SEEN: A Study on Steganalysis using Convolutional Neural Network

Jerico R. Agustin and Joseph Anthony C. Hermocilla

INTRODUCTION

The rise of computer age has impacted the lives of many people especially in this generation. It augmented different areas of life, at the same time, it accentuated the importance of securing the information that are available on the Internet. The challenge is to preserve the confidentiality, integrity and availability of the resources. Confidentiality is one of the key aspects in terms of securing communication of two entities.

Nowadays, many cyber criminals are making sophisticated attacks in order to get what they want, and one of those attacks is the use of steganography. The criminals may inject data that has spyware which can give access to communication between malicious programs, or any new malware[4] on the images and infect an individual's device. By creating a program that uses Convolutional Neural Network, a program can statistically identify the probability of whether an image is a stego-bearing image or is just an ordinary image and help people lessen the risk of being infected by the malicious programs inserted in images on the Internet.

OBJECTIVES

The objective of this study is to determine the accuracy of the Convolutional Neural Network in identifying stego-bearing images. Specifically, this project aims to:

1. gather 500 different JPEG images with size of 512 x 512;
2. create 4 different orientations of the images and then create another 4 sets of it;
3. apply steganography to every 2000 images using Salgado's image steganography software that implements Jsteg, F5, Outguess;
4. create a application that implements Convolutional Neural Network;
5. feed the dataset to the Machine Learning algorithm and label it according to the steganography algorithm that is used to it;
6. create an application that uploads JPEG image, and analyses and classifies whether it is a stego bearing image or not;
7. evaluate the results for classifying the images that used the steganographic algorithms in Salgado's work; and
8. given the results, determine the prediction rate of the Convolutional Neural Network and Couchot et al.'s work.

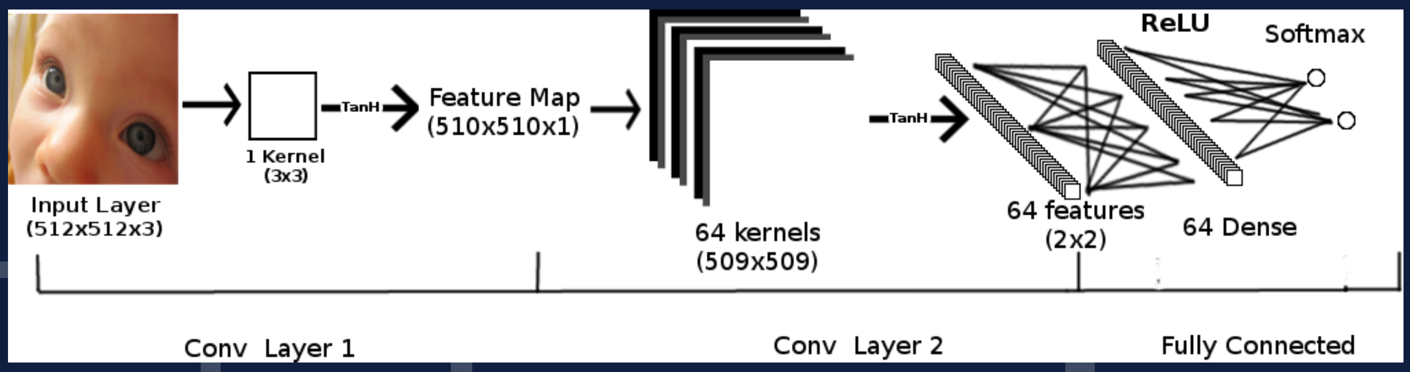
METHODOLOGY

Python 3.5.2

Keras

Tensorflow

Convolutional Neural Network Architecture

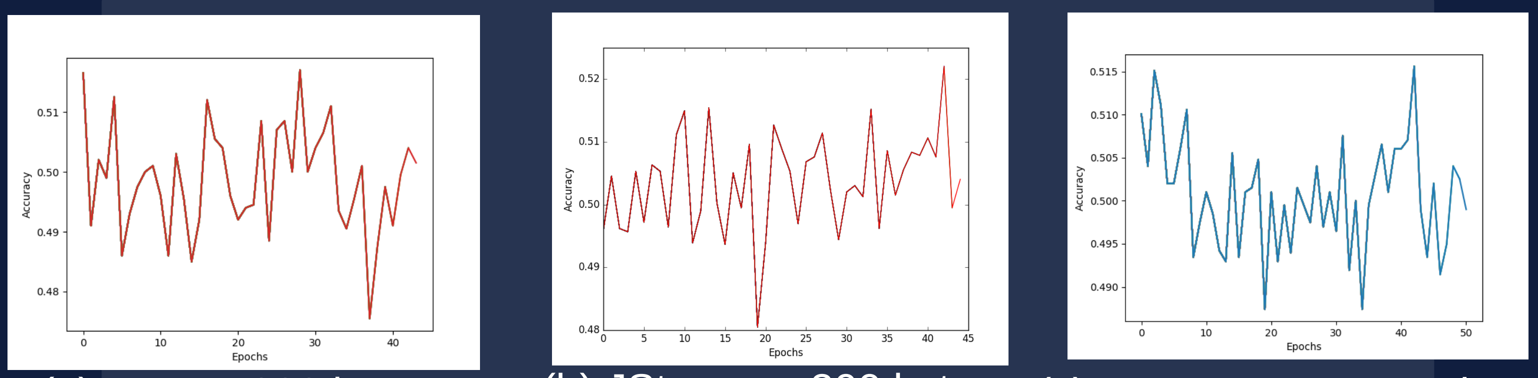


Building Dataset

6000 JPEG images were created to stego-bearing images that uses F5, JSteg and Outguess from Salgado's SP. And another dataset was taken from BOSS (Break Our Steganographic Sysyem) dataset that contains 8156 of each steganographic algorithms namely HUGO, J-UNIWARD and WOW.

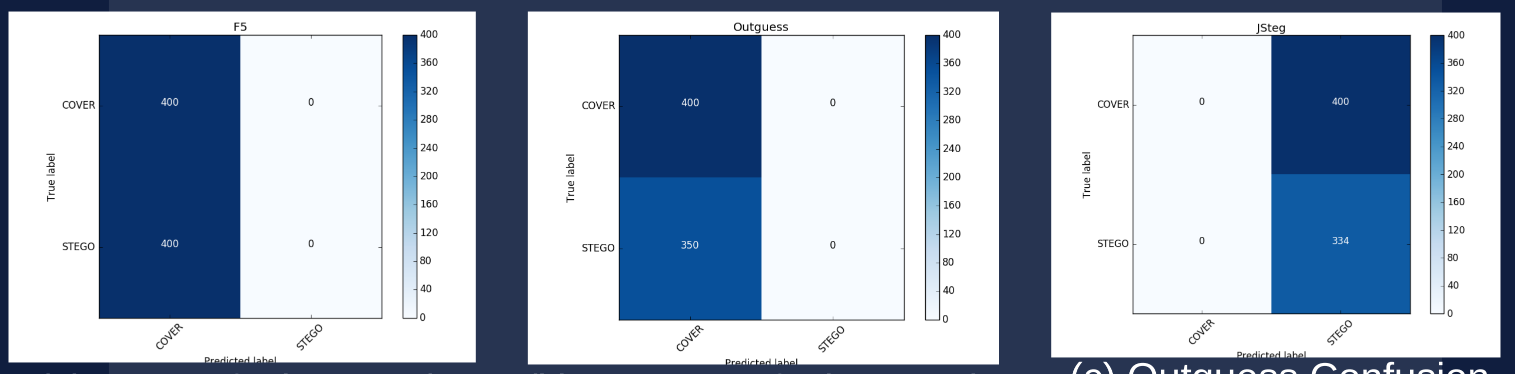
RESULTS

F5, JSteg and Outguess



(a) F5, α ≤ 300 bytes (b) JSteg, α ≤ 300 bytes (c) Outguess, α ≤ 300 bytes

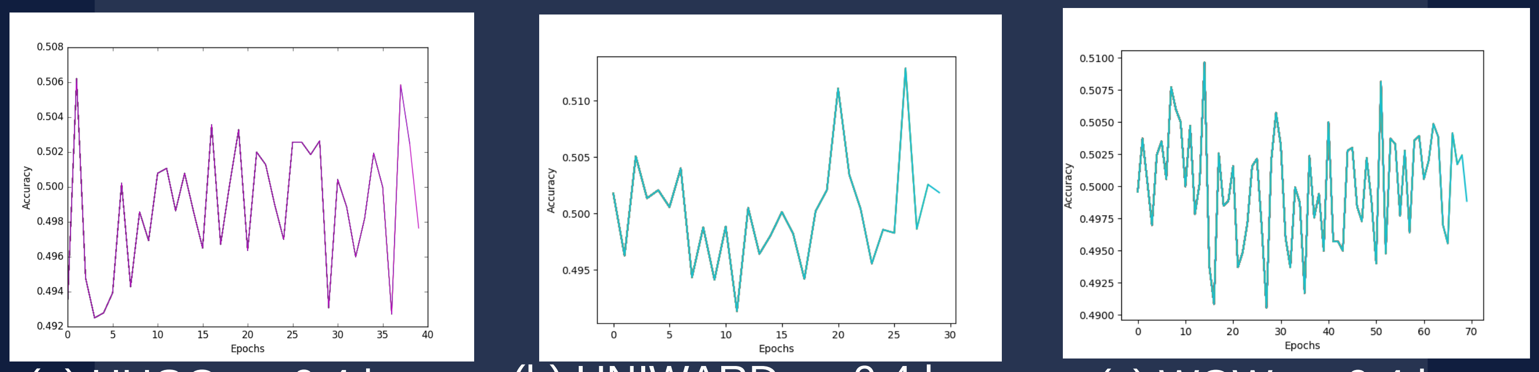
Fig. 1: Average accuracy in every iterations(epoch) of the datasets in case of F5, JSteg, and Outguess steganographic schemes (with a payload α)



(a) F5 Confusion Matrix (b) JSteg Confusion Matrix (c) Outguess Confusion Matrix

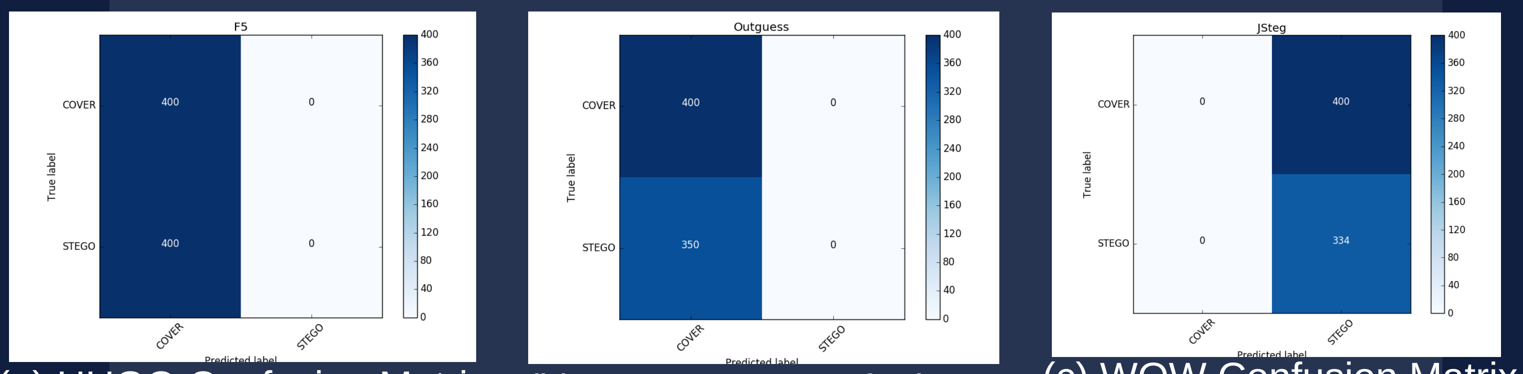
Fig. 2: Confusion Matrix of the test dataset that were created using Salgado's work

HUGO, UNIWARD and WOW



(a) HUGO, α=0.4 bpp (b) UNIWARD, α=0.4 bpp (c) WOW, α=0.4 bpp

Fig. 3: Average accuracy in every iterations(epoch) of the datasets in case of HUGO, UNIWARD, and WOW steganographic schemes (with a payload α) using the proposed CNN Architecture



(a) HUGO Confusion Matrix (b) UNIWARD Confusion Matrix (c) WOW Confusion Matrix

Fig. 3: Confusion Matrix of the test dataset that were taken from the BOSSbase Dataset

Aboutt the Author

Jerico R. Agustin BS Computer Science student from the University of the Philippines Los Banos. A proud member of Philippine Campus Crusade for Christ, called to be an evangelist and set apart for the Gospel of God