Camouflage: A Deep Steganography Framework for Hiding Images in Plain Sight

Team members :

Name	Roll number
Anuvind M P	AM.EN.U4AIE22010
R S Harish Kumar	AM.EN.U4AIE22042

Abstract

This project, "Camouflage," leverages advanced deep learning techniques to embed secret images seamlessly within ordinary host images, creating a powerful steganography framework. Steganography is the technique of covering secret data within a regular, non-secret, file or message in order to avoid detection. Camouflage ensures that concealed images are embedded and can later be accurately extracted with minimal degradation, even under scrutiny or compression. This approach achieves high fidelity and robustness, allowing secure, covert communication and digital watermarking across a range of sensitive applications. Camouflage transforms traditional steganography, making data invisibility as intuitive and reliable as data encryption.

Problem Statement

In today's digital landscape, where secure communication and data integrity are increasingly critical, traditional steganography methods often fail to provide adequate security, embedding capacity, and resilience against image transformations like compression or resizing. Our project addresses this challenge by leveraging deep learning to develop a robust framework for invisibly embedding high-fidelity images within host images, preserving perceptual quality while ensuring the concealed data remains undetectable and accurately retrievable. This project offers a powerful solution for secure data transmission, digital watermarking, and anti-tampering applications, making it possible to achieve invisible data embedding with resilience and security in a wide range of sensitive fields.

Background

Steganography has become increasingly important in today's digital world, where data privacy and security are crucial. As cyber threats rise and surveillance expands, the need for hidden communication methods has grown. Unlike encryption making it valuable for journalists, businesses, military operations, and artists who need to share sensitive data discreetly or protect intellectual property with hidden watermarks.

With the increase of digital media, effective steganographic techniques must embed data within images, audio, or video files without affecting their quality. The advancement of deep learning technologies offers exciting possibilities for improving steganography, positioning it as a key tool for ensuring secure communications and protecting privacy in an interconnected world.

Datasets

We are considering COCO and CIFAR-10/100 datasets for diverse and robust model training in deep steganography.

1. COCO (Common Objects in Context) https://cocodataset.org/ :
   Large-scale dataset with over 330,000 images covering 80 object categories and various complex scenes. It provides high-resolution images with detailed annotations, making it ideal for testing steganography across diverse backgrounds and settings.

2. CIFAR-10 & CIFAR-100 https://www.kaggle.com/c/cifar-10 :
   Small-scale datasets of 32x32 pixel images, each containing 60,000 images. CIFAR-10 includes 10 object categories, while CIFAR-100 covers 100 categories. Their small size makes them ideal for quick prototyping and evaluating how well steganographic techniques handle basic image structures.

Deliverable Objectives

1. Develop a deep learning-based steganography model capable of embedding images within other images while preserving visual quality.
2. Ensure accurate recovery of hidden images with minimal degradation, even after transformations like compression or resizing.
3. Deliver comprehensive documentation, including code, usage guidelines, and performance evaluation metrics for reproducibility and usability.

Models and Tools

1. TensorFlow or PyTorch
2. OpenCV
3. Matplotlib or Seaborn
4. CNN
5. Generative Adversarial Networks (GANs)
6. Autoencoders