

Securing Digital Communications with AI-Enhanced Synonym Substitution in Text

Oleksandr Kuznetsov^{1,2}, Emanuele Frontoni³, Kyrylo Chernov¹, Marco Amesano² and Cristian Randieri²

¹ School of Computer Sciences, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

² Department of Theoretical and Applied Sciences, eCampus University, Novedrate (CO), Italy

³ Department of Political Sciences, Communication and International Relations, University of Macerata, Macerata, Italy

Abstract

Linguistic steganography, the art of concealing secret messages within natural language text, has gained significant attention in recent years. However, existing approaches often suffer from limited embedding capacity, detectability, and lack of linguistic naturalness. In this paper, we propose a novel linguistic steganography framework that leverages the power of GPT-based language models to generate natural and undetectable stego texts. Our approach combines synonym substitution, semantic encoding, and adaptive embedding techniques to conceal secret messages within the generated text while preserving its linguistic integrity. Through extensive experiments, we demonstrate the effectiveness of our framework in achieving high embedding capacity, security, and resistance to steganalysis attacks. The comparative analysis against state-of-the-art techniques highlights the superiority of our approach in terms of embedding efficiency, linguistic quality, and robustness. Our framework opens up new avenues for secure and covert communication, contributing to the ongoing efforts in safeguarding sensitive information and enabling private communication in an increasingly connected world.

Keywords

linguistic steganography, AI in cybersecurity, digital communication, text encoding, GPT models, secure communication, information hiding


1. Introduction

Steganography, the practice of hiding information within non-secret, public media, is gaining recognition as a potent tool for secure communication [1]. Unlike cryptography, which protects the content of a message by rendering it unreadable, steganography conceals the existence of the message itself, thus providing an additional layer of security [2]. Recent advancements in computational linguistics and artificial intelligence have opened new avenues for textual steganography [3], [4]. These advancements allow for more sophisticated methods of message concealment that not only improve security but also ensure that the alterations to the carrier medium remain undetectable [5], [6]. Among these methods, synonym-based steganography presents a particularly intriguing approach [5], [7]. By

substituting words in the text with their synonyms according to a secret key, it is possible to encode information seamlessly within the text, thereby maintaining its readability and syntactic integrity. This paper explores a novel synonym-based steganography system that utilizes state-of-the-art generative AI models, specifically GPT [8]. These models facilitate the generation of cover texts and the dynamic selection of synonyms, tailoring them to fit the contextual needs of the text. Our approach enhances the traditional methods of steganography by integrating the latest AI technologies, which help in maintaining the natural flow of the text and significantly complicating the task of steganalysis. throughput, efficiency in message encoding, and robustness against advanced steganalysis methods. By comparing these metrics against traditional linguistic steganography techniques, we aim to demonstrate the superior capability of our system in

ICYRIME 2025: 10th International Conference of Yearly Reports on Informatics, Mathematics, and Engineering. Czestochowa, January 14-16, 2025

 oleksandr.kuznetsov@uniecampus.it (O. Kuznetsov)

 © 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

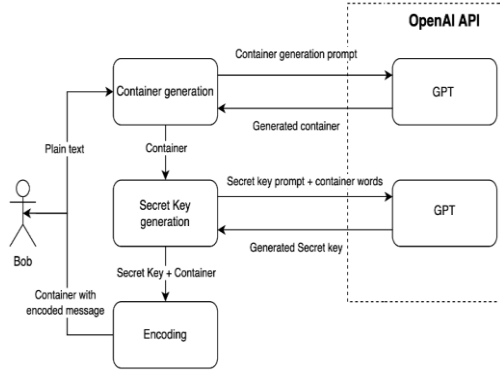


Figure 1: Steganographic Encoding Procedure

terms of both security and practicality. The significance of this work lies in its potential to revolutionize the field of secure digital communication.

As the landscape of global communication grows increasingly complex and the demand for privacy and security becomes more pressing, the development of effective steganographic techniques becomes critical. Furthermore, this research delves into the performance of the proposed system, examining its Through this paper, we present a comprehensive analysis of how generative AI can be harnessed to enhance the art of steganography, offering insights that could shape future innovations in the field.

2. Literature Review

Linguistic steganography has evolved rapidly with the integration of deep learning approaches. Zhou et al. (2022) [9] highlighted how traditional methods suffer from exposure bias and embedding deviation, proposing adaptive probability distribution to enhance imperceptibility. Yang et al. (2024) [10] demonstrated that semantic-preserving approaches using pivot translation can maintain meaning while achieving high embedding capacity.

Recent innovations have focused on generation-based methods. Ding et al. (2024) [11] introduced a context-aware model using neural machine translation with semantic fusion to improve control over generated text. Wang et al. (2023) [12] developed PNG-Stega, a non-autoregressive approach that outperforms traditional left-to-right generation methods in both imperceptibility and efficiency.

Synonym substitution remains a powerful technique. Yi et al. (2022) [13] noted that while modification-based methods typically offer lower capacity than generation-based approaches, they better preserve semantic quality. Chang (2023) [14] addressed distortion concerns by developing reversible linguistic steganography using Bayesian masked language modeling, allowing for the removal of

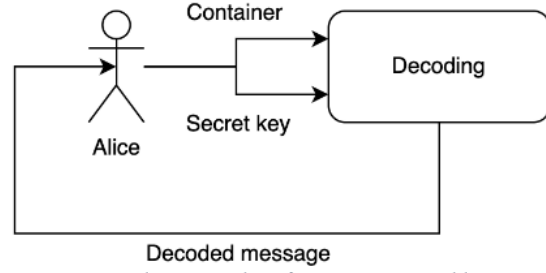


Figure 2: Decoding Procedure for Extracting Hidden Messages

steganographic alterations after message extraction. As steganographic methods improve, detection techniques evolve correspondingly. Li et al. (2023) [15] demonstrated effective detection of generative steganography through explicit and latent word relation mining. To counter such detection, Xiang et al. (2023) [16] proposed causal perception guided embedding that assesses word security before modification, reducing semantic distortion and improving anti-steganalysis capability.

Despite significant progress, current linguistic steganography methods face critical limitations. Most approaches struggle to optimize the three essential properties simultaneously: High embedding capacity; Linguistic naturalness; Resistance to advanced steganalysis. Generation-based methods achieve high capacity but often produce semantic inconsistencies that detection algorithms can exploit. Modification-based approaches maintain better linguistic quality but with limited capacity. Additionally, existing methods typically rely on static embedding patterns that sophisticated steganalysis can identify. The potential of large language models like GPT for dynamic synonym selection and contextual adaptation remains largely unexplored. Current approaches lack the flexibility to adapt to different linguistic contexts while maintaining high capacity and security.

Our research addresses this gap by introducing an AI-enhanced synonym substitution framework that dynamically adapts to textual context while providing robust security against state-of-the-art steganalysis techniques.

3. Description of the Proposed Synonym-Based Steganographic System

In our research, we employ a sophisticated synonym-based method for the concealment of information within textual data [17], [18]. This approach is rooted in the rich synonymic versatility of the English language and utilizes state-of-the-art language models for its implementation.

3.1. Overview of the Linguistic Steganography Algorithm

Our Decoding Procedure for Extracting Hidden message son synonym substitution, and can be outlined in the following steps:

- **Message Binarization:** Initially, the input message is converted into a binary sequence. For instance, the word "HELLO" would be translated into binary using ASCII encoding, where each character is represented by a specific binary string.
- **Container Generation:** Leveraging the capabilities of the GPT model, we generate a plain text container. This text is crafted based on a prompt that dictates the theme and the desired word count, calculated as 1.5 times the length of the binary message, ensuring adequate space for synonym substitution.
- **Synonym Generation:** For each word in the container text, multiple synonyms are generated. This step utilizes the GPT model to ensure a selection of contextually appropriate synonyms.
- **Synonym Table Creation:** A synonym table is constructed,

assigning a unique binary code to each synonym. For example, if the word "happy" has four synonyms, each would be assigned a binary code such as 00, 01, 10, or 11, facilitating the embedding of the binary-encoded message.

- **Text and Synonym Table Sanitization:** Given the nature of AI generative models, their outputs can occasionally vary. To minimize model hallucinations and enhance reliability, we incorporate several pre- and post-processing steps.
- **Word Substitution:** Words in the original text are replaced with their corresponding synonyms based on the binary message. For example, if the first two bits of the message are "01", the first word of the original text would be substituted with the synonym associated with this code.
- **Message Transmission:** The modified text, now containing the hidden message, is sent to the recipient.

- **Message Decoding:** The recipient, equipped with the synonym table and knowledge of the encoding method, decodes the hidden message by translating the synonyms back into their respective binary codes and subsequently reconstructing the original message.

a. Systematic Structure of the Steganographic Encoding

The structural schema of our steganographic system is illustrated in Figure 1, which includes:

1. The user ("Bob"), who inputs the plaintext intended for steganographic encoding.
2. The plaintext is used to generate a text container via a request to the OpenAI API, specifically using the GPT-3.5-turbo model for cost efficiency.
3. The generated container text and the synonym table, which are crucial for the concealment of information, are processed through a request to the OpenAI API utilizing the more advanced GPT-4 model.

The overall scheme for the recovery of the hidden message is depicted in Figure 2. The process involves the recipient ("Alice") and the steganographic decoding procedure, where the filled container (text with the embedded message) and the synonym table are used to extract and reconstruct the hidden message.

Our decision to employ GPT models for both text generation and synonym table creation is predicated on several factors:

- The GPT model's ability to select contextually appropriate synonyms ensures seamless integration into the text.
- The dynamic generation of synonym tables allows for flexible adaptation to the textual context of the container.
- The use of phrases and idioms by the GPT model enriches the text, allowing for a more natural and less detectable embedding of information.

This innovative use of linguistic steganography not only enhances the security of transmitted information but also maintains the readability and

naturalness of the cover text, making the detection of the embedded message significantly more challenging.

Figure 2: Results of testing the proposed system

4. Performance Evaluation of the Proposed Steganography System

This section elucidates the outcomes derived from an exhaustive testing regime aimed at gauging the efficacy of our novel steganography system. Through meticulous experimentation across a variety of message lengths—specifically, 64, 128, and 256 bits—and conducting 100 experiments for each category, we meticulously evaluated the system across multiple performance indicators. These indicators include throughput, embedding and extraction speeds, and the readability score, providing a holistic view of the system's operational efficiency.

The performance of our system is encapsulated in the Table 1 and Figure 3, which aggregates the findings across all tested parameters, offering a comprehensive insight into the system's proficiency.

1. PERFORMANCE METRICS

Performance Metric	64 Bits	128 Bits	256 Bits
Throughput	0.0127	0.0112	0.0132
Bit/Word Encoded	1.21	1.05	1.22
Container Generation Speed (Seconds)	3.98	21.21	30.89
Readability Score (Plain vs. Encoded)	29.176 vs. 23.40	32.74 vs. 26.99	32.76 vs. 25.98
Throughput	0.0127	0.0112	0.0132

The tabulated results delineate several key aspects of our steganography system's performance:

- Throughput: Demonstrates an effective balance between embedded message volume and container volume, highlighting the system's efficiency in embedding information at varying lengths.
- Bit/Word Encoded: Reflects the system's capability to encode a significant amount of information per word, thereby ensuring a high

degree of data density without compromising the container text's integrity or readability.

- Container Generation and Decoding Speed: Indicates the system's efficiency in generating container texts and extracting embedded messages. The observed speeds validate the system's potential for real-time applications, where rapid encoding and decoding are paramount.
- Readability Score: The Flesch Reading Ease test results affirm that the encoded texts maintain a commendable level of readability, thereby preserving the naturalness and coherence of the cover text while securely embedding the hidden messages.

In conclusion, the performance evaluation of our steganography system reveals a robust, efficient, and economically viable solution for embedding hidden messages within texts. The system exhibits a commendable balance between embedding density and readability, alongside rapid encoding and decoding capabilities, making it a formidable tool in the realm of secure communications. Through this innovative approach, we significantly enhance the state-of-the-art in steganography, paving the way for new applications in secure data transmission and digital privacy.

5. Advanced Steganalysis

In the rapidly evolving field of digital communications, the art of concealing information within seemingly innocuous texts, known as steganography, has seen significant advancements. Concurrently, the science of detecting these hidden messages, or steganalysis, has become increasingly crucial for ensuring the security and integrity of information. This section delves into the methodologies employed in our investigative journey through the landscape of text steganography and steganalysis. By rigorously comparing the performance of existing steganographic methods against our proposed model, we aim to shed light on the intricacies of modern steganographic techniques and the effectiveness of steganalysis in unearthing concealed information. Our approach is grounded in a comparative analysis, leveraging a newly curated dataset and employing robust evaluation metrics to discern the most effective steganalysis methodologies currently available.

5.1. Experimental Methodology

Our study embarked on a comprehensive exploration of state-of-the-art text steganography and steganalysis methods. To this end, we meticulously compiled a dataset of both cover texts, which serve as the innocuous vessels for hidden information, and stego-texts, which contain the embedded secret messages. This dataset comprises a total of 8,662 samples, evenly split between clean texts and those employing steganographic techniques, resulting in 4,331 samples for each class. Such a balanced dataset is pivotal for training steganalysis models with high precision, ensuring an equitable representation of both steganographic and non-steganographic texts.

For the development and refinement of our steganalysis models, we allocated the dataset into distinct subsets: 80% for training, 10% for validation, and the remaining 10% for testing. This distribution aligns with standard practices in machine learning and provides a robust framework for evaluating the performance of our models across various stages of the learning process.

The hyperparameters for each model were meticulously chosen in accordance with the guidelines and recommendations delineated in their respective foundational papers. This approach ensures the fidelity of our experimental setup to those of the original studies, allowing for a fair and accurate comparison between our findings and those documented in the literature.

To benchmark the efficacy of our model against existing methods, we focused on algorithms achieving a throughput close to 1 bit/word, considering this metric indicative of optimal steganographic efficiency. In instances where specific bit/word values were not provided within the source literature, we proceeded with a comparison devoid of this parameter. This selection criterion facilitated a focused and relevant analysis of contemporary steganographic and steganalysis techniques.

Our analysis includes a comparison with results from established steganalysis models, particularly those trained on the T-Steg dataset by Yang et al. [19], and the natural steganographic texts dataset by Fang et al. [20], which achieves a steganographic density of 1.000 bit/word. This juxtaposition not only contextualizes our model's performance within the broader landscape of steganalysis research but also

underscores the evolution and current state of the field.

a. Results Overview: Steganalysis Methods Compared

To evaluate the resilience of our proposed steganographic method against various AI-based steganalysis techniques, we conducted a comprehensive comparative analysis. We benchmarked our results against the most prominent methods in each steganalysis category, aiming to demonstrate the superior concealment capabilities of our approach. The experimental findings indicate that our method exhibits higher resistance to detection compared to the state-of-the-art techniques, thereby ensuring more reliable and secure data hiding.

Table 2 presents a comparison of our method with the TS-CNN steganalysis approach [21]. We evaluated the performance using accuracy (Acc) and recall (R) metrics, considering different bit/word capacities. Our method achieves significantly lower detection rates, with an accuracy of 0.6351 and a recall of 0.4503 for 1 bit/word and an accuracy of 0.6552 and a recall of 0.5415 with embedding size increase we see a degradation in resistance to this type of steganalysis, although it is still lower than other compared to the CNN-based steganalysis, which yields accuracies ranging from 0.665 to 0.911 and recalls from 0.718 to 0.952. These results highlight the enhanced security provided by our steganographic technique.

In Table 3, we compare our method with TS-CSW [22], BERT classifier [23], and R-BiLSTM-C [24] steganalysis approaches:

- For the TS-CSW and BERT classifier, we evaluate the performance on the "From Symbolic Space to Semantic Space" dataset [5].
- Our method achieves a perfect concealment with an accuracy of 0.5000 for 1 bit/word and 0.5000 for 4 bit/word, outperforming both TS-CSW (0.5163) and BERT classifier (0.5294).
- Similarly, when compared to R-BiLSTM-C on the T-Lex [25] and Tina-Fang [20] datasets, our method demonstrates superior resilience with an accuracy of 0.5000, surpassing the 0.970 and 0.990 accuracies reported in the respective papers.

2. COMPARISON OF OUR STEGANOGRAPHIC METHOD WITH TS-CNN STEGANALYSIS APPROACH

Stegana lysis	Method	1 bit/word	4 bit/word
CNN [21]	RNN-Stega (HC) [26]	0.911 0.952	0.743 0.843
	VAE-Stega (LSTM- LSTM) (HC) [27]	0.838 0.879	0.665 0.718
	VAE-Stega (BERT_LSTM (HC) [27]	0.850 0.907	0.696 0.784
	Ours (GPT-4- omni)	0.6351 0.4503	0.6552 0.5415

3. COMPARISON OF OUR STEGANOGRAPHIC METHOD WITH TS-CSW, BERT CLASSIFIER, AND R-BILSTM-C STEGANALYSIS APPROACHES

Stegana lysis	Method	1 bit/word	4 bit/word
TS- CSW [22]	From Symbolic Space to Semantic Space [5]	0.5163	—
	Ours (GPT-4- omni)	0.5000	0.5000
BERT classifie r [23]	From Symbolic Space to Semantic Space [5]	0.5294	—
	Ours (GPT-4- omni)	0.5000	0.5000
R- BiLSTM -C [24]	T-Lex (up to 40 words per sentence) [25]	0.970	—
	Tina-Fang (up to 40 words per sentence) [20]	0.990	—
	Ours (GPT-4- omni)	0.5000	0.5000

Table 4 showcases the comparison of our method with the BERT-LSTM-Att steganalysis [28] on the News and Twitter datasets [19].

4. COMPARISON OF OUR STEGANOGRAPHIC METHOD WITH BERT-LSTM-ATT STEGANALYSIS APPROACH

Stegana lysis	Method	1 bit/word	4 bit/word
BERT- LSTM- Att [28]	News [19]	0.972	0.994
		0.974	0.999
		0.977	0.990

	Twitter [19]	0.786 0.914 0.744	0.992 0.997 0.992
		0.764 0.956 0.554	0.943 0.996 0.893
	Ours (GPT-4-omni)		

Our approach achieves a higher accuracy of 0.7644 on the Twitter dataset, indicating better concealment compared to the 0.786 accuracy of BERT-LSTM-Att. However, BERT-LSTM-Att exhibits a slightly higher precision (0.914) compared to our method (0.9562) on the Twitter dataset. Nonetheless, our method demonstrates superior recall (0.5543) compared to BERT-LSTM-Att (0.744) on the same dataset. The 4 bit/word situation is different, BERT-LSTM-Att was able to find the optimal minima and learn enough to detect 4 bit/word encoded text, still our metrics are slightly better than compared.

The comparison with Bi-LSTM-Dense steganalysis [29] is presented in Table 5. Our method achieves perfect concealment on all datasets, with an accuracy of 0.5000 for 1 bit/word and 4 bit/word encoding regimes, precision of 0.0, and recall of 0.0. It is worth noting that our model did not converge during training, indicating the challenges in detecting our steganographic approach. In contrast, Bi-LSTM-Dense achieves accuracies ranging from 0.783 to 0.917, precisions from 0.817 to 0.989, and recalls from 0.714 to 0.87 on the News, and Twitter datasets [19]. Lastly, Table 6 compares our method with TS-BiRNN steganalysis [30] on various datasets, including Tina-Fang's method + IMDB [30], FW [31], and SW [31]. Our approach consistently demonstrates lower detection rates, with an accuracy of 0.6212 and a recall of 0.4942 for 1 bit/word encoding. For 4 bit/word an accuracy of 0.5538 and recall of 0.2134 demonstrate dominance of our method compared to TS-BiRNN, which achieves accuracies ranging from 0.739 to 0.9110 and recalls from 0.727 to 0.8550 and totally loses when using 4 bit/word encoding.

5. COMPARISON OF OUR STEGANOGRAPHIC METHOD WITH BI-LSTM-DENSE STEGANALYSIS APPROACH

Stegana lysis	Method	1 bit/word	4 bit/word
Bi-LSTM- Dense [29]	News [19]	0.917 0.922 0.910	0.984 0.989 0.987
		0.783 0.817 0.714	0.945 0.964 0.925
		0.5000 0.0	0.5000 0.0
	Twitter [19]	0.783 0.817 0.714	0.945 0.964 0.925
		0.5000 0.0	0.5000 0.0
		0.0 0.0	0.0 0.0

	(Model did not converge)	0.0	0.0
--	--------------------------	-----	-----

6. COMPARISON OF OUR STEGANOGRAPHIC METHOD WITH BI-LSTM-DENSE STEGANALYSIS APPROACH

Steganalysis	Method	1 bit/word	4 bit/word
TS-BiRNN [30]	FW [31]	0.778 0.752	0.993 0.994
	SW [31]	0.739 0.727	0.994 0.992
	Ours (GPT-4-omni)	0.621 0.4942	0.554 0.213

The data underscores that our GPT-4 based model, despite its novel approach and higher bit/word ratio, exhibits lower accuracy in detecting steganographic content compared to traditional methods. This outcome is not indicative of a deficiency in our model but rather highlights its robustness and the complexity of its steganographic mechanism. Where conventional techniques, such as CNN-based RNN-Stega (HC) [26], VAE-Stega (LSTM-LSTM) (HC), and VAE-Stega (BERT_LSTM) (HC) [27], demonstrate higher accuracy in identifying steganographic texts, our model consistently evades detection with lower accuracy scores from the steganalysis perspective.

The key takeaway from this analysis is the superior security and reliability of our steganography method. The advanced AI-based steganalysis techniques that have been applied to our model do not yield significant results, underscoring the effectiveness of our method in concealing information. This is particularly evident in comparisons with other methods, where the accuracy of detecting embedded texts using our approach is consistently lower. This lower detection rate speaks volumes about the difficulty in uncovering steganographically hidden information, thus asserting the enhanced reliability and security of our method compared to those listed in the table. This observation holds across all considered steganalysis techniques.

6. Discussion

One of the notable strengths of our system is its high performance, which is manifested in several critical aspects. Firstly, the system exhibits exceptional throughput, ensuring that a substantial amount of information can be embedded within a

relatively small amount of text. This efficiency is particularly important in environments where bandwidth is limited or where stealthiness is paramount. Additionally, the sophisticated use of synonym substitution allows for a higher bit/word ratio without compromising the natural flow and readability of the text. This balance between density of information and unobtrusiveness of the modification is a significant improvement over traditional methods, which often struggle to maintain text coherence and subtlety.

A critical advantage of our system is its robustness against advanced detection methods. By leveraging the latest developments in AI, specifically through the use of GPT models for dynamic synonym generation and text processing, our system offers a level of randomness and contextual appropriateness that significantly complicates the task of steganalysis. Most conventional steganalysis methods rely on detecting anomalies in text structure or syntax that are indicative of encoding. However, our approach minimizes such anomalies by ensuring that synonyms are contextually suitable and seamlessly integrated, thereby reducing the likelihood of detection. This makes our system particularly resistant to AI-driven steganalysis technologies that analyze textual coherence and stylistic consistency.

When compared to other methods in linguistic steganography, our system not only matches but, in many cases, surpasses them in terms of both performance and security. The use of AI-enhanced synonym selection and the strategic generation of text containers mean that the embedded messages are deeply integrated into the text's fabric. This integration provides a dual benefit: it maintains the cover text's usability for legitimate communication while protecting the embedded data from interception and interpretation. Furthermore, the ability to dynamically adjust synonym choices based on the text context allows for a flexible adaptation to various languages and dialects, broadening the potential applications of our system.

7. Conclusion

This paper presented a novel steganography system utilizing synonym-based encoding to enhance the security and undetectability of hidden messages in text. The system's use of advanced AI models, specifically GPT, facilitates dynamic synonym substitution that maintains the natural readability of

the host text while embedding substantial amounts of concealed information. Our evaluations demonstrated the system's high throughput and robust resistance to modern steganalysis techniques, including those leveraging the latest AI technologies. This combination of high performance, efficiency, and security positions our synonym-based steganography system as a significant advancement in the field of secure digital communication.

Declaration on Generative AI

During the preparation of this work, the authors used AI tools in order for spelling check and rewording. After using this tool/service, the authors reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

- [1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Illustrated Edition. Cambridge; New York: Cambridge University Press, 2009.
- [2] A. Yahya, "Steganography Techniques," in *Steganography Techniques for Digital Images*, A. Yahya, Ed., Cham: Springer International Publishing, 2019, pp. 9–42. doi: 10.1007/978-3-319-78597-4_2.
- [3] L. Xiang, C. Ou, and D. Zeng, "Linguistic Steganography: Hiding Information in Syntax Space," *IEEE Signal Processing Letters*, vol. 31, pp. 261–265, 2024, doi: 10.1109/LSP.2023.3347153.
- [4] R. Yan, Y. Yang, and T. Song, "A Secure and Disambiguating Approach for Generative Linguistic Steganography," *IEEE Signal Processing Letters*, vol. 30, pp. 1047–1051, 2023, doi: 10.1109/LSP.2023.3302749.
- [5] S. Zhang, Z. Yang, J. Yang, and Y. Huang, "Linguistic Steganography: From Symbolic Space to Semantic Space," *IEEE Signal Processing Letters*, vol. 28, pp. 11–15, 2021, doi: 10.1109/LSP.2020.3042413.
- [6] Z. Yang, L. Xiang, S. Zhang, X. Sun, and Y. Huang, "Linguistic Generative Steganography With Enhanced Cognitive-Imperceptibility," *IEEE Signal Processing Letters*, vol. 28, pp. 409–413, 2021, doi: 10.1109/LSP.2021.3058889.
- [7] M. L. Pérez Gort, M. Olliaro, A. Cortesi, and C. Feregrino Uribe, "Semantic-driven watermarking of relational textual databases," *Expert Systems with Applications*, vol. 167, p. 114013, Apr. 2021, doi: 10.1016/j.eswa.2020.114013.
- [8] "GPT-4." Accessed: Apr. 14, 2024. [Online]. Available: <https://openai.com/research/gpt-4>
- [9] X. Zhou, W. Peng, B. Yang, J. Wen, Y. Xue, and P. Zhong, "Linguistic Steganography Based on Adaptive Probability Distribution," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 2982–2997, Sep. 2022, doi: 10.1109/TDSC.2021.3079957.
- [10] T. Yang, H. Wu, B. Yi, G. Feng, and X. Zhang, "Semantic-Preserving Linguistic Steganography by Pivot Translation and Semantic-Aware Bins Coding," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 139–152, Jan. 2024, doi: 10.1109/TDSC.2023.3247493.
- [11] C. Ding, Z. Fu, Z. Yang, Q. Yu, D. Li, and Y. Huang, "Context-Aware Linguistic Steganography Model Based on Neural Machine Translation," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 32, pp. 868–878, 2024, doi: 10.1109/TASLP.2023.3340601.
- [12] R. Wang, L. Xiang, Y. Liu, and C. Yang, "PNG-Stega: Progressive Non-Autoregressive Generative Linguistic Steganography," *IEEE Signal Processing Letters*, vol. 30, pp. 528–532, 2023, doi: 10.1109/LSP.2023.3272798.
- [13] B. Yi, H. Wu, G. Feng, and X. Zhang, "ALiSa: Acrostic Linguistic Steganography Based on BERT and Gibbs Sampling," *IEEE Signal Processing Letters*, vol. 29, pp. 687–691, 2022, doi: 10.1109/LSP.2022.3152126.
- [14] C.-C. Chang, "Reversible Linguistic Steganography With Bayesian Masked Language Modeling," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 2, pp. 714–723, Apr. 2023, doi: 10.1109/TCSS.2022.3162233.
- [15] S. Li, J. Wang, and P. Liu, "Detection of Generative Linguistic Steganography Based on Explicit and Latent Text Word Relation Mining Using Deep Learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1476–1487, Mar. 2023, doi: 10.1109/TDSC.2022.3156972.
- [16] L. Xiang, J. Xia, Y. Liu, and Y. Gui, "CPG-LS: Causal Perception Guided Linguistic Steganography," *IEEE Signal Processing Letters*, vol. 30, pp. 1762–1766, 2023, doi: 10.1109/LSP.2023.3332298.
- [17] S. Mahato, D. A. Khan, and D. K. Yadav, "A modified approach to data hiding in Microsoft Word documents by change-tracking technique," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 2, pp. 216–224, Feb. 2020, doi: 10.1016/j.jksuci.2017.08.004.
- [18] S. Mahato, D. K. Yadav, and D. A. Khan, "A novel information hiding scheme based on social networking site viewers' public comments," *Journal of Information Security and Applications*, vol. 47, pp. 275–283, Aug. 2019, doi: 10.1016/j.jisa.2019.05.013.
- [19] Z. Yang, N. Wei, J. Sheng, Y. Huang, and Y. Zhang, "TS-CNN: Text Steganalysis from Semantic Space Based on Convolutional Neural Network," *ArXiv*, Oct. 2018, Accessed: Mar. 24, 2024. [Online].

- [20] T. Fang, M. Jaggi, and K. Argyraki, "Generating Steganographic Text with LSTMs," in *Proceedings of ACL 2017, Student Research Workshop*, A. Ettinger, S. Gella, M. Labeau, C. O. Alm, M. Carpuat, and M. Dredze, Eds., Vancouver, Canada: Association for Computational Linguistics, Jul. 2017, pp. 100–106. Accessed: Mar. 24, 2024. [Online]. Available: <https://aclanthology.org/P17-3017>
- [21] J. Wen, X. Zhou, P. Zhong, and Y. Xue, "Convolutional Neural Network Based Text Steganalysis," *IEEE Signal Processing Letters*, vol. 26, no. 3, pp. 460–464, Mar. 2019, doi: 10.1109/LSP.2019.2895286.
- [22] Z. Yang, Y. Huang, and Y.-J. Zhang, "TS-CSW: text steganalysis and hidden capacity estimation based on convolutional sliding windows," *Multimed Tools Appl*, vol. 79, no. 25, pp. 18293–18316, Jul. 2020, doi: 10.1007/s11042-020-08716-w.
- [23] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. 2018.
- [24] Y. Niu, J. Wen, P. Zhong, and Y. Xue, "A Hybrid R-BILSTM-C Neural Network Based Text Steganalysis," *IEEE Signal Processing Letters*, vol. 26, no. 12, pp. 1907–1911, Dec. 2019, doi: 10.1109/LSP.2019.2953953.
- [25] "T-Lex Steganography," bitsofbinary. Accessed: Mar. 24, 2024. [Online]. Available: <https://bitsofbinary.wordpress.com/category/t-lex-steganography/>
- [26] Z.-L. Yang, X.-Q. Guo, Z.-M. Chen, Y.-F. Huang, and Y.-J. Zhang, "RNN-Stega: Linguistic Steganography Based on Recurrent Neural Networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1280–1295, May 2019, doi: 10.1109/TIFS.2018.2871746.
- [27] Z.-L. Yang, S.-Y. Zhang, Y.-T. Hu, Z.-W. Hu, and Y.-F. Huang, "VAE-Stega: Linguistic Steganography Based on Variational Auto-Encoder," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 880–895, 2021, doi: 10.1109/TIFS.2020.3023279.
- [28] J. Zou, Z. Yang, S. Zhang, S. ur Rehman, and Y. Huang, "High-Performance Linguistic Steganalysis, Capacity Estimation and Steganographic Positioning," in *Digital Forensics and Watermarking*, X. Zhao, Y.-Q. Shi, A. Piva, and H. J. Kim, Eds., Cham: Springer International Publishing, 2021, pp. 80–93. doi: 10.1007/978-3-030-69449-4_7.
- [29] H. Yang, Y. Bao, Z. Yang, S. Liu, Y. Huang, and S. Jiao, "Linguistic Steganalysis via Densely Connected LSTM with Feature Pyramid," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, in IH&MMSec '20. New York, NY, USA: Association for Computing Machinery, Jun. 2020, pp. 5–10. doi: 10.1145/3369412.3395067.
- [30] Z. Yang, K. Wang, J. Li, Y. Huang, and Y.-J. Zhang, "TS-RNN: Text Steganalysis Based on Recurrent Neural Networks," *IEEE Signal Processing Letters*, vol. 26, no. 12, pp. 1743–1747, Dec. 2019, doi: 10.1109/LSP.2019.2920452.
- [31] Y. Luo and Y. Huang, "Text Steganography with High Embedding Rate: Using Recurrent Neural Networks to Generate Chinese Classic Poetry," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, in IH&MMSec '17. New York, NY, USA: Association for Computing Machinery, Jun. 2017, pp. 99–104. doi: 10.1145/3082031.3083240.
- [32] Lo Sciuto G., Russo S., Napoli C., "A cloud-based flexible solution for psychometric tests validation, administration and evaluation.," *CEUR Workshop Proceedings*, vol. 2468, pp. 16-21.