PROC. INTERNAT. CONF. SCI. ENGIN.
Volume 3, April 2020 | Pages: 207-211

ISSN 2597-5250
E-ISSN 2598-232X

Steganalysis Using Yedrodj-net net's Convolutional Neural Networks (CNN) Method on Steganography Tools

Nurmi Hidayasari[1,]*, Imam Riadi[2], Yudi Prayudi[3]
[1,3]Informatics Engineering Departement, UII Yogyakarta,
[2]Information System Departement, UAD Yogyakarta
Email*: 16917219@students.uii.ac.id

Abstract. Steganalysis method is used to detect the presence or absence of steganography files or can be referred to anti-steganography. Steganalysis can be used for positive purposes, which is to know the weaknesses of a steganography method, so that improvements can be made. One category of steganalysis is blind steganalysis, which is a way to detect secret files without knowing what steganography method is used. Blind steganalysis is difficult to implement, but then machine learning techniques emerged that could be used to create a detection model using experimental data, one of which is Convolutional Neural Networks (CNN). A study proposes that the CNN method can detect steganography files using the latest method with a low error probability value compared to other methods, CNN Yedroudj-net. As one of the steganalysis methods with the latest machine learning steganalysis techniques, an experiment is needed to find out whether Yedroudj-net can be a steganalysis for the output of many tools commonly used for steganography applications. Knowing the performance of CNN Yedroudj-net on several steganography tools is very important, to measure the level of ability in terms of steganalysis of some of these tools. Especially so far, machine learning performance is still doubtful in blind steganalysis. Plus some previous research only focused on certain methods to prove the performance of the proposed technique, including Yedroudj-net. This study will use five tools that are Hide In Picture (HIP), OpenStego, SilentEye, Steg and S-Tools, which are not known exactly what steganography methods are used on the tools. Yedroudj-net method will be implemented in the steganography file from the output of the five tools. Then a comparison with the popular steganalysis tool is used, StegSpy. The results show that Yedroudj-net is quite capable of detecting the presence of steganography files, slightly better than StegSpy.

Keywords: Blind steganalysis, convolutional neural networks (CNN), steganalysis, Yedroudj-net

INTRODUCTION

Steganography is a technique for hiding or inserting messages into media. The messages and storage media used can be text, images, audio, video, and so on. Steganography is even easier to use with open source tools that can be used by anyone and anywhere, and can be easily found online. Most tools are made with techniques that can be fairly safe, such as the addition of a secret key and encryption techniques. Examples steganography tools are S-Tools, and OpenStego.

Steganalysis as an anti-steganography method is a technique used to detect the presence of steganography files. Steganalysis for good purposes can be made as a benchmark to find trends, need to develop methods of steganography. Improving safer insertion techniques (Pamungkas, Hidayat and Andini, 2017). While the purpose is not good, which is to look for a gap in the existence of secret messages and then destroy them.

One of the main categories of steganalysis is universal or blind steganalysis, a technique that attempts to detect messages that are inserted with any steganography method, in other words, steganalysis is done without knowing what steganography methods are used to hide data. Universal steganalysis is difficult to apply because one of the obstacles is that it is difficult to find relevant features of the characteristics of steganography images. But then, machine learning techniques emerged that were used to create a detection model using experimental data (Karampidis, Kavallieratou and Papadourakis, 2018).

One example of steganalysis using machine learning techniques is the Convolutional Neural Networks (CNN) method. Recent research related to CNN was developed by Yedroudj, Comby, and Chaumont (2018), the method was developed to be more complex by adding the number of filters used in each process as well as five convolutional layers and batch normalization. With an error probability value of 14%.

As one of the steganalysis methods with the latest machine learning steganalysis techniques, an experiment is needed to find out whether the CNN Yedroudj-net is able to be a steganalysis for the output of a number of tools commonly used for steganography applications. Knowing the performance of CNN Yedroudj-net on several steganography tools is very important, to measure the level of ability in terms of steganalysis of some of these tools.

Especially so far, the performance of machine learning is still in doubt about universal steganalysis or blind steganalysis. Plus some previous research only focused on certain methods to prove the performance of the proposed technique. Until now, there has not been a comprehensive review discussing the performance of

steganalysis with machine learning techniques especially CNN Yedroudj-net as a steganalysis of some tools commonly used in society. Therefore, in this study a trial will be conducted on CNN Yedroudj-net to determine the extent of its ability to detect steganography generated from tools.

In this study we will use five steganography tools that are considered quite good, namely Hide In Picture (HIP), OpenStego, SilentEye, Steg and S-Tools. In (Cheddad, Condell, Curran, & Mckevitt, 2012), it states that OpenStego and also Hide In Picture include tools that have good quality based on the results of a steganalysis trial by calculating its PSNR value (Peak Signal to Noise Ratio). In this case PSNR is used to compare the quality of original media and also media that has been hidden messages (media stego).

Another consideration using the tools mentioned earlier is that the five tools have a high level of security. This can be seen by the writer directly when opening each tool. Where each tool provides a message encryption feature that is commonly used. With the addition of encryption techniques, it is likely that messages will be increasingly difficult to detect. Another consideration is that the five tools are still easy to find and download on online sites, so anyone can use them freely. This could lead to widespread use of steganography.

MATERIALS AND METHODS

Steganography Tools

Hide In Picture

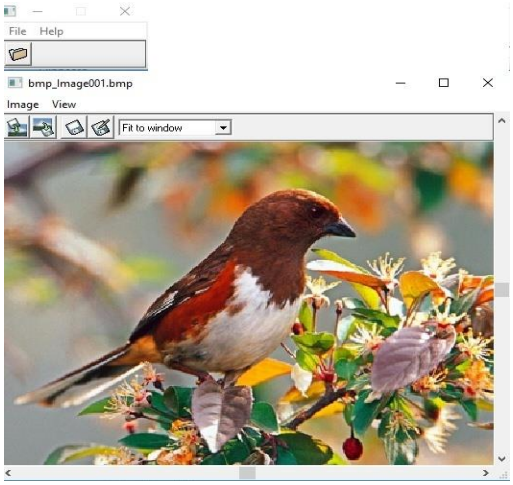

Figure 1. Tools Hide In Picture.

Hide In Picture (HIP) was created by Davi Tassinari de Figueireddo in 2001. Formats that can be used on HIP are BMP and GIF. In HIP, the message file bits are randomly stored in a media file with an encryption algorithm, based on the password entered. The position to store message bits will be chosen randomly using random techniques. In this way, it will be more difficult to know the whereabouts of messages stored in the media (Cheddad et al., 2012).

OpenStego

It is a java based tool, which has two functions which can be used to hide data or for watermarking. Files that can be used as storage media for these tools are, BMP, GIF, JPEG, JPG, PNG, and WNMP. Then the file that has been pasted the message will be saved in PNG format. OpenStego provides passwords to increase security on stego files (Kunjir, Patil, Jabeen, Bhosale, and College, 2016).

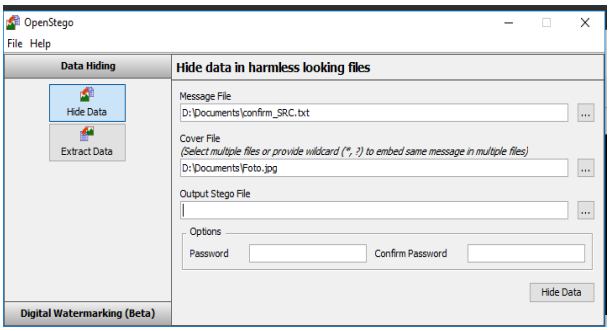

Figure 2. Tools OpenStego.

SilentEye

This tool provides an interface that can be used on all operating systems with a pretty good appearance and easy integration of the new steganography algorithm. Media files that use data are BMP, JPG, PNG, GIF, TIF and WAV. This tool also features a password addition for files with BMP and JPG formats (Kunjir et al., 2016).

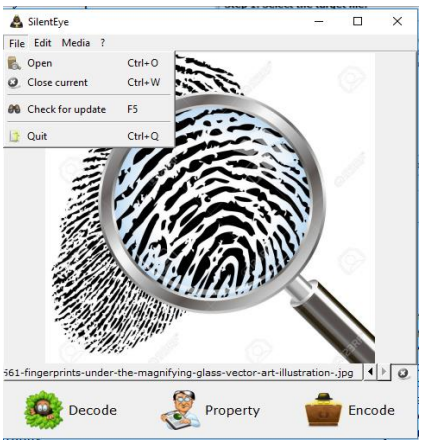

Figure 3. Tools SilentEye.

Steg

Tools written in C ++ are very easy to use because they are portable. This Steg tool combines steganography and kiptography techniques to hide messages. Image formats that can be used as media are JPG, TIF, PNG and BMP and the message format is in the form of TXT. Stego files can be saved in PNG and TIF formats. The

cryptographic keys used are symmetrical and asymmetrical (Kunjir et al., 2016).

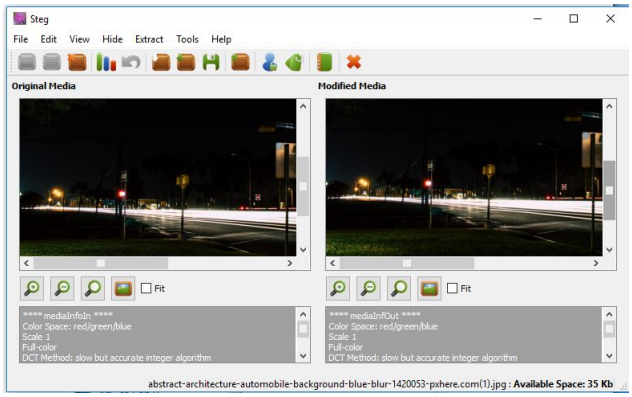

Figure 4. Tools Steg.

S-Tools

The tools made by Andy Brown have similarities with HIP, namely file formats that can be used as media are GIF and BMP only. S-Tools is fairly easy to use because the interface is designed so simple. To load images, users only need to drag the image to the system. After the image is dragged, the system will provide information about the number (size) of files that can be accommodated by the image.

S-Tools involves changing the LSB (Least Significant Bit) of each of the three colors (Red, Green, Blue) in pixels in a 24-bit image. In S-Tools there is a pre-processing step to reduce the number of color entries by using measurement distances to identify colors that are similar in terms of intensity. After this step, any insignificant color will be associated with two other colors, one of which is a place to store messages (Cheddad et al., 2012).

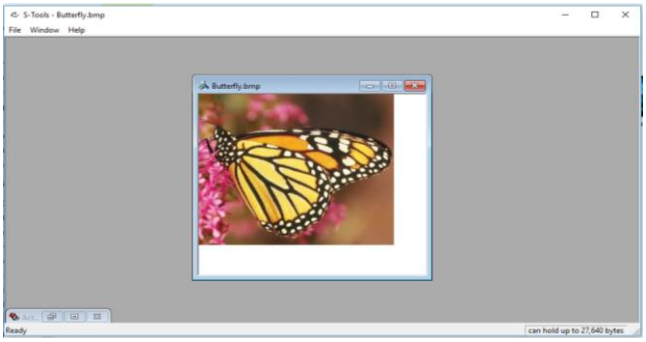

Figure 5. Tools S-Tools.

Steganalysis

Steganalysis is a procedure that is contrary to steganography, which is a way to detect whether an object has a secret message that is hidden or not. In general, steganalysis consists of two parts, namely active and passive steganalysis. Passive steganalysis only determines whether a particular media is stego by comparing the original and stego media. While active will try to detect the length of the message and extract it, it can even do the destruction of the message and the media stego (Karampidis et al., 2018). Based on the technique, steganalysis is divided into two, namely based on subjective (visual) and statistics (Chen, 2005). Subjective (visual) techniques utilize the senses of human vision to observe stego images or those suspected of being stego images. For example the StegSpy application and also the Enhanced LSB algorithm. Whereas steganalysis with statistical techniques is a technique that uses mathematical assistance to analyze between the original image and the stego image. The Yedroudj-net CNN method includes steganalysis using statistical techniques.

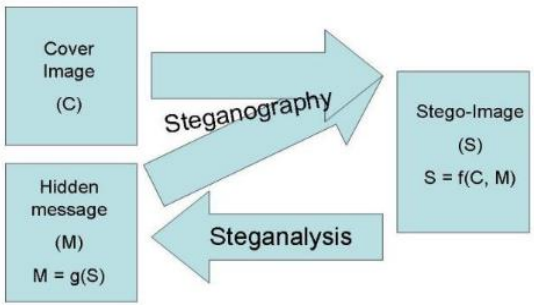

Figure 6. Overview of the Steganalysis Process (Sutanto, 2010).

Convolutional Neural Networks (CNN) Methods

Convolutional Neural Networks (CNN), is a class of deep feed-forward artificial neural networks that are widely used for image or image analysis. CNN itself is inspired by biological processes, in which connectivity patterns between neurons resemble the visual cortex in animals (Suyanto, 2018). According to Aloem, et al (2018), CNN consists of one input layer, one output layer, and a number of hidden layers. This hidden layer usually contains convolutional layers, pooling layers, normalization layers, ReLU layers, fully connected layers and loss layers (Suyanto, 2018)

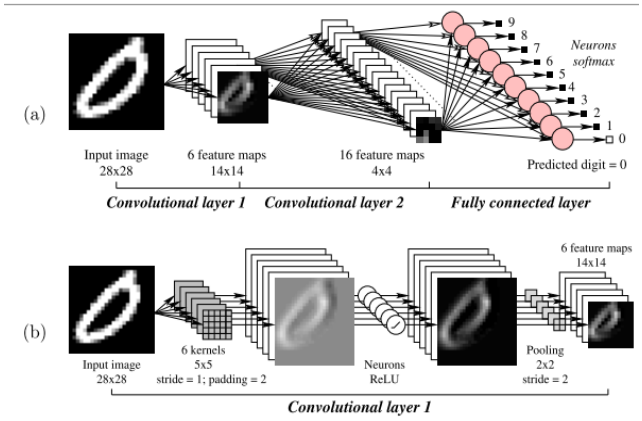

Figure 7. CNN architecture in general (a), Detail view of convolutional layers (b).

Yedroudj-net CNN Methods (Yedroudj et al., 2018)
The Yedroudj-net CNN method is basically the same as the other CNN methods, but it is more complex because there are some additions or modifications to each layer. This technique consists of five pre-processing blocks, five convolutional blocks, and a fully connected block consisting of three fully connected layers and finally followed by softmax. The network produces a probability distribution through two class labels. The pre-processing block filters the original image or stego image with a predetermined high-pass filter to extract residual noise.

Images that have been processed, then processed in the network. Pre-processing using a high-pass filter can largely suppress image content, dynamically reduce the range, and thereby increase the signal-to-noise ratio between a weak stego signal and the original image signal. As a result, CNN is able to learn from stronger signals. CNN Yedroudj-net uses 30 basic filters, to process the previous input image.

Furthermore, the CNN Yedroudj-net is divided into convolutional layers dedicated to the representation feature, which transforms input images into feature vectors and classification modules consisting of three layers. This layer is connected to the softmax layer, which results in a classification decision whether the image is an original or stego image. As with other CNN methods (such as Xu-Net), the convolutional module has five blocks marked with Block 1 to Block 5, to extract effective features to cover and stop image discrimination, can be seen on images below:

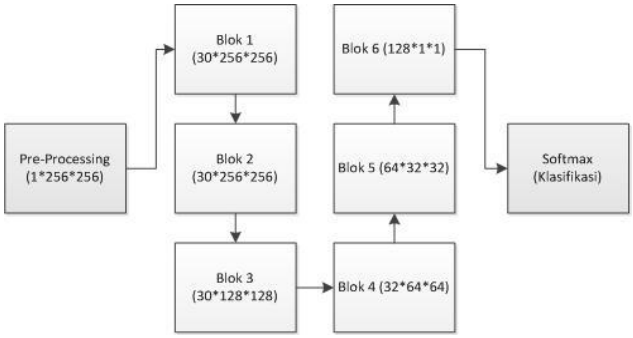

Figure 8. General description of the Yedroudj-net method.

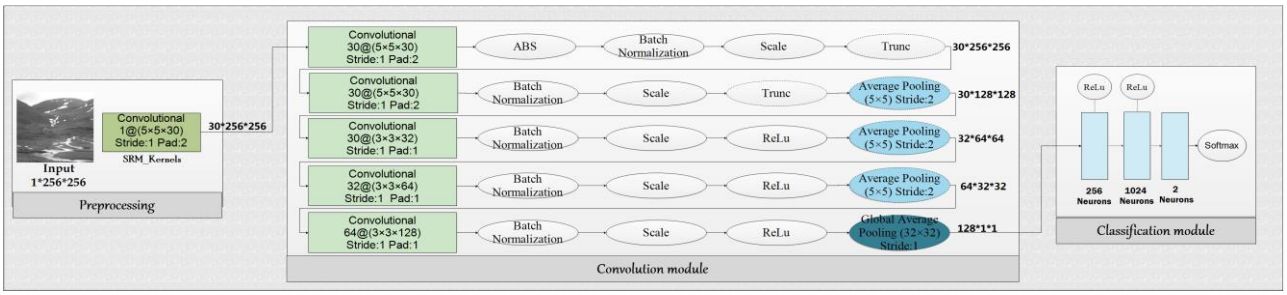

Figure 9. Illustration of the entire Yedroudj-net method.

Collection of images

The initial stage will be collecting images that will be used to hide the message. Images will be collected or downloaded using the help of the Add-Ons DownThemAll provided by the Firefox browser application. These add-ons can be found at https://addons.mozilla.org/en-US/firefox/addon/save-all-images-webextension. To add Add-ons to the browser, you can select the "Add to Firefox" button, as can be seen in the image below:

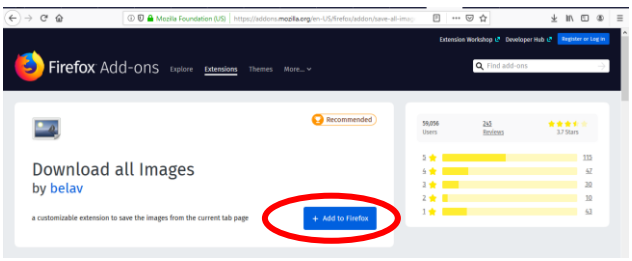

Figure 10. Illustration of the entire Yedroudj-net method.

Use of Steganography tools

This stage will perform the steganography process using the five tools mentioned earlier, namely Hide In Picture (HIP), OpenStego, SilentEye, Steg and S-Tools. Each tool has input and output with different image formats, and secret messages that are inserted are also different. A full explanation can be seen in the following table:

Table 1. Detailed format image and messages used for each tools.

Tools	Original Images (Input)	Messages	Stego Images (uotput)
OpenStego	JPG	Pesan Rahasia.txt	PNG
HIP	BMP	Pesan Rahasia.txt	BMP
Steg	JPG	Pesan Rahasia 2.txt	JPG
S-Tools	BMP	Pesan Rahasia.txt	BMP
SilentEye	BMP	Pesan Rahasia.txt	BMP

RESULTS AND DISCUSSION

Previously, a steganography process was carried out using five tools, then this stage will implement the Yedroudj-net CNN method using the stego (output) file. Output from the previous stage, to find out the extent of the ability of the method to detect stego images. Then the results will be compared with the StegSpy tools. In this study, the images used for data training 200 and data testing 100. For testing, the method uses two classes, namely the stego file class and the normal file (non-stego). The results are briefly shown in Table 2.

Table 2. Results of steganography tools.

Tools	Results	
	CNN Yedroudj-net	**StegSpy**
Hide In Picture	12.5%	0.3%
OpenStego	14.3%	0.32%
SilentEye	11%	0.3%
Steg	10.8%	0.02%
S-Tools	19.1%	0.88%

CONCLUSIONS

This study shows that the CNN Yedroudj-Net method as one of the machine learning methods in steganalysis has good performance, especially in detecting stego images generated from tools. It shows that CNN Yedroudj-Net has the ability to detect universal or blind steganalysis. Compared to the commonly used steganalysis tools (StegSpy), the results obtained are not much different. However, StegSpy is more superior, the results obtained are better than the CNN Yedroudj-Net method. Maybe for further research, it can compare CNN Yedroudj-Net method with other newer and more complex CNN methods.

REFERENCES

Cheddad A, Condell J, Curran K, Mckevitt P. 2012. A Comparative Analysis of Steganographic Tools. School of Computing and Intelligent Systems. 29–37.

Chen W. 2005. Study of Steganalysis Methods. A Thesis Submitted to the Faculty of New Jersey Institute of Technology in Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical Engineering.

Karampidis K, Kavallieratou E, Papadourakis G. 2018. A Review of Image Steganalysis Techniques for Digital forensics. Journal of Information Security and Applications 40: 217–235. https://doi.org/10.1016/j.jisa.2018.04.005

Kunjir SM, Patil SD, Jabeen S, Bhosale SV, College DYPACS. 2016. Review On Stenography Tools. International Research Journal of Engineering and Technology (IRJET) 3(10): 1223–1225.

Pamungkas FG, Hidayat B, Andini N. 2017. Implementasi Teknik Steganalisis Menggunakan Metode Improvement Difference Image Histogram. 1–7.

Sutanto H. 2010. Kajian Mengenai Stegosistem dan Steganalisis pada File Gambar.

Suyanto. 2018. Machine Learning - Tingkat Dasar dan Lanjut. Penerbit Informatika, Bandung.

Yedroudj M, Comby F, Chaumont M. 2018. Yedroudj-Net: An Efficient CNN for Spatial Steganalysis. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing-Proceedings April 2018, 2092–2096. https://doi.org/10.1109/ICASSP.2018.8461438

THIS PAGE INTENTIONALLY LEFT BLANK