StegaCraft – The Art of Hiding Secrets

Dr. K. Shirisha Reddy, Shreejit Cheela, Vignya Durvasula, and Sidhi Anish Kumar

Vignana Bharathi Institute of Technology, Hyderabad.

kshirishacse@vbithyd.ac.in [1],
shreejit.jithu2002@gmail.com [2],
vignyadurvasula@gmail.com [3] and
sidhi.anishkumar4064@gmail.com [4]

Abstract. StegaCraft is an integrated system preserving traditional steganographic techniques, enabling end-to-end concealment of data within carrier media. Leveraging deep learning and LSB methods, it facilitates hiding text within text, audio within audio, and image within image, while optimizing resource utilization and ensuring data authenticity.

Keywords: Steganography, Data Security, Deep learning, Text, Audio, Image, Flask-Ajax

1 Introduction

Steganography has been around in the world of history for many centuries. In earlier days, kings or nations used to hide secret information in letters and cover the message tablets with wax to hide the important information from their enemies. This method has been transformed into a technology in which secret or confidential information is being hidden in a not-so-important cover or container. In recent years, there has been a buzz around the concepts of Artificial Intelligence and Machine Learning, and there is no doubt that this technology has crept into the field of steganography. This project demonstrates the use of deep learning to hide secret information within a container media.

Existing System. While there are many techniques that perform steganography on different data sources – image, audio, video and text-hiding text message in a cover image, hiding audios in text files and so on, leveraging the deep learning techniques, there exists a lack of an end-to-end steganographic model for these data sources.

Proposed System. The proposed system is a steganographic model that performs end-to-end steganography (hiding text in text, audio in audio, images inside images,), leveraging deep learning and LSB techniques to build a separate pipeline for each of the modal and integrating them into a virtual pipeline that allows user to select the modal they want to use from image, audio and text. We aim to provide a one-stop platform for hiding any type of media (text, audio and image) in its corresponding cover input. The StegaCraft website allows the users to enter cover and secret inputs and conveniently download the encoded and decoded outputs.

Scope. This steganographic system hides text, audio, and images within their own formats, offering security in communication, digital forensics, and privacy protection. It's valuable in government, military, and business contexts for secure data exchange. It also helps protect intellectual property and enables covert communication, with potential in entertainment for enhancing user engagement. Its adaptability makes it suitable for diverse applications, ensuring robust data hiding across domains.

2 Literature Survey

In their research [1], the authors tapped into Long Short-Term Memory (LSTM) networks to perform text steganography in Arabic, showcasing the potential of deep learning techniques in strengthening steganographic security and capacity. Their findings revealed a notable 45% boost in storage capacity through LSTM-based techniques, underscoring the efficacy of deep learning, especially LSTM networks, in concealing confidential information within Arabic text. This research highlights the promising fusion of artificial intelligence and steganography, opening avenues for enhanced data security in sensitive contexts.

In paper [2], various deep learning techniques for text steganography are explored,lile LSTMs for generating text and Generative Adversarial Networks to produce stego text base on adaptive probability distributions. . Additionally, a secure generative linguistic steganographic method is proposed, leveraging Adaptive Dynamic Grouping (ADG) to recursively embed secret information. This method enhances imperceptibility by adaptively grouping tokens according to their probabilities, dynamically embedding secrets into the generated stego text. The approaches demonstrate high security and fluency in generating stego text, with the statistical coverless text steganography method showing superior anti-steganalysis ability, promising advancements in steganographic security.

In study [3], a new convolutional neural network (CNN) method is introduced to enhance audio steganalysis. It features specialized layers to capture steganographic noise, a linear unit for activating shallow layer outputs, and pooling to prevent overfitting. By comparing against four state-of-the-art techniques, including handcrafted feature-based and CNN-based methods, the proposed approach demonstrates superior performance. It notably improves detection of LSB matching and STC-based steganography, surpassing recent CNN-based methods by approximately 7% and 19%, respectively. These results highlight the efficacy of deep learning, particularly CNN, in advancing audio steganalysis across different embedding rates.

In work [4], the authors utilized Convolutional Neural Networks (CNNs) for steganography and watermarking. Their proposed architecture involves gated convolutions in three blocks for encoding, four blocks for carrier decoding, and six blocks for message decoding, each with 64 kernels of size 3x3. They fine-tuned the network parameters to minimize errors between the original and embedded carriers and messages. Human subjective experiments, measuring Word Error Rate (WER) and Character Error Rate (CER), yielded promising results, with CER/WER measured at 5.1%/2.86% for original messages and 5.15%/2.78% for reconstructed messages. Speaker recognition evaluations, both human and automatic, showed high accuracy, with the proposed system achieving an Equal Error Rate (EER) of 18% (82% accuracy) on generated messages and 15% EER (85% accuracy) on original messages. These findings indicate the model's effectiveness in maintaining message intelligibility and speaker recognition accuracy while ensuring undetectability of hidden messages by humans.

In their pioneering work [5], the authors introduce SteganoGAN, a steganographic framework utilizing a critic to evaluate steganographic image quality. They employ three encoder variants—basic, residual, and dense—to enhance hidden capacity and visual quality, achieving up to 4.4 bpp on the COCO dataset. In this paper, the applications of deep learning in image steganography to overcome limitations like restricted capacity and susceptibility are explored. The study details SteganoGAN's network structure, highlighting joint training of the encoder-decoder and critic networks, supported by a three-loss metric to balance task objectives and minimize modifications in low-frequency image regions.

Study [6] showcases SteganoCNN, a steganography model based on deep convolutional neural networks (CNNs), with a focus on enhancing steganography capacity while maintaining security. They explore three network architectures—CNN, Unet, and FCDenseNet—each addressing the limitations of traditional methods by considering the complexity of R, G, and B three-channel textures for embedding information. SteganoCNN achieves a carrier image load rate of 0.3 bits per pixel, surpassing existing models in both capacity and security. This innovative approach not only advances the current understanding of steganography but also provides opportunities for further refinement and application in diverse context.

3 Methodology

StegaCraft's architecture is designed to seamlessly integrate multiple data modalities, including text, audio, and image inputs, facilitating a comprehensive solution for concealing sensitive information. StegaCraft follows a modular design, employing a

virtual pipeline that branches into three distinct modules based on user-selected data types: Text, Audio, and Image. Upon user selection, the system navigates to the corresponding module to initiate the steganographic process tailored to the chosen data modality

3.1 Design and Architecture

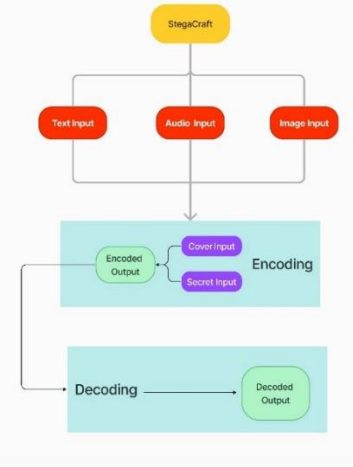

Figure 1: System Architecture

Text Module. In the Text module, StegaCraft operates on textual data, enabling users to conceal information within text-based documents or messages. The module accepts both Cover and Secret inputs, where the Cover input serves as the carrier for hiding the Secret input. StegaCraft employs sophisticated encoding techniques within this module to embed the Secret input seamlessly into the Cover input while preserving the readability and integrity of the text.

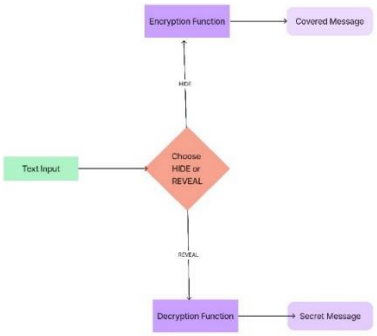

Figure 2: Model Architecture of Text Module

Audio Module. For audio data, StegaCraft leverages advanced algorithms to embed information discreetly within audio files. Upon receiving the Cover and Secret inputs, the Audio module employs specialized steganographic techniques to embed the Secret input imperceptibly into the Cover input audio file. This process ensures that the hidden information remains undetectable to human senses while maintaining the quality and authenticity of the audio.

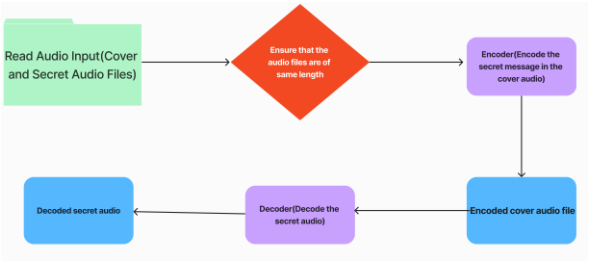

Figure 3: Model Architecture of Audio Module

Image Module. In the Image module, StegaCraft facilitates the concealment of information within digital images. By leveraging sophisticated image processing

algorithms, this module enables users to embed data seamlessly within the pixels of the Cover image. The Image module carefully integrates the Secret input into the Cover input image without perceptible alterations, ensuring that the hidden information remains effectively concealed.

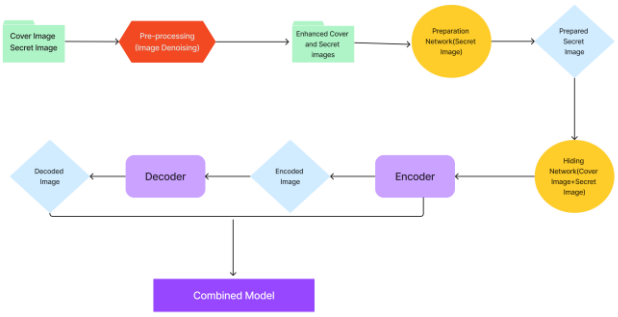

Figure 4: Model Architecture of Image Module

3.2 Implementation

The successful implementation of StegaCraft involved the fusion of advanced techniques in steganography with robust model architectures and seamless integration with web technologies. Leveraging the versatility and efficiency of Python, alongside the interactive capabilities of HTML, CSS, and JavaScript, it emerged as a end-to-end steganography approach implemented in our model represents a sophisticated solution wherein the concealment of information seamlessly integrates with the respective data modalities. This conventional steganographic process underscores its versatility and efficacy in addressing diverse concealment requirements across different data types, thereby enhancing privacy and security in digital communication.

Python serves as the backbone of StegaCraft's implementation, providing a powerful resource equipped with rich ecosystem of libraries and frameworks for the development of steganographic algorithms and model architectures.

The HTML interface provided establishes a user-friendly platform titled "StegaCraft" aimed at concealing and managing various types of data. Visually, it employs a gradient background and balanced alignment for an aesthetic appeal. The interface comprises three distinct options encapsulated within stylish containers, each representing a data type: text, speech, and image. They are adorned with corresponding icons and labels, facilitating intuitive navigation for users. Upon selection, each option redirects users to specific functionalities. Facilitating the integration between frontend and backend, StegaCraft leverages Flask and AJAX, to enhance user experience by enabling asynchronous data exchange between the client and server.

Text Steganography. The heart of text integration lies in the text_hide() function. This function acts as a hub for handling HTTP POST requests and receives input data in JSON format. This script for Text Steganography is a straightforward encryption and decryption tool designed to work with strings.

It defines two key functions:

- first_replace_words(input_str): This function takes a string as input and encrypts it by replacing each word in the string with its corresponding value from the dictionary. If a word is absent in the dictionary, it is unchanged.
- revert_words(input_str): This function decrypts previously encrypted string by replacing each word with its corresponding key in dictionary. Just like the prior function, if a word isn't in the dictionary, it remains unchanged.

By avoiding the duplication of existing text-based encryption techniques, we've been able to devote our efforts to exploring innovative pathways within audio and image concealment methods. This strategic approach has allowed us to push the boundaries of the field by presenting novel solutions instead of replicating established practices.

Audio Steganography. Leveraged the Least Significant Bit (LSB) Manipulation to discreetly hide secret audio signals within other audio signals. The idea behind this method is that by altering only the least significant bits of audio data, the changes are typically imperceptible to the human ear. The underlying principle involves the secret message, in this case, an audio signal, is combined with the cover audio, each sample of the cover audio is subtly adjusted to include part of the secret message. This is done by replacing the least significant bits of the cover audio samples with the most significant bits from the secret audio samples. This ensures that the cover audio still sounds normal, maintaining the secrecy of the hidden message. It's crucial to recognize that although the encoded audio appears as clear as the original audio and is imperceptible to the human ear, the decoded audio typically exhibits more noise due to extraction from the encoded version. Despite this, the message hidden within the encoded audio remains audible after decoding.

Image Steganography. This module has a pipeline for hiding a 64x64 secret image in a 64x64 cover image with 3 color channels. Firstly, all the images are processed such that any noise in the images is alleviated. We used the OpenCV library's fastNlMeansDenoisingColored technique to perform denoising. The denoised cover and secret images are split into train and validation sets and a function is used to generate data for the model. The model architecture is inspired by [12] has three important components – preparation network, hiding network and reveal network. The encoder acts as a wrapper for preparation and hiding networks. Similarly, decoder wraps the reveal network. The model architecture is essentially a Convolutional Neural Network (CNN). The preparation network has five convolutional layers and one up-sampling layer, while the hiding and reveal networks have 18 convolutional layers each. Popular state-of-the-art datasets like ImageNet and CIFAR-10 have been used for training and testing. After the model is successfully built, we have also used the model on resized HD images, where the model has been found to perform well.

4 Results

Figure 5: Homepage

Figure 6: Text Module, before interaction

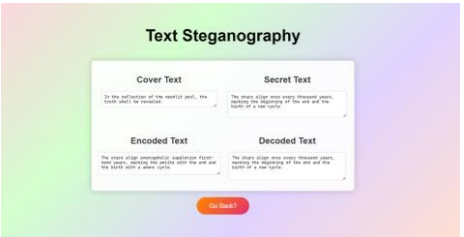

Figure 7: Text Module, after interaction

Figure 8: Audio Module, before interaction

Figure 9: Audio Module, after interaction

Figure 10: Image Module, before interaction

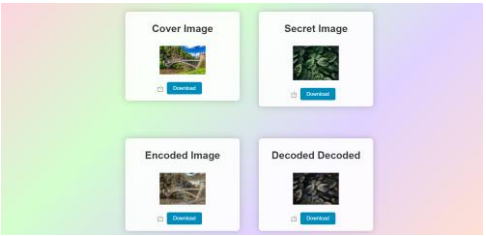

Figure 11: Image Module, after interaction

References

1 Adeeb, Omer & Kabudian, Seyed. (2022). Arabic Text Steganography Based on Deep Learning Methods. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3201019

2 Majeed, M.A.; Sulaiman, R.; Shukur, Z.; Hasan, M.K. A Review on Text Steganography Techniques. Mathematics 2021, 9, 2829. https://doi.org/10.3390/math9212829

3 Lin, Yuzhen & Wang, Rangding & Yan, Diqun & Dong, Li & Zhang, Xueyuan. (2019). Audio Steganalysis with Improved Convolutional Neural Network. 210-215. 10.1145/3335203.3335736

4 Kreuk, Felix & Adi, Yossi & Raj, Bhiksha & Singh, Rita & Keshet, Joseph. (2019). Hide and Speak: Deep Neural Networks for Speech Steganography

5 Zhang, S.; Li, H.; Li, L.; Lu, J.; Zuo, Z. A High-Capacity Steganography Algorithm Based on Adaptive Frequency Channel Attention Networks. Sensors 2022, 22, 7844. https://doi.org/10.3390/s22207844

6 Duan, X.; Liu, N.; Gou, M.; Wang, W.; Qin, C. SteganoCNN: Image Steganography with Generalization Ability Based on Convolutional Neural Network. Entropy 2020, 22, 1140. https://doi.org/10.3390/e22101140

7 Baluja, Shumeet. "Hiding Images in Plain Sight: Deep Steganography." Neural Information Processing Systems (2017)

8 Balgurgi, P.P., Jagtap, S.K. (2013). Audio Steganography Used for Secure Data Transmission. In: Kumar M., A., R., S., Kumar, T. (eds) Proceedings of International Conference on Advances in Computing. Advances in Intelligent Systems and Computing, vol 174. Springer, New Delhi. https://doi.org/10.1007/978-81-322-0740-5_83

9 Hamdan, A. M., and Hamarsheh, A. (2016) AH4S: an algorithm of text in text steganography using the structure of omega network. Security Comm. Networks, 9: 6004–6016. doi: 10.1002/sec.1752

10 Dutta, Hrishikesh & Das, Rohan & Nandi, Sukumar & Prasanna, S.. (2019). An Overview of Digital Audio Steganography. IETE Technical Review. 37. 1-19. 10.1080/02564602.2019.1699454

11 Tanwar, Rohit & Bisla, Monika. (2014). Audio steganography. ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology. 322-325. 10.1109/ICROIT.2014.6798347

12 https://github.com/MaddulaPrakash/image-steganography-using-deep-learning/tree/main

13 https://github.com/harveyslash/Deep-Steganography

14 https://github.com/ktekeli/audio-steganography-algorithms