Image Steganography

Yendluri Lohith JayaSurya , Yendluri Priya Yasaswini , Somepalli Saranya

Abstract*: Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography is that the intended secret message does not attract attention to itself as an object of scrutiny. Steganography is concerned both with concealing the fact that a secret message is being sent and its contents. The change is so subtle that someone who is not specially looking for it is unlikely to notice the change. We intend to perform image steganography by designing a neural network that prepares the secret jpg image and hides the prepared jpg image in a cover jpg image.

***Keywords* : steganography , neural network , jpg image**

I. INTRODUCTION

JPEG steganography embeds data into quantized Discrete Cosine Transform coefficients of JPEG images. Existing methods include JSteg,JPHide and F5 steganography techniques. JSteg embeds information into the image by successively replacing the LSB of non zero quantized DCT coecients with secret message bits.JPHide is similar to JSteg but uses a pseudo-random generator controlled by a key to select the coecients to hide the message bits. In F5 steganographic method, instead of simply replacing the lsb of selected DCT coefficients, the absolute value of the DCT is rst decreased by 1 if needed to be modified. In all these methods, selection of the DCT coefficients is done with the help of some functions and this makes it easier to decipher which pixels have actually been changed. We intend to design a neural network which learns the pattern to hide a secret image within a cover image such that the loss of information between the original secret message and revealed secret message is minimized. Current methods which implement Image Steganography are not secure. By replacing bits of cover image with bits of secret image using pre-defined techniques, it becomes easier for an outsider to find out if a cover image has been modified and also reveal the secret image by backtracking i.e. by reversing the transformation. By using Convolutional Neural Network to learn the patterns of hiding secret image within cover image, it is made sure that the learning is unique to the training set, thereby reducing the chances of a successful attempt of revealing the secret image hidden within the cover image.

Revised Manuscript Received on September 25, 2020.

***** Correspondence Author

Yendluri Lohith Jayasurya, Computer Science and engineering, Amrita Vishwa vidyapeetham, , Coimbatore , India.

Yendluri Priya Yasaswini, Computer Science and engineering, SRM institute of technology, Amravathi , India

Somepalli Saranya , Electronics and communications engineering, vellore institute of technology, Vellore , India

II. SPECIFIC OBJECTIVIES

In our project, we are planning to embed JPG images inside JPG images. The size of the images does not matter as we reshape the images to 224*224. Only Convolutional Neural Networks is considered in our project. The CNN consists of three layers :the preparation network, the hiding network and the extracting network.

III. EXISTING WORKS

The following section provides a review of the literature related to the development of image steganography using convolution neural networks. This image steganography is implemented using google colabs. The goal is to visually hide a full N*N*RGB pixel secret image(JPG) in another N*N*RGB cover image(JPG), with minimal distortion to the cover image. The development was largely based on the methods discussed in ”Hiding Images in Plain Sight: Deep Steganography”,by Shumeet Baluja[1] which was submitted in ”31st conference on neural information processing systems(NIPS)” during the year 2017.The author provides a detail research on Steganography. Steganography is the art of covered or hidden writing; the term itself dates back to the 15th century, when messages were physically hidden.In modern steganography, the goal is to covertly communicate a digital message. The steganographic process places a hidden message in a transport medium, called the carrier. The carrier may be publicly visible. For added security, the hidden message can also be encrypted, thereby increasing the perceived randomness and decreasing the likelihood of content discovery even if the existence of the message detected. In this paper, the author’s goal was 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 (each color channel is 8 bits).However, unlike previous studies, in which a hidden text message must be sent with perfect 3 reconstruction, the author relaxes the requirement that the secret image is losslessly received. Instead, the author is willing for acceptable trade-offs in the quality of the carrier and secret image. The author also provides brief discussions of the discoverability of the existence of the secret message. Previous studies have demonstrated that hidden message bit rates as low as 0.1bpp can be discovered; our bit rates are 10*40*higher. Though visually hard to detect, given the large amount of hidden information, The author does not expect the existence of a secret message to be hidden from statistical analysis. Nonetheless, The author will show that commonly used methods do not end it, and the author gives promising directions on how to trade-o the difficulty of existence-discovery with reconstruction quality, as required. Though steganography is often confused with cryptography, in the author’s 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 primary focus of this paper is to concretely demonstrate that it is possible to encode a large amount of information in an image with limited visually noticeable artifacts. However, no explicit attempt has been made to actively hide the existence of that information from machine detection. Though The author cannot expect to completely hide the fact that up to 1/2 of the information is part of a hidden message, measures can be taken to make it more difficult to discover.

IV. SYSTEM ARCHITECTURE

A. Our neural network based model consists of 3 layers: the preparation network,the hiding network and the extraction network.The input to the preparation network is set of modied normalized JPG images.We rescale the images to make them of size 224*224. The preparation network consist of four 3*3 convolutional layers having 50 lters,kernel size of 3 and using activation function relu.This is followed by four 4*4 convolutional layers having 50 lters,kernel size of 4 and using activation function relu.This is followed by four 5*5 convolutional layers having 50 lters,kernel size of 5 and using activation function relu.This is followed by one 5*5 convolutional layer having 50 filters,kernel size of 5 and using activation function relu.This is followed by one 4*4 convolutional layer having 50 filters, kernel size of 4 and using activation function relu.This is followed by one 3*3 convolutional layer having 50 lters,kernel size of 3 and using activation function relu. The optimizer used is Adam optimizer. The output of the preparation network is sent as the input to the hiding network.Second input to this hiding network is cover image.Hiding network is similar to the preparation network in its design.The input of the reveal network is the output 5 of hiding network ad output of the revealing network is the secret message embedded in the cover image. The reveal network also has similar structure to the preparation network.

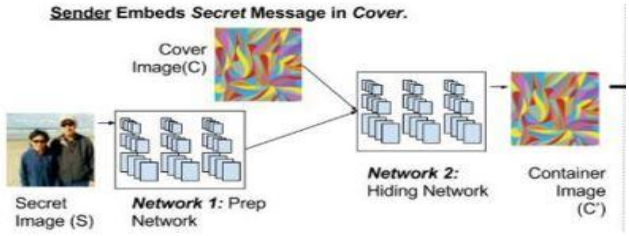

Figure 4.1: System Architecture

B. Methodology

The model takes as input a set of JPG images. This set is then separated into a set of secret images (images which will be hidden) and cover images (images which will hide the secret images). The model makes sure that the secret images and cover images are resized into 224*224. These images are then normalized before they are fed into the model. The model then fits itself on these sets of images. It consists of three layers - the preparation network, the hiding network and the reveal network - the architecture of which has been specified under 'System Architecture'. After the model learns to hide images within cover images with minimum loss, it is ready for deployment.

C. Implementation

Implementation details of the model is as follows: • TensorFlow : Used for creating the Convolutional Neural Network Model • Python3 : Language used to implement the model • Google Colab with GPU accelerator: Cloud PaaS for running the Deep Learning Model

V. RESULTS AND DISCUSSIONS

A. The model minimizes the loss between the original secret message and revealed secret message. This loss function is shown in 4.1 and 4.2. The loss function to be mininimized is given by L(C,C',S,S')=MSE(C-C')+beta*MSE(S-S')

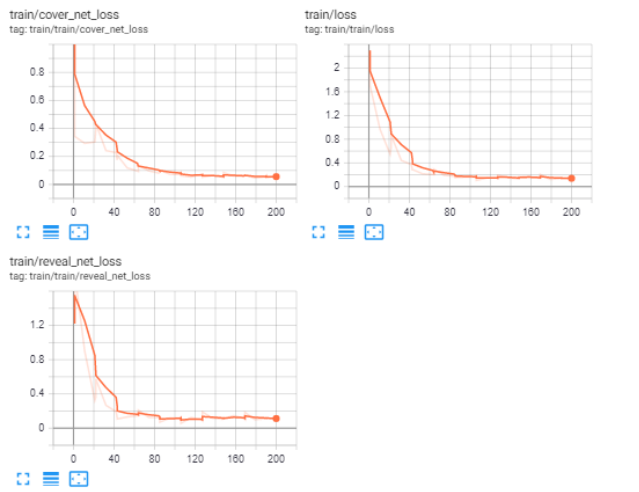

Figure 5.1: Minimizing loss - training graph

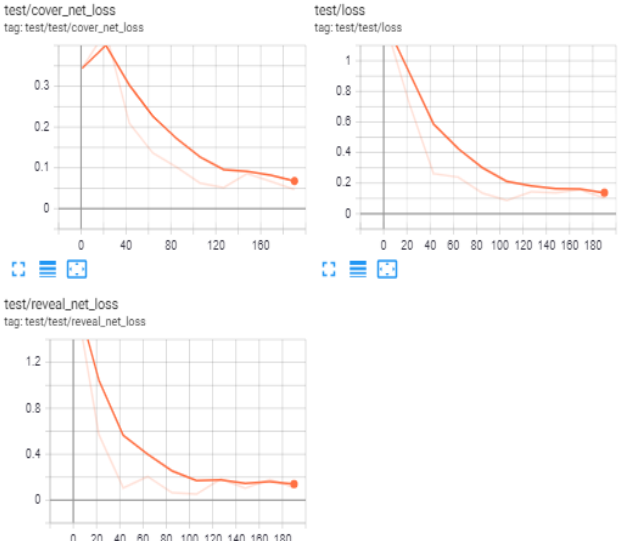

Figure 5.2: Minimizing loss - testing graph

The model successfully hides the secret image inside a cover image such that there is not much difference between the original cover image and the container image(Secret image + cover image) As shown in figures 5.3

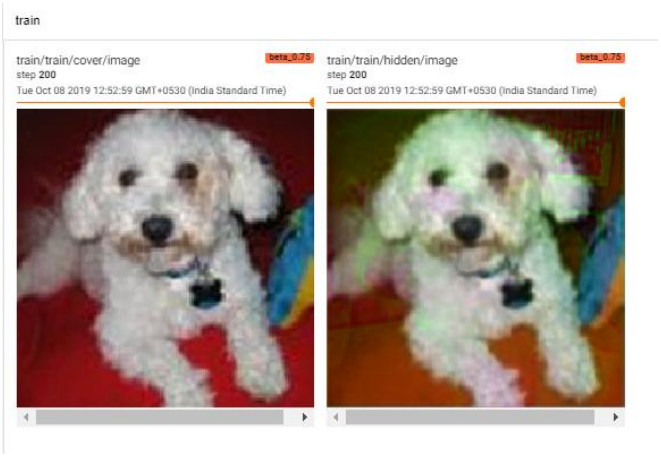

Figure 5.3: Cover Image(Left) and Container Image(Right)

Since there is not much difference between the cover image and container image and also since the method used by the convolutional neural network model is not known it becomes a very difficult task to find out whether an image has been hidden within the cover image,thus making the situation of an outsider finding out the secret image a near impossible one. The difference between the original secret image and the revealed secret image from the container image is low thus reducing the loss of information between the sender and the intended receiver all of the above results show that the model is successful both in hiding secret images from attackers and in transmitting the secret image to the intended receiver with minimum loss.

Figure 5.4: Secret image

Figure 5.5: Revealed image

VI. CONCLUSION AND FUTURE WORK

To hide confidential information, steganography can be effectively used. The objective of any Steganographic method is to hide maximum secret information which is immune to external attacks and also should not convey the fact that the cover medium is a carrier of secret information. Future works include use of pretrained models for steganalysis to discover secret message as adversial networks in GAN to reduce errors and permutations of various bits and sender key to enhance handling ability of network.This study opens a new avenue for exploration with steganography and, more generally, in placing supplementary information in images. Several previous methods have attempted to use neural networks to either augment or replace a small portion of an image-hiding system. We have demonstrated a method to create a fully trainable system that provides visually excellent results in unobtrusively placing a full-size, color image into another image. Although the system has been described in the context of images, the same system can be trained for embedding text, different-sized images, or audio. Additionally, by using spectrograms of audio files as images, the techniques described here can readily be used on audio samples..

REFERENCES

1. Shumeet Baluja,Hiding Images in Plain Sight: Deep Steganography, 31st Conference on Neural Information Processing Systems(NIPS 2017), Long Beach, CA, USA.
2. Jessica Fridrich,Miroslav Goljan,and RuiDu.Detecting lsb steganography in color,and gray-scale images.IEEE multimedia, 8(4):2228, 2001.
3. Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan. Deep learning for steganalysis via convolutional neuralnetworks.In SPIE/IST Electronic Imaging ,International Society for Optics and Photonics, 2015H.

4. Sabah Husien and Haitham Badi.Articial neural network for steganography.Neural Computing and Applications, 26(1):111116, 2015.
5. Robert Jaruek,Eva Volna,and Martin Kotyrba. Neural network approach to image steganography techniques.In Mendel 2015, pages 317327.Springer, 20
6. Georey E Hinton and Ruslan R Salakhutdinov.Reducing the dimensionality of data with neural networks.Science, 313(5786):504507, 2006.

AUTHORS PROFILE

Yendluri Lohith Jayasurya , Btech computer science Amrita Vishwa vidyapeetham , Coimbatore , India

Yendluri Priya Yasaswini , Btech Computer science
Srm institute of technology , Amravathi , india

Somepalli Saranya , Electronics and communications engineering, vellore institute of technology, Vellore , India