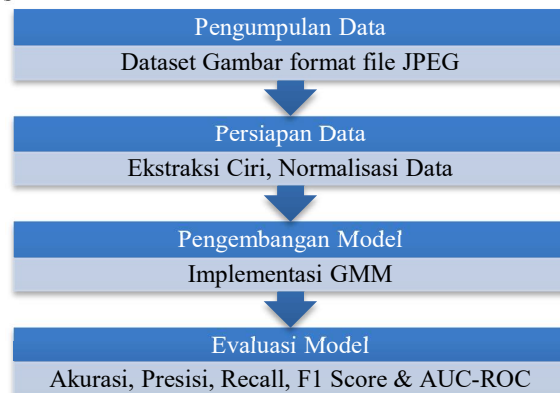
Beberapa pendekatan berbasis pembelajaran mesin, seperti penggunaan *deep convolutional neural networks* (CNNs), telah diteliti untuk deteksi steganografi dan menunjukkan hasil yang menjanjikan [11] [12]. Meski demikian, pendekatan ini membutuhkan daya komputasi yang besar dan waktu pelatihan yang cukup lama. Di sisi lain, teknik yang lebih ringan namun tetap efektif seperti model campuran gaussian (GMM) juga mulai mendapatkan perhatian [13]. Model ini memiliki kemampuan untuk memodelkan distribusi data yang kompleks dan dapat mengelompokkan data berdasarkan karakteristik yang tidak terdeteksi secara langsung, menjadikannya metode yang efisien untuk mendeteksi pola dalam gambar steganografi [6]. Penelitian ini mengusulkan penggunaan GMM yang dikombinasikan dengan algoritma pembelajaran lain seperti Random Forest untuk mendeteksi steganografi pada citra JPEG. GMM di sini digunakan untuk mengidentifikasi cluster atau kelompok piksel yang memiliki karakteristik distribusi tertentu, yang kemudian dianalisis lebih lanjut dengan model ensemble untuk meningkatkan akurasi deteksi [14].

Pendekatan ini bertujuan untuk meningkatkan performa deteksi dibandingkan metode sebelumnya, seperti SVM dan teknik-teknik ekstraksi fitur tradisional yang memiliki keterbatasan dalam mengenali pola steganografi yang adaptif [15] [16][17]. Secara keseluruhan, studi ini bertujuan untuk mengembangkan kerangka kerja berbasis pembelajaran mesin yang memanfaatkan kekuatan GMM dalam klasifikasi probabilistik untuk mengidentifikasi gambar yang mengandung pesan

tersembunyi. Dengan demikian, penelitian ini berpotensi untuk memberikan kontribusi signifikan dalam bidang keamanan digital, khususnya dalam hal deteksi steganografi yang efisien pada citra JPEG.

II. METODE PENELITIAN

Metode penelitian ini dirancang untuk mengembangkan dan melakukan evaluasi terhadap pendekatan machine learning dan deteksi steganografi pada citra JPEG. Penelitian ini dilakukan mulai dari melakukan pengumpulan data, olah data, pengembangan model dan evaluasi kinerja model. Berikut ini alur penelitian terlihat pada gambar 1.



Gambar 1. Alur Penelitian

2.1. Pengumpulan Data

Dalam penelitian ini, dataset yang digunakan terdiri dari citra JPEG yang mencakup gambar asli dan gambar yang telah disisipkan pesan steganografi menggunakan metode LSB (*Least Significant Bit*). Dataset ini diperoleh dari referensi yang tercantum pada [18].

2.2. Persiapan Data

- Ekstraksi Ciri:** Teknik ekstraksi fitur seperti histogram, matriks, serta analisis frekuensi akan digunakan untuk memperoleh ciri-ciri citra yang diperlukan dalam tahap klasifikasi.
- Normalisasi Data:** Data fitur akan dinormalisasi untuk memastikan bahwa semua fitur berada pada skala yang seragam, guna meningkatkan kinerja model pembelajaran mesin.

2.3. Pengembangan Model

Model Pembelajaran Mesin: Model Campuran Gaussian (GMM) akan diterapkan untuk mengidentifikasi pola tersembunyi dalam citra. Model ini akan dilatih menggunakan fitur yang telah diekstraksi dari citra. Gaussian Mixture Model (GMM) digunakan untuk mendeteksi pola-pola yang terkait dengan teknik Least Significant Bit (LSB) dalam gambar JPEG. GMM berfungsi sebagai model

probabilistik untuk mengidentifikasi pola yang mencerminkan adanya pesan tersembunyi pada gambar. Model ini mengklasifikasikan gambar berdasarkan probabilitas distribusi fitur yang diekstraksi, membedakan gambar asli dari gambar yang mengandung steganografi. GMM memisahkan gambar ke dalam kelompok berdasarkan distribusi fitur yang ada. Penerapan GMM dapat dijelaskan dengan persamaan berikut:

$$p(x|\lambda) = \sum_{k=1}^K \pi_k N(x|\mu_k, \Sigma_k)$$

Di mana:

- $p(x|\lambda)$ adalah probabilitas data xxx diberikan model GMM,
- K adalah jumlah komponen Gaussian dalam model,
- π_k adalah bobot komponen ke- k ,
- $N(x|\mu_k, \Sigma_k)$ adalah distribusi normal dengan mean dan kovarians Σ_k untuk komponen ke- k .

2.4. Evaluasi Model

Evaluasi kinerja model GMM dilakukan dengan menggunakan beberapa metrik untuk mengukur efektivitas deteksi steganografi, seperti akurasi, presisi, recall, F1-Score, dan AUC-ROC. Metrik ini memberikan gambaran menyeluruh tentang kemampuan model dalam membedakan gambar asli dan gambar yang mengandung pesan tersembunyi.

- a. Akurasi: Untuk mengukur persentase gambar yang terdeteksi dengan benar oleh model.

$$\text{Akurasi} = \frac{TP + TN}{TP + TN + FP + FN}$$

Di mana:

- TP: True Positive (gambar yang benar terdeteksi sebagai steganografi),
 - TN: True Negative (gambar yang benar terdeteksi sebagai asli),
 - FP: False Positive (gambar asli yang terdeteksi sebagai steganografi),
 - FN: False Negative (gambar steganografi yang terdeteksi sebagai asli).
- b. Presisi dan Recall: Kedua metrik ini akan digunakan untuk menilai sejauh mana model dapat mendeteksi citra yang mengandung steganografi dengan akurasi dan kelengkapan.

$$\text{Presisi} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

- c. F1-Score: Merupakan kombinasi antara presisi dan recall yang memberikan gambaran umum mengenai kinerja model secara keseluruhan.

$$F1 - \text{Score} = \frac{2 * \text{Presisi} * \text{Recall}}{\text{Presisi} + \text{Recall}}$$

- d. AUC-ROC: Kurva AUC-ROC akan digunakan untuk mengukur kemampuan model dalam membedakan gambar asli dengan gambar yang berisi pesan steganografi.

$$AUC = \int_0^1 TPR(FPR) dFPR$$

Di mana:

- TPR adalah Probabilitas data yang benar diklasifikasikan sebagai positif (gambar steganografi yang benar-benar dideteksi sebagai steganografi).
- FPR adalah Probabilitas data yang salah diklasifikasikan sebagai positif (gambar asli yang salah terdeteksi sebagai steganografi).
- $dFPR$ merupakan diferensial dari FPR, digunakan dalam proses integrasi untuk menghitung luas di bawah kurva (Area Under Curve). $dFPR$ menunjukkan perubahan kecil dalam nilai FPR sepanjang kurva ROC.

III. HASIL DAN PEMBAHASAN

3.1 Dataset dan Teknik Penelitian

Dataset JPEG yang digunakan dalam penelitian ini dipilih secara spesifik untuk menyertakan gambar asli dan gambar yang telah disisipkan pesan melalui teknik *Least Significant Bit* (LSB). Untuk memastikan analisis yang akurat, semua gambar dinormalisasi sehingga fitur yang diekstraksi dari gambar berada dalam skala yang seragam, mengurangi potensi variasi antar gambar yang dapat mengganggu hasil. Normalisasi ini juga meningkatkan konsistensi dalam pembelajaran model, karena setiap gambar memiliki atribut yang dapat dibandingkan secara efektif. Teknik LSB memungkinkan penyisipan pesan tersembunyi dengan memanfaatkan bit terakhir dari setiap piksel, yang tidak terlalu mempengaruhi tampilan visual gambar. Dengan cara ini, pesan dapat disembunyikan tanpa terdeteksi oleh mata manusia, seperti terlihat pada Gambar 2 gambar asli dan gambar 3 gambar dengan steganografi.



Gambar 2. Gambar asli



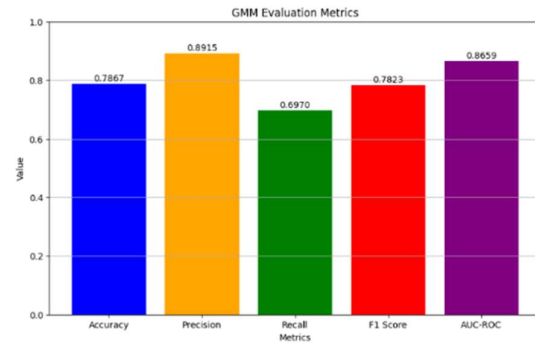
Gambar 3. Gambar disisipkan steganografi

3.2 Hasil Pembahasan

GMM berperan penting dalam mengenali pola-pola spesifik dari LSB pada gambar-gambar yang mungkin mengandung steganografi dibandingkan dengan gambar normal. Model ini memisahkan data ke dalam kelompok-kelompok, seperti gambar yang mengandung pesan tersembunyi dan yang tidak, berdasarkan variasi yang ditemukan dalam pola LSB. GMM membantu mengidentifikasi pola yang tidak biasa pada bit terakhir gambar, yang memiliki variansi tinggi sebagai indikasi adanya steganografi. Penelitian ini menunjukkan efektivitas pendekatan berbasis *Gaussian Mixture Models* (GMM) dalam mengidentifikasi steganografi pada gambar JPEG. Menggunakan dataset dengan pesan tersembunyi yang disisipkan menggunakan metode LSB, model GMM dievaluasi menggunakan berbagai metrik kinerja seperti akurasi, presisi, *recall*, F1-Score, dan kurva AUC-ROC. Hasil evaluasi menunjukkan bahwa model ini memiliki kinerja yang baik dalam mengklasifikasikan gambar, dengan akurasi mencapai 78,67% (0,786667), menunjukkan tingkat ketepatan yang baik dalam mendeteksi steganografi. Dengan nilai presisi 89,15%, sebagian besar prediksi positif yang dihasilkan model terbukti akurat, sebuah aspek penting dalam deteksi steganografi di mana kesalahan positif dapat berdampak besar. Namun, *recall* sebesar 69,70% menunjukkan adanya peluang perbaikan untuk lebih meningkatkan jumlah deteksi positif. F1-Score yang diperoleh sebesar 78,23% menunjukkan keseimbangan yang cukup baik antara presisi dan *recall*, namun peningkatan *recall* dapat memperbaiki performa keseluruhan. Nilai AUC-ROC sebesar 86,59% juga mengindikasikan kemampuan model yang cukup baik dalam membedakan gambar steganografi dari gambar asli.

Selain kinerja deteksi, GMM juga efisien dalam hal komputasi. Model ini membutuhkan waktu 2-5 detik untuk mendeteksi steganografi pada satu gambar, tergantung pada kompleksitasnya, dengan dataset yang terdiri dari 500 citra asli dan 500 citra steganografi. Penggunaan memori selama pelatihan dan inferensi stabil di sekitar 350 MB untuk 1.000

gambar, dan hanya menggunakan sekitar 20% kapasitas CPU. Ini menjadikan GMM cocok digunakan pada perangkat dengan kapasitas terbatas, dengan keseimbangan yang baik antara kinerja dan efisiensi.



Gambar 3. Metrik Evaluasi GMM

Gambar 3 menampilkan metrik evaluasi yang diperoleh, menunjukkan akurasi dan presisi yang tinggi, dengan performa yang seimbang antara deteksi positif dan negatif. Berdasarkan hasil evaluasi, GMM memberikan hasil yang baik dalam mendeteksi perubahan kecil pada gambar yang mungkin mengindikasikan adanya pesan tersembunyi. Model ini menunjukkan keandalan dalam membedakan antara gambar asli dan gambar yang berisi steganografi. Meski demikian, peningkatan *recall* dapat dicapai melalui penyetelan parameter, penambahan data pelatihan, atau teknik pra-pemrosesan yang lebih lanjut untuk meningkatkan sensitivitas model terhadap gambar yang mengandung pesan steganografi.

3.3 Diskusi

Penelitian ini memperkenalkan model berbasis *Gaussian Mixture Models* (GMM) untuk mendeteksi steganografi pada citra JPEG dengan teknik *Least Significant Bit* (LSB), sebuah pendekatan yang berbeda dari metode sebelumnya yang lebih umum digunakan seperti *Support Vector Machine* (SVM), *Random Forest*, atau *deep learning* [19],[20]. Kebanyakan studi terdahulu menggunakan metode berbasis jaringan saraf konvolusional (CNN) atau SVM yang mengandalkan karakteristik visual mendalam dari gambar untuk mendeteksi pola anomali [21]. Namun, metode tersebut membutuhkan sumber daya komputasi yang cukup besar, yang mungkin menjadi kendala dalam implementasi pada perangkat dengan keterbatasan kapasitas komputasi [22].

Dalam penelitian ini, penggunaan GMM sebagai model probabilistik menawarkan keunggulan dalam hal efisiensi komputasi dan ketepatan dalam mengidentifikasi perbedaan pola pada bit terakhir gambar. GMM mampu membedakan gambar yang

memiliki variasi LSB yang lebih tinggi, yang biasanya mengindikasikan adanya pesan tersembunyi, dari gambar normal yang tidak mengandung steganografi. Dengan memanfaatkan teknik probabilistik ini, penelitian ini menunjukkan bahwa model dapat secara efektif membedakan antara citra asli dan citra yang telah dimanipulasi, bahkan ketika perbedaannya sangat minim secara visual, seperti yang terlihat pada citra steganografi LSB.

Studi ini juga memberikan evaluasi kinerja yang menyeluruh, mencakup metrik akurasi, presisi, recall, F1-Score, dan AUC-ROC, yang lebih jarang ditemukan dalam literatur yang cenderung menitikberatkan pada satu atau dua metrik utama [23]. Evaluasi yang lebih lengkap ini menegaskan posisi GMM sebagai alternatif yang kompetitif dalam deteksi steganografi, dengan nilai presisi yang cukup tinggi yang mengindikasikan kemampuan model untuk secara andal mendeteksi gambar-gambar dengan pesan tersembunyi. Hasil ini berbeda dari studi terdahulu yang berfokus pada metode supervised, di mana model umumnya membutuhkan pelabelan manual yang intensif dan sering kali gagal mempertahankan kinerja optimal di luar dataset yang dilatih.

Dengan demikian, penelitian ini tidak hanya menawarkan pendekatan baru melalui penerapan GMM untuk deteksi pola LSB, tetapi juga menggarisbawahi bahwa metode ini cocok untuk skenario di mana efisiensi komputasi dibutuhkan. Selain itu, hasil evaluasi yang menunjukkan akurasi dan presisi tinggi dengan model probabilistik ini memperkuat nilai penelitian dalam menyediakan alternatif yang lebih ringan dan efektif dibandingkan dengan pendekatan berbasis *deep learning* atau *supervised* lainnya

IV. KESIMPULAN

Penelitian ini mengevaluasi penggunaan machine learning untuk mendeteksi pesan tersembunyi pada citra JPEG melalui teknik steganografi *Least Significant Bit* (LSB) dengan mengintegrasikan *Gaussian Mixed Model* (GMM). Dataset terdiri dari citra asli dan citra yang disisipkan pesan steganografi. Model GMM berhasil mengklasifikasikan 78,67% data dengan akurasi 89,15%, tetapi hasil *recall* lebih rendah yaitu 69,70%, yang menunjukkan adanya potensi perbaikan. Nilai AUC-ROC sebesar 86,59% menunjukkan kemampuan model yang baik dalam membedakan citra asli dengan citra steganografi.

REFERENSI

- [1] H. Zhang, J. Liu, and W. Zhang, "Steganography detection in digital images: A comprehensive review," *J. Inf. Secur. Appl.*, vol. 58, p. 102520, 2021, doi: 10.1016/j.jisa.2021.102520.
- [2] A. Purbaningrum, K. S. Amalia, and I. A. Saputro, "Penerapan Metode Least Significant Bit (LSB) dalam Menyisipkan Pesan Rahasia pada Citra Digital: Sebuah Pendekatan Steganografi," in *Prosiding SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNAS) 2023*, 2023, no. November, pp. 176–183.
- [3] K. Wang and J. Wu, "Analysis and Improvement of LSB Steganography Detection Techniques," *Digit. Signal Process.*, vol. 116, p. 103055, 2021.
- [4] W. Wu, X. Yang, and G. Li, "Robust image steganography detection using deep learning techniques," *Neurocomputing*, vol. 430, pp. 32–44, 2021, doi: 10.1016/j.neucom.2021.02.052.
- [5] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *J. Inf. Secur. Appl.*, vol. 40, pp. 217–235, 2018, doi: <https://doi.org/10.1016/j.jisa.2018.04.005>.
- [6] Y. Xu, J. Zhang, and Y. Zhao, "Image steganography detection using Gaussian mixture model and machine learning," *J. Electr. Eng. & Technol.*, vol. 18, no. 2, pp. 623–630, 2023, doi: 10.1007/s42835-023-01779-3.
- [7] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, and C. Valli, "Integration of Biometrics and Steganography: A Comprehensive Review," *Technologies*, vol. 7, no. 2, 2019, doi: 10.3390/technologies7020034.
- [8] A. P. Ratnasari and F. A. Dwiyanto, "Metode Steganografi Citra Digital," *Sains, Apl. Komputasi dan Teknol. Inf.*, vol. 2, no. 2, p. 52, 2020, doi: 10.30872/jsakti.v2i2.3300.
- [9] B. Li and J. Zhang, "Detection of adaptive steganography using statistical features and machine learning algorithms," *Comput. Mater. & Contin.*, vol. 70, no. 2, pp. 2855–2870, 2022, doi: 10.32604/cmc.2022.022702.
- [10] C. M. Azzura, M. Pratiwi, and D. Desyanti, "Implementasi Watermarking Desain Citra Menggunakan Metode Modifikasi End of File (Meof)," *JUTEKINF (Jurnal Teknol. Komput. dan Informasi)*, vol. 11, no. 1, pp. 1–

- 9, 2023, doi: 10.52072/jutekinf.v11i1.473.
- [11] C.Nagesh, N. K. Kumar, G. S. Gowd, and G. P. Reddy, "Adaptive Artificial Intelligence Techniques for QoS and Congestion Management in 5G Wireless Networks: A Literature," *INTERANTIONAL J. Sci. Res. Eng. Manag.*, vol. null, p. null, 2024, doi: 10.55041/ijrsrem36077.
- [12] M. Ahmed and S. Ramani, "Deep convolutional networks for steganography detection: A comparative analysis," *Comput. & Secur.*, vol. 107, p. 102278, 2022, doi: 10.1016/j.cose.2021.102278.
- [13] X. Zhang, R. Liu, and Y. Zhao, "Integrating Cipher Keys with GMM for Steganography Detection," *J. Inf. Secur. Appl.*, vol. 74, p. 103491, 2024.
- [14] K. Patel and S. Das, "A novel approach for steganography detection using Gaussian mixture model and ensemble classifiers," *J. Appl. Comput. Sci. & Math.*, vol. 22, no. 1, pp. 13–26, 2024, doi: 10.1007/s41451-024-00539-7.
- [15] A. Widyanto, K. Kusriani, and K. Kusnawi, "Pengaruh Keseimbangan Data terhadap Akurasi Model Support Vector Machine pada Data Set Donor Darah," *J. Teknol. Terpadu*, vol. 9, no. 2, pp. 79–88, 2023, doi: 10.54914/jtt.v9i2.771.
- [16] Y. Yohannes, M. E. Al Rivani, S. Devella, and M. Meiriyama, "Klasifikasi Motif Songket Palembang menggunakan Support Vector Machine berdasarkan Histogram of Oriented Gradients," *J. Teknol. Terpadu*, vol. 9, no. 2, pp. 143–149, 2023, doi: 10.54914/jtt.v9i2.1032.
- [17] P. Suresh and D. Kumar, "A novel machine learning-based approach for detecting adaptive steganography in digital images," *J. Digit. Forensics, Secur. Law*, vol. 18, no. 1, pp. 54–69, 2023, doi: 10.15394/jdfsl.2023.2116.
- [18] S. Ghojaria, "Sneakers Image Dataset Pinterest." 2022.
- [19] İ. Yağ and A. Altan, "Artificial Intelligence-Based Robust Hybrid Algorithm Design and Implementation for Real-Time Detection of Plant Diseases in Agricultural Environments," *Biology (Basel)*, vol. 11, no. 12, p. 1732, Nov. 2022, doi: 10.3390/biology11121732.
- [20] M. Wojciuk, Z. Swiderska-Chadaj, K. Siwek, and A. Gertych, "The Role of Hyperparameter Optimization in Fine-Tuning of Cnn Models," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4087642.
- [21] M. Rijal, A. M. Yani, and A. Rahman, "Deteksi Citra Daun untuk Klasifikasi Penyakit Padi menggunakan Pendekatan Deep Learning dengan Model CNN," *J. Teknol. Terpadu*, vol. 10, no. 1, pp. 56–62, 2024, doi: 10.54914/jtt.v10i1.1224.
- [22] H. Haeruddin, H. Herman, and P. P. Hendri, "Pengembangan Aplikasi Emoticon Recognition dan Facial Recognition menggunakan Algoritma Local Binary Pattern Histogram (LBPH) dan Convolutional Neural Network (CNN)," *J. Teknol. Terpadu*, vol. 9, no. 1, pp. 49–55, 2023, doi: 10.54914/jtt.v9i1.613.
- [23] B. Hu, J. Tang, J. Wu, and J. Liu, "Rolling Bearing Fault Diagnosis Method Based on Improved Deep Belief Network," *J. Phys. Conf. Ser.*, vol. 1820, p. null, 2021, doi: 10.1088/1742-6596/1820/1/012105.