Adaptive Practical Effective Image Steganography using Convolutional Encoder-Decoder Network

Mrs. S.Lakshmi

*Department of Computer Science and Engineering*

*SRM Institute of Science and Technology, Ramapuram* Chennai, India lakshmis9@srmist.edu.in

Kunal Sugandhi

*Department of Computer Science and Engineering*

*SRM Institute of Science and Technology, Ramapuram* Chennai, India kp9067@srmist.edu.in

Chandarshekar Readdy

*Department of Computer Science and Engineering*

*SRM Institute of Science and Technology, Ramapuram* Chennai, India mm8755@srmist.edu.in

Akash Nagaria

*Department of Computer Science and Engineering*

*SRM Institute of Science and Technology, Ramapuram* Chennai, India aa3646@srmist.edu.in

***Abstract*—** Steganography is the practice of concealing information within digital media to maintain privacy and secure communication. In this paper, we present an adaptive, practical, and effective approach to image steganography using a Convolutional Encoder-Decoder Network (CED-Net). Our deep learning-based model is designed to embed and extract secret information from digital images while preserving high visual quality and robustness. The encoder learns spatial dependencies to imperceptibly embed the secret image into a cover image, while the decoder reconstructs the hidden image from the stego image with high fidelity. Our system balances payload capacity, imperceptibility, and resistance to steganalysis. Extensive experiments demonstrate that our model outperforms traditional and contemporary methods in terms of Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and recovery accuracy. This work establishes a scalable, efficient, and interpretable framework for real-world secure image communication.

**Keywords—** Steganography, Convolutional Neural Network, Encoder-Decoder, Image Security, Deep Learning

1. **Introduction**

With the increasing reliance on digital communication, securing sensitive information has become a critical requirement in many domains, including defense, healthcare, and personal privacy. Traditional encryption methods provide confidentiality but often fail to hide the very existence of a message, making them susceptible to detection and analysis. Steganography addresses this limitation by embedding secret information into innocuous cover objects, such as images, audio, or video files.

Digital image steganography has gained prominence due to the wide usage and redundancy present in image data. However, classical methods like Least Significant Bit (LSB) substitution or Discrete Cosine Transform (DCT)-based embedding often suffer from limited payload capacity, low resistance to detection, and perceptible image degradation.

Recent advancements in deep learning have revolutionized various computer vision tasks. Convolutional Neural Networks (CNNs) in particular have demonstrated excellent capabilities in learning hierarchical representations of images. In this context, we propose a Convolutional Encoder-Decoder Network (CED-Net) for image steganography, which uses deep learning to perform adaptive and effective hiding and recovery of secret images.

Our approach includes:

1. A novel encoder-decoder architecture designed for end-to-end image hiding and reconstruction.
2. A multi-objective loss function that optimizes for minimal distortion and high-fidelity reconstruction.
3. Robustness against transformations such as compression and noise.
4. Practical applicability through efficient design and ease of deployment.

The proposed method offers a compelling solution for embedding large amounts of information in cover images without compromising visual quality, making it suitable for secure and covert communications.

1. **RELATED WORK**

Numerous methods have been proposed for image steganography. These can be broadly categorized into traditional techniques and deep learning-based approaches.

**A. Traditional Techniques**
Classical image steganography techniques such as LSB substitution involve embedding bits of the secret message into the least significant bits of the pixel values of the cover image. Although simple, these methods are vulnerable to noise and steganalysis.

Transform domain methods, including DCT and Discrete Wavelet Transform (DWT), improve robustness by embedding information in the frequency domain. However, they still suffer from limited embedding capacity and poor visual quality at higher payloads.

**B. Deep Learning-Based Approaches**
Baluja (2017) introduced a CNN-based model that embeds one image within another. The approach demonstrated the ability of deep networks to perform end-to-end image hiding. Zhu et al. (2018) proposed HiDDeN, an adversarially trained network that embeds messages into images and is robust against distortions. Their model, however, requires significant computational resources.

Tan and Pei (2019) developed StegNet using a U-Net-based encoder-decoder structure, improving image quality and recovery rate. However, the model struggled with scalability for high-resolution inputs.

Wu et al. (2018) proposed a residual CNN approach emphasizing adaptiveness to resist steganalysis. While effective, their model lacks generalizability across diverse image types.

Our work builds on these methods by introducing a balanced model that is both lightweight and effective, achieving a trade-off between imperceptibility, robustness, and computational efficiency.

1. **METHODOLOGY**

The proposed CED-Net architecture consists of an Encoder for hiding the secret image and a Decoder for reconstructing it from the stego image. The model is trained end-to-end with a custom loss function.

**A. Architecture Design**
The Encoder comprises multiple convolutional layers with ReLU activation functions. Both the cover and secret images are processed in parallel feature extraction pipelines. These are merged through concatenation and passed through additional convolutional layers to generate the stego image.

The Decoder mirrors the Encoder structure using transposed convolutions and upsampling layers to reconstruct the secret image from the stego image. Skip connections are employed to retain low-level features and improve detail preservation.

**B. Data Preparation**
We used publicly available image datasets like CIFAR-10 and ImageNet subsets for training. All images were resized to 256×256 and normalized. Training data consisted of pairs of cover and secret images, selected randomly to encourage generalization.

**C. Loss Function**
The objective function used during training is a weighted sum of two Mean Squared Error (MSE) losses:

* Embedding Loss: MSE between the cover and stego images.
* Reconstruction Loss: MSE between the secret and decoded images.

Total Loss = α \* Embedding Loss + β \* Reconstruction Loss, where α and β are hyperparameters balancing visual quality and accuracy.

**D. Training Details**
The model was implemented in TensorFlow and trained on an NVIDIA RTX GPU. Training used the Adam optimizer with a learning rate of 0.001 and batch size of 16. Early stopping based on validation loss ensured optimal generalization.

1. **Proposed Architecture**

**

Fig. 1. BLOCK DIAGRAM OF THE PROPOSED SYSTEM

1. **RESULTS AND DISCUSSION**

We evaluate our model using metrics such as PSNR, SSIM, payload capacity (bits per pixel), and recovery accuracy.

|  |  |
| --- | --- |
| **Metric** | **Value** |
| PSNR (Stego-Cover) | 40.27 dB |
| SSIM | 0.981 |
| Payload Capacity | 1 bpp |
| Recovery Accuracy | 98.6% |

Our model significantly outperforms traditional methods, which typically yield PSNR values below 35 dB. The SSIM score of 0.981 indicates high structural similarity between the cover and stego images. The Decoder achieves a recovery accuracy of 98.6%, effectively reconstructing the hidden image.

Visual inspection confirms that the stego images are nearly indistinguishable from their original counterparts. Additionally, robustness tests involving JPEG compression and Gaussian noise show minimal degradation in reconstruction quality.

Compared to recent deep learning-based models, our approach provides a better trade-off between accuracy and computational cost. It generalizes well across different image types and resolutions.

1. **CONCLUSION**

In this paper, we presented an adaptive and practical image steganography method using a Convolutional Encoder-Decoder Network. Our approach achieves high payload capacity, visual imperceptibility, and reconstruction accuracy, making it suitable for real-world applications in secure image communication.

The model balances complexity and performance, offering an interpretable and scalable solution. Future work can explore integration with adversarial training for further robustness, deployment on edge devices through model pruning or quantization, and extension to video steganography or multimodal hiding.

1. **References**
* Baluja, S. (2017). "Hiding Images within Images". arXiv preprint arXiv:1703.00371
* Zhu, J. et al. (2018). "HiDDeN: Hiding Data with Deep Networks". ECCV
* Tan, C., & Pei, Z. (2019). "StegNet: Mega Image Steganography Capacity with Deep Convolutional Network". arXiv:1901.03892
* Wu, H., et al. (2018). "A Novel Convolutional Neural Network Approach for Steganography". IEEE Access.
* Fridrich, J., & Kodovsky, J. (2012). "Rich Models for Steganalysis of Digital Images". IEEE Transactions on Information Forensics and Security
* Qian, Y., Dong, J., & Tan, T. (2015). "Deep Learning for Steganalysis via Convolutional Neural Networks". Media Watermarking, Security, and Forensics.