Penerapan Embedding Transformer untuk Enkripsi Teks dengan Pendekatan Steganografi

Rafi Mahmud Zain[1], Adrian Hartanto[2], Dhaman[3], Septian Pratama[4]
[1,2,3,4] Program Studi Teknik Informatika S-2, Universitas Pamulang
e-mail: rafizain777@gmail.com[1], adrian.hartanto692@gmail.com[2],
mas.dhaman@gmail.com[3], tian_yama@yahoo.com[4]

***Abstrak*— Penelitian ini mengkaji penerapan teknik steganografi berbasis transformer untuk menyembunyikan informasi dalam bentuk vektor embedding. Sistem yang dikembangkan terdiri dari tiga tahap utama: pertama, teks dikonversi menjadi vektor embedding menggunakan model transformer; kedua, embedding tersebut dienkripsi menggunakan algoritma Advanced Encryption Standard (AES); dan ketiga, embedding yang telah dienkripsi dapat didekripsi kembali untuk memperoleh embedding asli. Meskipun teks asli tidak dapat dikembalikan secara langsung, metode ini mampu menjaga integritas embedding sehingga tetap dapat digunakan untuk aplikasi tertentu. Hasil implementasi menunjukkan bahwa metode ini efektif dalam menyamarkan informasi melalui embedding dan memberikan tingkat keamanan yang baik berdasarkan analisis entropi menggunakan formula Shannon. Pengujian entropi membuktikan bahwa ciphertext yang dihasilkan memiliki tingkat keacakan yang tinggi, sehingga sulit untuk dianalisis secara langsung. Teknik ini menawarkan pendekatan sederhana namun inovatif dalam steganografi, dengan potensi aplikasi di berbagai domain, seperti komunikasi digital yang aman dan perlindungan data berbasis cloud. Namun, terdapat keterbatasan seperti ketergantungan pada ukuran embedding dan algoritma enkripsi yang memengaruhi efisiensi sistem. Penelitian ini memberikan kontribusi awal untuk pengembangan lebih lanjut dari teknik steganografi berbasis transformer, dengan peluang peningkatan dalam hal efisiensi, keamanan, dan skalabilitas.**

***Kata Kunci*—steganografi, transformer, *embedding*, enkripsi, AES, Shannon entropy**

I. PENDAHULUAN

Menyikapi era kita yang semakin digital, keamanan informasi telah menjadi perhatian utama di banyak bidang, dari komunikasi pribadi hingga data sensitif yang dimiliki oleh organisasi besar[1]. Pendekatan yang banyak digunakan untuk melindungi data adalah enkripsi. Tujuan metode ini adalah mengubah data asli ke dalam format yang tidak dapat dibaca oleh orang yang tidak berwenang. Meskipun enkripsi telah lama digunakan untuk melindungi informasi, ada teknik lain yang juga penting untuk menjaga kerahasiaan data: steganografi[2].

Steganografi adalah seni dan ilmu menyembunyikan pesan dalam media seperti gambar, teks atau audio sehingga orang yang tidak berwenang tidak dapat melihat pesan tersebut[3]. Teknik ini menyediakan lapisan keamanan ekstra dengan menyembunyikan fakta bahwa suatu pesan sedang dikirim. Steganografi dan enkripsi sering digunakan bersama-sama, tetapi steganografi berfokus pada penyembunyian keberadaan pesan, sedangkan enkripsi berfokus pada perlindungan isi pesan itu sendiri.

Dengan perkembangan di bidang kecerdasan buatan (AI), khususnya pembelajaran mendalam, model Transformer seperti BERT dan GPT telah terbukti sangat efektif dalam memahami dan menghasilkan teks berkualitas tinggi[4]. Model-model ini digunakan untuk tugas-tugas seperti pemrosesan bahasa alami (NLP), tetapi dapat juga digunakan untuk menghasilkan representasi numerik, atau penyematan, yang mencerminkan makna teks[5].

Tujuan dari pekerjaan ini adalah untuk menggabungkan teknik steganografi dengan transformer untuk secara efektif menyembunyikan pesan dalam bentuk penyisipan teks. Setelah menghasilkan padding, pesan dienkripsi menggunakan algoritma enkripsi simetris seperti AES (*Advanced Encryption Standard*) untuk keamanan tambahan[6][7]. Pendekatan ini memberikan cara sederhana namun efektif untuk menyembunyikan informasi. Prosedurnya terdiri dari tiga fase utama. Pertama, gunakan model transformator untuk mengubah teks menjadi penyematan, kemudian mengenkripsi penyematan, dan terakhir mendekripsi penyematan dan mengubah pesan[8].

Meskipun metode yang diusulkan dalam penelitian ini relatif sederhana dan bersifat eksperimental, penerapannya memperluas model berbasis transformator yang awalnya dikembangkan untuk pemrosesan bahasa alami hingga keamanan dan keamanan data. Penelitian ini tidak dimaksudkan untuk menggantikan sistem kriptografi yang ada dengan implementasi yang lebih sederhana, melainkan untuk menunjukkan bagaimana teknologi baru dapat digunakan untuk melindungi informasi, terutama dengan menggabungkan teknik AI baru yang kami tuju.

Karya ini berkontribusi pada pengembangan sistem steganografi yang lebih canggih dengan skala yang lebih kecil dan fokus pada penyembunyian teks biasa dengan menggunakan model Transformer untuk menghasilkan teknik penyisipan dan enkripsi untuk penyembunyian informasi. Diharapkan bahwa. Aplikasi ini menciptakan peluang untuk penelitian lebih lanjut untuk

mengembangkan metode keamanan yang lebih kompleks dan aman menggunakan teknologi berbasis AI.

II. METODE PENELITIAN

Pada bab ini, dijelaskan mengenai metode penelitian yang digunakan dalam eksperimen untuk menggabungkan teknik steganografi dengan model transformer, khususnya dalam menyembunyikan pesan melalui representasi embedding. Penelitian ini bertujuan untuk menunjukkan penerapan teknik-teknik ini dalam sebuah sistem yang sederhana namun efektif dalam menyembunyikan informasi. Berikut adalah tahapan metode yang digunakan dalam penelitian ini.

A. Pemilihan Model Transformer

Langkah pertama dalam penelitian ini adalah memilih model transformer yang digunakan untuk mengonversi teks menjadi representasi numerik atau *embedding*. Model transformer yang dipilih adalah All-MiniLM-L6-v2, sebuah model berbasis BERT yang telah terlatih untuk memahami semantik dari teks. Model ini mampu menghasilkan embedding dengan dimensi yang lebih kecil dan dapat digunakan untuk memahami makna kata atau kalimat dalam konteks tertentu. *Embedding* yang dihasilkan oleh model ini digunakan sebagai dasar untuk langkah-langkah selanjutnya dalam proses steganografi dan enkripsi.

B. Konversi Teks ke Embedding

Setelah pemilihan model, teks yang akan disembunyikan atau dienkripsi diubah menjadi embedding. Proses ini dilakukan dengan memasukkan teks ke dalam model transformer. Setiap kata atau kalimat yang dimasukkan akan diproses untuk menghasilkan vektor numerik yang merepresentasikan makna dari teks tersebut. Vektor ini memiliki dimensi tertentu, tergantung pada arsitektur model yang digunakan, dan dapat dianggap sebagai representasi semantik dari input teks. Sebagai contoh, jika kata "Rafi" dimasukkan ke dalam model transformer, model akan menghasilkan vektor dengan serangkaian angka yang menggambarkan makna semantik dari kata tersebut. Dalam penelitian ini, untuk menyederhanakan proses, hanya diambil sejumlah komponen pertama dari vektor tersebut untuk digunakan sebagai data yang akan dienkripsi.

C. Enkripsi Embedding dengan AES

Setelah embedding teks dihasilkan, langkah berikutnya adalah mengenkripsi vektor tersebut menggunakan algoritma enkripsi simetris, yaitu AES (*Advanced Encryption Standard*). AES dipilih karena merupakan algoritma yang banyak digunakan dalam berbagai aplikasi untuk menjaga kerahasiaan data. Pada tahap ini, vektor embedding yang telah dihasilkan diubah menjadi bentuk byte yang dapat diproses oleh algoritma AES. Proses enkripsi dilakukan dengan menggunakan kunci enkripsi yang aman. Kunci ini tidak hanya memastikan bahwa data terenkripsi dengan aman, tetapi juga memungkinkan untuk mendekripsi data kembali ke bentuk semula. Hasil dari enkripsi ini adalah data yang tidak dapat dibaca oleh pihak yang tidak berwenang, meskipun mereka dapat mengakses data tersebut.

D. Dekripsi dan Pemulihan Embedding

Setelah data terenkripsi, tahap terakhir dalam penelitian ini adalah dekripsi, yaitu untuk mengembalikan data yang telah dienkripsi menjadi bentuk yang dapat dibaca kembali. Dalam hal ini, dekripsi dilakukan menggunakan kunci yang sama dengan yang digunakan dalam enkripsi. Proses ini memungkinkan untuk mengembalikan *embedding* yang terenkripsi menjadi bentuk yang dapat digunakan kembali untuk merepresentasikan pesan semula. Namun, penting untuk dicatat bahwa meskipun *embedding* yang dihasilkan oleh model transformer dapat didekripsi, informasi semantik yang terkandung dalam *embedding* tersebut tidak dapat dipulihkan kembali ke bentuk teks aslinya. Ini adalah batasan yang dihadapi dalam metode ini, karena transformasi dari teks menjadi embedding bersifat satu arah dan tidak sepenuhnya *reversible*.

E. Pengamatan, Pengujian dan Evaluasi

Untuk menguji efektivitas sistem, dilakukan pengamatan dan evaluasi terhadap hasil enkripsi dan dekripsi. Pengujian dilakukan dengan menggunakan sejumlah kata atau kalimat yang disembunyikan dan dienkripsi menggunakan metode yang telah dijelaskan. Evaluasi ini mencakup dua aspek utama: pertama, seberapa efektif teknik steganografi dalam menyembunyikan pesan, dan kedua, apakah dekripsi dapat mengembalikan vektor embedding yang benar. Dalam hal ini, meskipun dekripsi tidak dapat mengembalikan teks asli, vektor embedding yang berhasil didekripsi harus mendekati bentuk asli dari embedding sebelum dienkripsi.

Selain itu, pengujian juga dilakukan untuk mengukur tingkat kerandoman atau keacakan pada hasil enkripsi menggunakan analisis entropi[9]. Entropi di sini mengacu pada seberapa tidak terprediksi atau acak data yang dihasilkan, dengan menggunakan Shannon Entropy sebagai ukuran kuantitatif. Shannon Entropy dirumuskan sebagai berikut:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log 2\, p(x_i) \quad (1)$$

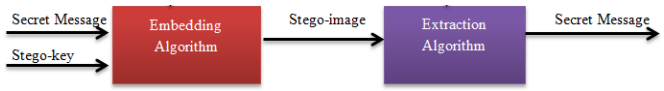
di mana:

- $H(X)$ adalah entropi dari data X,
- $p(x_i)$ adalah probabilitas kemunculan simbol x_i dalam data, dan

- n adalah jumlah simbol unik dalam data.

Pengujian entropi dilakukan pada hasil enkripsi untuk mengevaluasi tingkat keacakan ciphertext. Semakin tinggi nilai entropi, semakin sulit bagi pihak ketiga untuk menebak pola atau memprediksi isi data yang disembunyikan. Data ciphertext yang memiliki entropi mendekati maksimal menunjukkan bahwa metode enkripsi berhasil menghasilkan keluaran yang acak, yang merupakan karakteristik penting dari sebuah sistem keamanan informasi.

Hasil dari pengukuran entropi ini kemudian dibandingkan dengan nilai teoretis maksimum untuk memastikan bahwa metode yang digunakan cukup kuat dalam menyembunyikan pola dari data asli. Dengan melakukan pengujian ini, sistem dapat dievaluasi tidak hanya dari aspek keberhasilan proses enkripsi dan dekripsi, tetapi juga dari sisi keamanan data terhadap kemungkinan serangan analisis pola.



Gambar 1. Demonstrasi Proses Manipulasi Matriks AlphaTensor. Biasakan untuk menunjukkan signfikansi dari gambar pada judul gambar (*caption*).

III. IMPLEMENTASI DAN EKSPERIMEN

Perkembangan teknologi transformer telah membuka berbagai peluang baru dalam pengolahan data teks, termasuk dalam aplikasi keamanan informasi. Dalam penelitian ini, teknik steganografi diterapkan dengan memanfaatkan kemampuan transformer untuk menghasilkan representasi numerik (*embedding*) dari teks. Representasi ini kemudian dienkripsi menggunakan algoritma kriptografi simetris untuk melindungi informasi.

Bab ini menguraikan tahapan-tahapan implementasi sistem, mulai dari transformasi teks menjadi embedding, proses enkripsi untuk menyembunyikan informasi, hingga dekripsi untuk memulihkan kembali data yang telah dilindungi. Selain itu, eksperimen dilakukan untuk menguji efektivitas sistem, dengan mengevaluasi hasil enkripsi dan dekripsi. Alat, metode, dan hasil eksperimen dijabarkan secara mendetail untuk memberikan gambaran menyeluruh tentang aplikasi sistem ini.

A. Lingkungan Implementasi

Proses implementasi dilakukan pada lingkungan pengembangan berbasis Python, dengan memanfaatkan pustaka dan teknologi sebagai berikut:

1. Transformers dari *Hugging Face* untuk menghasilkan *embedding* teks.
2. PyCryptodome untuk proses enkripsi dan dekripsi menggunakan algoritma AES.
3. Google Colab atau Komputer Lokal dengan spesifikasi minimal RAM 8 GB untuk menangani model transformer secara efisien.

B. Arsitektur Sistem

Sistem ini dirancang dalam tiga tahap utama:

1. Konversi Teks ke Embedding

   Teks input dimasukkan oleh pengguna melalui antarmuka. Sistem memanfaatkan model transformer untuk menghasilkan representasi *embedding*. Model yang digunakan, All-MiniLM-L6-v2, menghasilkan vektor berdimensi tetap untuk setiap input teks.

2. Proses Enkripsi Embedding

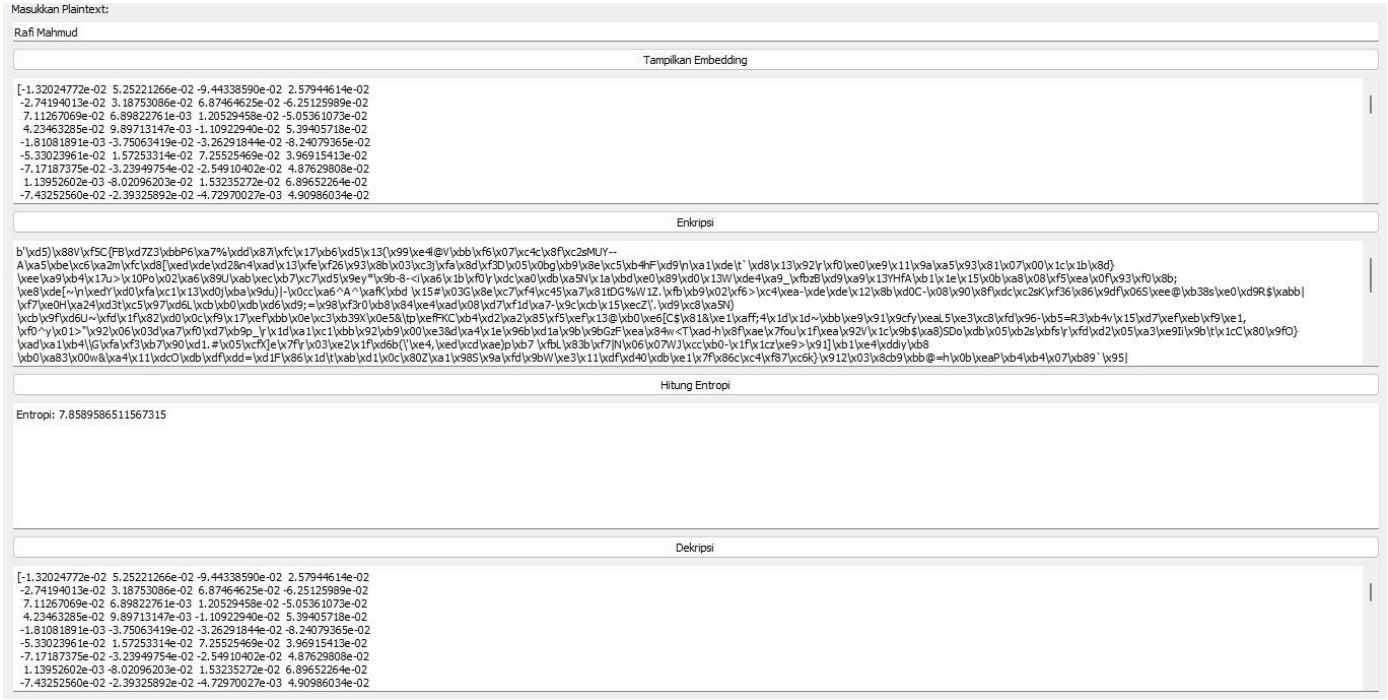
   Embedding yang dihasilkan dari tahap pertama dienkripsi menggunakan algoritma AES. Proses ini memerlukan kunci simetris yang harus dijaga kerahasiaannya. Hasil enkripsi berupa data yang tidak terbaca secara langsung dan aman untuk disembunyikan atau ditransmisikan.

3. Proses Dekripsi Embedding

   Ciphertext hasil enkripsi dapat didekripsi kembali dengan kunci yang sama. Hasil dekripsi berupa *embedding* dalam bentuk numerik yang sama dengan *embedding* asli sebelum dienkripsi.

IV. ANALISIS DAN HASIL PERCOBAAN

Pada bab ini, dilakukan analisis terhadap implementasi sistem dan eksperimen yang telah dilakukan. Tujuannya adalah mengevaluasi performa teknik steganografi berbasis transformer, baik dari segi keefektifan enkripsi dan dekripsi, tingkat keamanan data, maupun efisiensi proses. Hasil eksperimen menunjukkan bahwa embedding yang dihasilkan transformer dapat dienkripsi dengan baik menggunakan algoritma *Advanced Encryption Standard* (AES). Proses dekripsi juga berhasil memulihkan *embedding* yang terenkripsi menjadi bentuk awal tanpa kehilangan informasi. Namun, terdapat beberapa aspek yang perlu diperhatikan, seperti ukuran embedding yang cukup besar sehingga dapat memengaruhi kecepatan proses enkripsi dan dekripsi.



Gambar 2. Proses Keseluruhan Sistem, dari mulai Embedding, Enkripsi, Perhitungan Entropy dan Dekripsi

Salah satu keunggulan utama dari pendekatan steganografi berbasis transformer adalah kemampuan untuk memanfaatkan *embedding* yang dihasilkan model transformer sebagai representasi data yang kompleks namun tetap terstruktur. *Embedding* ini secara alami sudah memiliki tingkat abstraksi yang tinggi, sehingga lebih sulit untuk diinterpretasikan oleh pihak yang tidak memiliki kunci enkripsi. Ditambah dengan penerapan algoritma AES untuk proses enkripsi, metode ini menawarkan lapisan keamanan tambahan yang menjadikannya cocok untuk menyembunyikan informasi sensitif. Keunggulan lain adalah fleksibilitas metode ini dalam menangani berbagai jenis teks, baik yang pendek maupun panjang. Dengan bantuan model transformer, sistem dapat menangkap makna semantik dari teks yang dimasukkan, sehingga informasi yang tersembunyi tetap terjaga relevansinya saat diperlukan untuk proses dekripsi. Selain itu, metode ini dapat dengan mudah diadaptasi ke berbagai aplikasi, mulai dari komunikasi aman hingga penyimpanan data rahasia, tanpa memerlukan perubahan signifikan pada arsitektur dasar sistem.

Namun, pendekatan ini juga memiliki beberapa kelemahan yang perlu diperhatikan. Salah satunya adalah ketergantungan pada *embedding* yang dihasilkan model transformer, yang ukurannya dapat cukup besar. Hal ini dapat memengaruhi efisiensi proses enkripsi dan dekripsi, terutama jika sistem diimplementasikan pada perangkat dengan sumber daya terbatas. Selain itu, karena embedding yang dihasilkan bersifat deterministik, pihak yang memahami struktur model transformer yang digunakan mungkin dapat memanfaatkan informasi ini untuk mencoba membalikkan proses transformasi, meskipun tanpa kunci enkripsi hasilnya tetap sulit dipecahkan.

Keterbatasan lainnya terletak pada tingkat kompleksitas algoritma enkripsi dan dekripsi. Penerapan AES dalam proses ini membutuhkan pemrosesan tambahan yang dapat menambah waktu eksekusi secara keseluruhan, terutama ketika menangani

volume data yang besar. Di sisi lain, meskipun keamanan embedding dapat diperkuat dengan algoritma kriptografi, kelemahan dalam implementasi (seperti pengelolaan kunci yang kurang aman) dapat menjadi celah yang membahayakan integritas sistem. Secara keseluruhan, teknik ini menawarkan kombinasi unik antara representasi semantik berbasis transformer dan keamanan berbasis kriptografi, yang menjadikannya menarik untuk aplikasi praktis. Namun, penggunaannya memerlukan perencanaan yang matang untuk mengatasi kendala teknis dan memastikan keandalan sistem dalam skenario dunia nyata.

V. KESIMPULAN

Dalam penelitian ini, telah berhasil dikembangkan sebuah sistem sederhana yang menerapkan teknik steganografi berbasis transformer. Sistem ini memanfaatkan kemampuan transformer untuk menghasilkan vektor embedding dari teks, yang kemudian dienkripsi menggunakan algoritma AES sebelum disimpan atau ditransmisikan. Dekripsi dilakukan untuk mengembalikan vektor embedding yang mendekati bentuk aslinya, meskipun tidak bertujuan untuk mengembalikan teks awal secara langsung. Hasil implementasi menunjukkan bahwa pendekatan ini mampu menyembunyikan informasi dalam bentuk vektor embedding dengan tingkat keamanan yang dapat ditingkatkan melalui algoritma enkripsi yang digunakan. Pengujian entropi pada ciphertext juga memperlihatkan tingkat keacakan yang tinggi, mengindikasikan bahwa pola data asli telah berhasil disamarkan. Dengan demikian, metode ini tidak hanya efektif untuk menyembunyikan data, tetapi juga menunjukkan potensi keamanan yang baik terhadap analisis pola.

Namun, terdapat beberapa keterbatasan yang perlu dicatat. Pertama, metode ini hanya dapat digunakan untuk menyembunyikan informasi yang berbasis teks dan tidak dapat mengembalikan teks asli secara langsung setelah dekripsi. Kedua, performa sistem bergantung pada ukuran vektor embedding dan algoritma enkripsi yang digunakan, yang dapat memengaruhi efisiensi waktu dan konsumsi sumber daya. Meskipun demikian, penelitian ini memberikan kontribusi dalam memperkenalkan konsep steganografi berbasis transformer sebagai pendekatan yang sederhana namun inovatif. Dengan pengembangan lebih lanjut, teknik ini berpotensi diaplikasikan pada skenario yang lebih kompleks, seperti pengamanan data dalam komunikasi digital atau penyembunyian pesan pada sistem berbasis cloud.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Yayasan Sasmita Jaya Universitas Pamulang, Program Pascasarjana Universitas Pamulang, Program Studi Teknik Informatika S-2 Universitas Pamulang

DAFTAR PUSTAKA

[1] M. M., A. A., and F. A., “An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 3, pp. 361–366, 2016, doi: 10.14569/ijacsa.2016.070350.

[2] A. Supriyatna, “Analisis Bibliometrik Shannon Entropy : Tren Penelitian dan Relevansi Multidimensional,” *J. Infortech*, vol. 6, no. 2, pp. 163–170, 2024.

[3] F. Baso, N. A. Rais, H. Hatima, P. Auralia, and A. Nur, “Steganografi Berbasis Kecerdasan Buatan untuk Mengatasi Ancaman Terbaru dalam Keamanan Data,” *J. Mediat. J. Media Pendidik. Tek. Inform. dan Komput.*, vol. 7, no. 3, pp. 145–149, 2024.

[4] M. Bai, J. Yang, K. Pang, H. Wang, and Y. Huang, “Towards Next-Generation Steganalysis: LLMs Unleash the Power of Detecting Steganography,” *arXiv*, pp. 1–13, 2024, [Online]. Available: https://arxiv.org/abs/2405.09090v1

[5] M. Bai, J. Yang, K. Pang, Y. Huang, and Y. Gao, “Semantic Steganography: A Framework for Robust and High-Capacity Information Hiding using Large Language Models,” *arXiv*, 2024, [Online]. Available: http://arxiv.org/abs/2412.11043

[6] P. P. Bandekar and G. C. Suguna, “LSB Based Text and Image Steganography Using AES Algorithm,” *Proc. 3rd Int. Conf. Commun. Electron. Syst. ICCES 2018*, no. Icces, pp. 782–788, 2018, doi: 10.1109/CESYS.2018.8724069.

[7] S. F. Mare, M. Vladutiu, and L. Prodan, “Secret data communication system using steganography, AES and RSA,” *2011 IEEE 17th Int. Symp. Des. Technol. Electron. Packag. SIITME 2011 - Conf. Proc.*, pp. 339–344, 2011, doi: 10.1109/SIITME.2011.6102748.

[8] S. Zhang, Z. Yang, J. Yang, and Y. Huang, “Linguistic Steganography: From Symbolic Space to Semantic Space,” *IEEE Signal Process. Lett.*, vol. 28, pp. 11–15, 2021, doi: 10.1109/LSP.2020.3042413.

[9] A. Khumaidi, “Simulasi Entropi Shannon, Entropi Renyi, dan informasi pada kasus Spin Wheel,” *AKSIOMA J. Mat. dan Pendidik. Mat.*, vol. 12, no. 1, pp. 120–128, 2021, doi: 10.26877/aks.v12i1.6893.