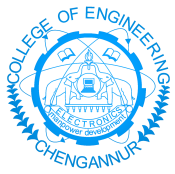
Deep Steganography: Hiding Images within Images

03CS6902 Mini Project

CHN20CSIP07 Sree Lekshmi B S
sreelekshmibs16@gmail.com
M. Tech. Computer Science & Engineering (Image Processing)



Department of Computer Engineering
College of Engineering Chengannur
Alappuzha 689121
Phone: +91.479.2165706
http://www.ceconline.edu
hod.cse@ceconline.edu

College of Engineering Chengannur
Department of Computer Engineering

C E R T I F I C A T E

This is to certify that, this report titled ***Deep Steganography: Hiding Images within Images*** is a bonafide record of the work done by

CHN20CSIP07 Sree Lekshmi B S

Second Semester M. Tech. Computer Science & Engineering (Image Processing)

student, for the course work in **03CS6902 Mini Project**, under our guidance and supervision, in partial fulfillment of the requirements for the award of the degree, M. Tech. Computer Science & Engineering (Image Processing) of **APJ Abdul Kalam Technological University**.

Guide

Syama S
Asst. Professor
in Computer Engineering

Coordinator

Ahammed Siraj K K
Associate Professor
in Computer Engineering

Head of the Department

October 6, 2021

Dr. Smitha Dharan
Professor
in Computer Engineering

Permission to Use

In presenting this mini project dissertation at College of Engineering Chengannur(CEC) in partial fulfillment of the requirements for a Postgraduate degree from APJ Abdul Kalam Technological University, I agree that the libraries of CEC may make it freely available for inspection through any form of media. I further agree that permission for copying of this dissertation in any manner, in whole or in part, for scholarly purposes may be granted by the Head of the Department of Computer Engineering. It is understood that any copying or publication or use of this dissertation or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to CEC in any scholarly use which may be made of any material in this mini project dissertation.

Sree Lekshmi B S.

Statement of Authenticity

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at College of Engineering Chengannur(CEC) or any other educational institution, except where due acknowledgement is made in the report. Any contribution made to my work by others, with whom I have worked at CEC or elsewhere, is explicitly acknowledged in the report. I also declare that the intellectual content of this report is the product of my own work done as per the **Problem Statement** and **Proposed Solution** sections of the mini project dissertation report. I have explicitly stated the major references of my work. I have also listed all the documents referred, to the best of my knowledge.

Sree Lekshmi B S.

Acknowledgements

Firstly, I thank God Almighty for being my guide light throughout the project and helping in completing it within the stipulated time.

I express my grateful thanks, to Dr. Jacob Thomas V., Principal, College of Engineering Chengannur for extending all the facilities required for doing my mini project. My deepest sense of gratitude to the head of the department, Dr. Smitha Dharan, Professor and Head of the department of Computer Science and Engineering, for providing constant support.

I express my heartfelt gratitude to my Project Co-ordinator Mr. Ahammed Siraj K K, Associate Professor in Computer Engineering and project guide Mrs. Syams S, Assistant Professor in Computer Engineering for their timely suggestions and encouragement given for the successful completion of the project work. I would always oblige for the helping hands of all other staff members of the department who directly or indirectly contributed in this venture.

Abstract

This project is an attempt to hide a full color image inside another of the same size with minimal quality loss to either image. For that deep neural networks are simultaneously trained to create the hiding and revealing processes. The full system is a series of three networks that are trained as a single large network. The system is trained on images drawn randomly from the ImageNet database and works well on natural images from a wide variety of sources. The challenge of good information hiding arises because embedding a message can alter the appearance and underlying statistics of the carrier. This work also attempt to maintain quality of images. With this work, not only the hidden information be kept secure, but the system can be used to hide even more than a single image. Unlike many popular steganographic methods that encode the secret message within the least significant bits of the carrier image, this approach compresses and distributes the secret image's representation across all of the available bits.

Contents

Chapter 1

Introduction

Steganography is an art and science of hiding secret message into cover medium. In steganography, secret message is embedded in an appropriate carrier object that may be image, video, sound or other file. The main objectives for any steganography algorithm are capacity, undetectibility and robustness.

There are many techniques to embedd data in a carrier. Information hiding is most commonly associated with secretly planning and coordinating criminal activities through hidden messages in images posted on public sites. Beyond the multitude of misuses, hiding information can be used for practical positive applications. For example, hidden images used as watermarks embed authorship and copyright information without visually distorting the image. Cryptography and steganography are main methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable or hides the meaning of the data while steganography hides the existence of the data. Steganography often use cover images to hide data.

1.1 Proposed Project

This project presents an efficient system to hide a full color image within another of same size. This work aims to hide an image without altering the appearance of cover image. It is implemented by deep neural networks which are simultaneously trained to create the hiding and revealing processes and are designed to specifically work as a pair.

1.1.1 Problem Statement

This project aims to hide large amount of information within a cover image without losing the quality of both. Also the amount of information hidden will not alter the appearance and underlying statistics of cover image.

1.1.2 Proposed Solution

For effective and efficient embedding of hidden image's information into host image it employs a series of three deep neural networks namely Preparation network, Hiding Network and Revealing Network. These network determines where to place the hidden information as well as how to compress and represent it. The entire system is divided into two phases ie the encoder and decoder phase. The encoder phase hides the secret images within a cover image using steganographic

technigues such as LSB manipulation, noise manipulation and color bit manipulation. The hidden image is dispersed throughout the bits in surrounding pixels and across all the color channels. A decoder phase that has been simultaneously trained with the encoder is used to reveal the hidden image. The Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) are used to quantify image quality degradation between the original and reconstructed images.

Chapter 2

Report of Preparatory Work

2.1 Literature Survey Report

1. **Block-Based High Capacity Multilevel Image Steganography**, [2], Journal of Circuits, Systems, and Computers Vol. 25, No. 8 , Oct. 2016, 1650091 (21 pages).

   This paper proposes a block-based high capacity steganography technique for digital images. The cover image is decomposed into blocks of equal size and the largest pixel of each block is found to embed the secret data bits and also the smallest pixel of each block is used for embedding to enhance the capacity. Embedding of secret data is performed using the concept that the pixel of a cover image has only two states even and odd. Multilevel approach is also combined in the proposed technique to achieve high embedding capacity. In order to make the proposed technique more secure, a key is generated using embedding levels, block size, pixel embedding way, encryption parameters, and starting blocks of each embedding levels. Embedding capacity and visual quality of stego images generated by the proposed steganography technique are higher than the existing techniques. Steganalysis tests have been performed to show the un-detectability and imperceptibility of the proposed technique. This does not guarantees hiding of large amount of data. This method is not performed in colour images.

2. **Colour Image Steganography using SHA-512 and Lossless compression** , [1], International Journal of Imaging and Robotics, vol. 18, July 2018.

   This paper introduces a colour image steganography that enhances the existing LSB substitution techniques. This method improve the security level of hidden information and increase embedding capacity of hidden-data. Lossless image compression technique are utilized to compress secret information and Hash-function is used to hash the hidden information. Hash function is used to map the data with limited size to a value of certain length. Hash-function will be executed in the stego image and its values will be stored in the host image for further checking during extraction process. This method demonstrates significantly improvement in terms of information security, embedding capacity and quality.

3. **Secure RGB Image Steganography based on Fused Distortion Measurement**, [**?**], International Journal of Research in Engineering, Science and Management, vol 2, Mar. 2019.

   This work aims to generate stego images with good visual quality and statistical security of anti-steganalysis. They introduces a new stegnographic scheme ie a fused distortion measurement is developed to better measure the distortions brought by flipping pixels. The flipping position optimization is designed to find better flipping positions for flipping pixels to embed secret messages. For constructing a distortion measurement to better measure the distortions brought by flipping pixels, they combine the merits of the flipping distortion measurement (FDM) and two data-carrying pixel location methods (including the edge adaptive grid method (EAG)and the "Connectivity Preserving" criterion (CPc) to design a fused distortion measurement. FDM focuses on the statistical security and measure the distortion scores by statistical characters, while EAG and CPc focus on the visual quality and select flippable pixels by local structured features.

4. **Practical steganalysis of digital images: State of the art** [**?**]. in Proc. Electron. Imaging, 2002, pp. 1–13

   Here classifies and reviewed current stego-detection algorithms that can be used to trace popular steganographic products. They recognize several qualitatively different approaches to practical steganalysis visual detection, detection based on first order statistics (histogram analysis), dual statistics methods that use spatial correlations in images and higher-order statistics (RS steganalysis), universal blind detection schemes, and special cases, such as JPEG compatibility steganalysis.They also present some new results regarding detection of LSB embedding using sensitive dual statistics. The recent steganalytic methods indicate that the most common paradigm in image steganography ie the bit-replacement or bit substitution is inherently insecure with "safe capacities" far smaller than previously thought.

5. **"Hiding an Image inside another Image using Variable-Rate Steganography"** ,[7], in Proc. ACM Int. Conf. Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 10, pp. 18–21, 2013.

   Here presents a new algorithm for hiding a secret image in the least significant bits of a cover image. The images used in this study are color or grayscale images. The number of bits used for hiding changes according to pixel neighborhood information of the cover image. The exclusive-or (XOR) of a pixel's neighbors is used to determine the smoothness of the neighborhood. A higher XOR value indicates less smoothness and leads to using more bits for hiding without causing noticeable degradation to the cover image. Experimental results are presented to show that the algorithm generally hides images without significant changes to the cover image, where the results are sensitive to the smoothness of the cover image.

6. **Deep learning for steganalysis via convolutional neural networks** [4], in Proc. Media Water Marking, security and forensics , Vol 9404, 2015, pp. 161–177.

   This paper proposes a new paradigm for steganalysis to learn features automatically via deep learning models. They propose a customized Convolutional Neural Network for steganalysis. The proposed model can capture the complex dependencies that are useful for steganalysis. Compared with existing schemes, this model can automatically learn feature representations with several convolutional layers. The feature extraction and classification steps are unified under a single architecture, which means the guidance of classification can be used during the feature extraction step. They demonstrate the effectiveness of the proposed model on three state-of-theart spatial domain steganographic algorithms - HUGO, WOW, and S-UNIWARD. Compared to the Spatial Rich Model (SRM), our model achieves comparable performance on BOSSbase and the realistic and large ImageNet database.

2.2 System Study Report

The primary focus of this project is to demonstrate that it is possible to encode a large amount of information in an image with limited visually noticeable artifacts with minimum distortions to cover image. The entire system is a series of three networks which are simultaneously trained. This system reconstructs the image with minimum quality loss and less distortion to the cover image. Tools exist to seek out hidden information in the LSBs. One such publicly available steganalysis toolkit, StegExpose was used to test the detectability of our hidden images. The dataset is prepared from tiny ImageNet dataset. The images used in the study are composed, at each pixel, of 24 bits ($8 \times$ (R,G,B)). If we flip the first bit of the R channel of all the pixels in the container image, we can measure its effects on the reconstructions on the container image itself and also, by propagating the modified image through reveal network on the reconstruction of the secret image.

Chapter 3

Project Design

3.1 Project Design

The goal of this project is to visually hide a full N × N RGB pixel secret image in another N ×N RGB cover image with minimal distortion to the cover image. Though steganography is often conflated with cryptography, in our approach the closest analogue is image compression through auto-encoding networks. The trained system must learn to compress the information from the secret image into the least noticeable portions of the cover image[**?**]. The architecture of the proposed system is shown in Figure 3.1. The three components in the systems are Preparation Network, Hiding Network and Revealing network and are trained as a single network.

Preparation-Network

The first component is the Preparation-Network that prepares the image to be hidden. The main function of this network is to transform the RGB-pixels of the hidden image into features that can be used by the Hiding-Network.

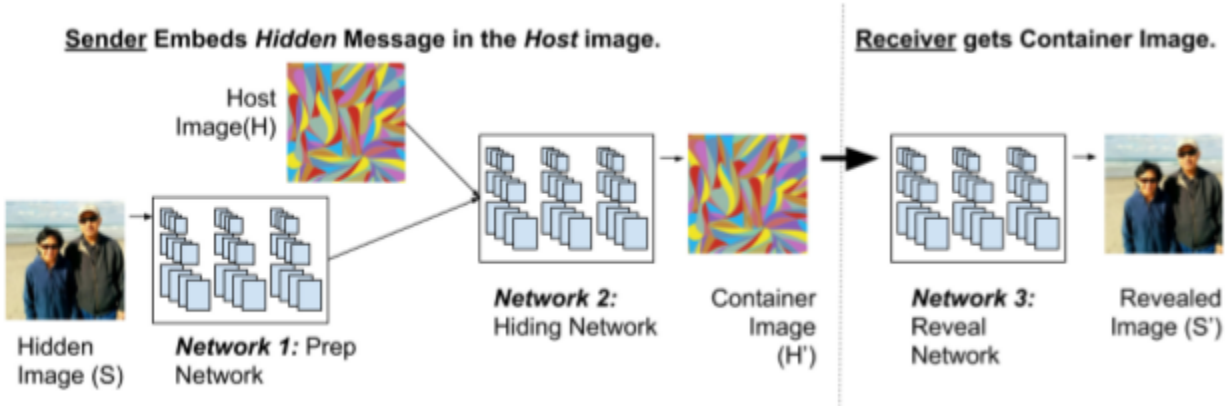


Figure 3.1: Architecture of proposed system

Hiding Network

The second and main component is the Hiding Network. The Hiding-Network receives the output of the Preparation-Network and the host image as input. The input is formatted as an$N \times N$ pixel field with depth concatenated RGB channels of the host image and the transformed channels of the hidden image. The output of this network is the Container image ($N \times N$, RGB pixels). The container image should appear as similar to the host as possible, while also containing enough information to recreate the hidden image.

Revealing Network

The third component is the Reveal-Network that is responsible for extracting the hidden image from the container. Though this network is used only by the receiver all three components are trained as a single network.

The system is trained by reducing the error shown below (H and S are the cover and secret images respectively, and is how to weighting their reconstruction errors):

$$\epsilon(H, H', S, S') = ||H - H'|| + \beta||S - S'||$$

By propagating this error signal to both the Preparation and Hiding networks the representations formed early in the system encode information about the hidden image.

Our aim is to encode a large amount of information into limited visually noticeable artifacts. The images used in the study are composed at each pixel of 24 bits (8 $\times$ (R,G,B)). We flip the first bit of the R channel of all the pixels in the container image, we can measure its effects on the reconstructions on the container image itself and also by propagating the modified image through reveal network on the reconstruction of the secret image. We can see that a bit flip in any bit position in any color channel of the container image has an effect across all color channels in the hidden image's reconstruction[**?**]. The information for the hidden image is spread across the color channels, the reason it was not detected by simply looking at the LSB. In addition to distributing the hidden image information across the color-bits the information is also spread in the spatial dimension.

So the representation for the hidden image is distributed both in surrounding pixels and in color bits. The encoding for each pixel of the hidden image is distributed in pixels that are up to a distance of 7 away from the corresponding pixel in the container image. Second, the amount of spatial distribution is directly related to the neural network architecture and the size of the convolutions.

To ensure that the networks do not simply encode the secret image in the LSBs, a small amount of noise is added to the output of the second network during training. The noise was designed such that the LSB was occasionally flipped; this ensured that the LSB was not the sole container of the secret image's reconstruction.

3.2 Hardware & Software Requirements

Dataset	: Tiny ImageNet dataset
Operating System	: Any Operating System
Supporting software	: Python(google collab)
Processor	: Intel Core i5 11th Gen 4.50GHz, 6GB GPU
RAM	: 16GB
Monitor	: Any colour monitor

Chapter 4

Implementation

4.1 CNN Creation

The full system in the project is a combination of two phases. They are encoder phase and decoder phase. In the encoder phase the sender need to embed the message into the image and send it to the receiver. The receiver which is the decoder phase needs to extract the secret message by extracting it from the stego image. Although the revealing network is in receiver side the sysytem is trained as a pair. To make sure that the quality of image is good PSNR value is calculated. These 2 phases consists of three CNN networks Preparation Network, Hiding Network and Revealing Network. Prep network uses 2 layers of 65 filters [50 3x3 filters, 10 4x4 filters and 5 5x5 filters]. Hiding network and Revealing network uses 5 layers of 65 filters[50 3x3filters,10 4x4 filters and 5 5x5 filters]. All Conv 2D layers are followed by ReLU activation. The three networks are trained simultaneously.

4.2 Training

The data set used is Tiny ImageNet dataset which contain 200 classes of 64×64 sized RGB images. The training set is divided into sets for secret and cover images. The input images are converted into matrices of matrices format. The secret message is encoded in LSB bits and distributed around surrounding pixels. Gaussian noise is added to the cover. This allows the hidden information to be encoded in bits other than the LSB of the cover image. At the receiver side a container image is obtained. The reveal network extracts the hidden features and reconsruct the secret image. Keras and tensorflow packages are used to build the three network The system has been trained for 300 epochs with a batch size of 256 and an additional 400 epochs with a batch size of 32 by reducing the error shown below.

$$\epsilon(H, H', S, S') = ||H - H'|| + \beta||S - S'||$$

The peak signal to noise ratio gets increased on every 2 epochs which quantifies the quality of encoded and decoded images.

Figure 4.1: Sample images for training

Figure 4.2: Training the model

Chapter 5

Results & Conclusions

The model can be tested by giving one secret and one cover image. The image is represented as matrices. The values extracted from secret image is embedded into the cover image using color bit manipulation, Gaussian manipulation and LSB manipulation techniques. The encoded image is passed to the decoder phase that will reveal the decoded secret image. The resulting encoded and decoded images retains their original quality.

5.1 Conclusion

In this project a model is developed that will hide an image with another of same size without losing the quality of either of the encoded and decoded images. Results shows that the developed model is an efficient and effective model for hiding an revealing purpose in steganography. The security of the system is ensured by performing Gaussian noise manipulation and LSB manipulation steganographic techniques. Since the full system is trained as a pair the encoder reconstructs the image by extracting the embedded features from cover image. The encoded and decoded images are normalized. The PSNR value indicates the quality of images that found to be good in this model.

Figure 5.1: Result

References

[1] Shumeet Baluj: Hiding Images within Images, IEEE Transactions on Pttern Analysis and Machine Intelligence, 2020

[2] Geeta Kasana, Kulbir Singh, Satvinder Singh Bhatia :Block-Based High Capacity Multilevel Image Steganography : New Delhi, 2016

[3] Ke-Huey Ng, Siau-Chuin Liew, Ferda Ernawan: Colour Image Steganography using SHA-512 and Lossless compression & associates, CA, USA, 2000

[4] A. Antony Raj , M. Vickraman , A. Vishnu , M. R. Mahalakshmi : Secure RGB Image Steganography based on Fused Distortion Measurement : International Journal of Research in Engineering, Science and Management Volume-2, Issue-3, March-2019

[5] http://www.netlib.org/pvm3/: Practical steganalysis of digital images: State of the art: in Proc. Electron. Imaging, 2002, pp. 1–13

[6] Ke-Huey Ng, Siau-Chuin Liew, Ferda Ernawan: Deep learning for steganalysis via convolutional neural networks & associates, in Proc. Media Water Marking, security and forensics , Vol 9404, 2015, pp. 161–177. CA, USA, 2000

[7] Sumeet Kaur, Savina Bansal, R. K. Bansal : Steganography and Classification of Image Steganography Techniques , in Proc. Media Water Marking, security and forensics , Vol 9404, 2015, pp. 161–177. CA, USA, 2000