SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

# Message Insertion Using the Convolutional Neural Network Model Approach

Lita Ambarwati
Universitas Prima Indonesia
Medan, Indonesia
Lithaambarwati@gmail.com

Agrifa Darwanto Sirait
Universitas Prima Indonesia
Medan, Indonesia
agrifacrly@gmail.com

Bella Siska Tambun
Universitas Prima Indonesia
Medan, Indonesia
bellasiskatambun@gmail.com

Eko Paskah Jeremia Purwanto
Universitas Prima Indonesia
Medan, Indonesia
mogumogukuronuma @gmail.com

Amir Mahmud Husein
Universitas Prima Indonesia
Medan, Indonesia
amirmahmud@unprimdn.ac.id

***Abstract***— One problem in computer vision that has long been sought for a solution is the classification of objects in the image in general. How to duplicate the ability of humans to understand image information, so that computers can recognize objects in the image as humans do. The feature engineering process used is generally very limited where it can only apply to certain datasets without the ability to generalize to any type of image. That is because various differences between images include differences in perspective, differences in scale, differences in lighting conditions, deformation of objects, and so on. Academics who have long struggled with this issue. The application of the Convolutional Neural Network (CNN) method for the insertion of messages in an image with the aim of securing the proposed message produces good security, from the test results, it can be concluded as follows The Convolutional Neural Network (CNN) method requires computing time to insert messages in a secret image. The model framework uses 2 (two) images with the aim of the cover image as input and the secret image where the secret image has been inserted a message so that the secret is not visible. The cover image that has been inserted a secret picture that contains the message looks not much different, but the file size of the secret picture has increased by 66%.

**Keywords**— Convolutional Neural Network, Citra Digital, Deep Learning, Steganography.

## I. INTRODUCTION

One problem in computer vision that has long been sought for a solution is the classification of objects in the image in general. How to duplicate the ability of humans to understand image information, so that computers can recognize objects in the image as humans do. The feature engineering process used is generally very limited where it can only apply to certain datasets without the ability to generalize to any type of image. That is because various differences between images include differences in perspective, differences in scale, differences in lighting conditions, deformation of objects, and so on. Academics who have long struggled with this issue.

Many attempts were made to devise a steganographic algorithm that minimizes interference in the cover message when the secret message is embedded in it, for the recovery of the secret message. Steganography only aims to hide or keep secret messages (Jain, Mr. Mahavir, et al., 2014). The recipient of the steganography image will then

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

decode to embed the message and extract the message's ciphertext and then decrypt it using the existing shared key (Zhang, Zhuo, et al., 2019).

Designing effective features turns out to be a difficult task and requires strong domain knowledge about steganography and steganylysis. Recently some interesting works have been proposed to detect steganography based on deep convolution neural networks (S. Tan & B. Li, 2014). Compared to traditional methods that extract CNN handmade features automatically learn the effective features of using various network architectures to distinguish cover images and stego images, propose a new CNN model to detect steganography based on residual learning and achieve a low detection error rate when cover images are paired (S. Wu, et al., 2017) (G. Xu, 2017).

## II. LITERATURE REVIEW

### *2.1 Convolutional Neural Network*

Convolutional Neural Networks combine three main architectures, namely local receptive fields, shared weight in the form of filters, and spatial subsampling in the form of pooling. Convolution or commonly called convolution is a matrix that functions to filter (Jamie & George, 2017). In conducting the filtering process there are two matrices, namely the matrix of the value input and the kernel matrix. In the Convolutional Neural Network, there are several layers that function to perform filters that have been set during the training process, namely the Convolutional Layer, the Pooling Layer, and the Fully Connected Layer. The architecture owned by the Convolutional Neural Network is as follows :

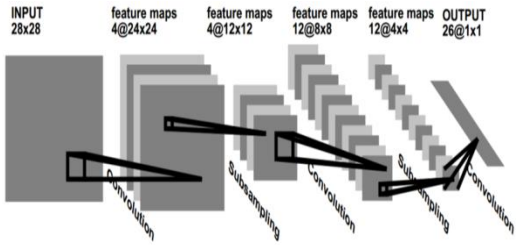



**Figure 2.1.** Convolutional Neural Network Architecture

Convolution Layer has several parameters, namely kernel size, skipping factors and connection table. The kernel in CNN always shifts to the area in the input image, while Skipping factor is the number of pixels shifted in the kernel (S. Tan and B. Li, 2014). The size of the output on the map is:

$$M_x^n = \frac{M_x^{n-1} - K_x^n}{S_x^n + 1} + 1 \; ; \; M_y^n \frac{M - K_y^n}{S_y^n + 1} + 1$$

Wich one :
$M_x, M_y$ = Size of feature maps
$S_x, S_y$ = Skipping Factors
$K_x, K_y$ = kernel size
n = Layers of layers during the process

The purpose of the pooling layer is to reduce the resolution of feature maps. In the pooling layer, there are several operations including: max pooling and average pooling (G. Xu, H. Wu, and Y.Q, 2016) The new max pooling feature map resolution can be obtained by:

$$a_j = \max_{N x N} a_i^{N \times N} \mu(n, n))$$

Information:
$a_j$ = value from the pooling map
$a_j$ = value of the input map
$\mu$ $(n, n)$ = window function

Here is an example of the process of Max Pooling with a size of 2 x 2.

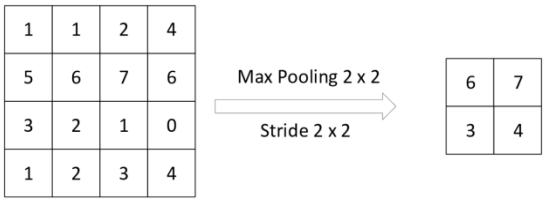



**Figure 2.2.** Example of the Pooling Layer Process

Fully Connected Layers connect each neuron from Layer to other Layer. Here's an example from Fully Connected Layers.

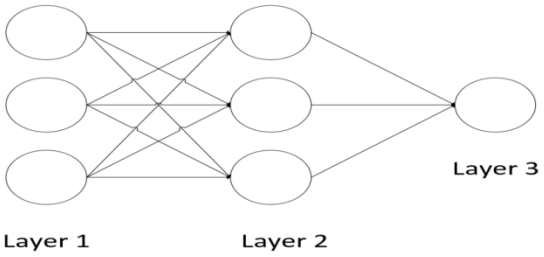



**Figure 2.3.** Fully Connected Layer

### 2.2 Digital Image

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Image is a representation, similarity or imitation of an object or objects (Yan, Min, et al., 2017). Digital images are images that can be processed by a computer. The term digital image is very popular today. Many electronic devices, such as scanners, digital cameras, digital microscopes, and fingerprint readers (fingerprint readers), which produce digital images are also very popularly used by users to process photos or for various other purposes. For example, Adobe Photoshop and GIMP (the GNU Image Manipulation Program) provide various features for manipulating digital images (Abdul & Adhi, 2013) ( Sari, et al., 2017).

Mathematically, the image referred to as a continuous function light intensity in a two-dimensional plane. The visible image is light reflected from an object. The image is divided into two, namely continuous images obtained from optical systems that receive analog signals (human eyes and analog cameras) and discrete (digital) images generated through the process of digitizing continuous images. The process of digitization in digital images is divided into two processes namely sampling and quantization. The sampling process is the process of taking a periodic discrete coordinate value (x, y) with a sampling period T. The quantization process is a process of grouping the gray image level of continuous images into several levels or is the process of dividing gray scale (0, L) into G levels that are expressed by an integer price, expressed as $G = 2$ with, where G is the degree of gray and m is a positive integer. Thus digital images are also called matrix $A$ sized $M$ (row) x $N$ (column) where the row and column indices represent a point in the image and the matrix element expresses the gray level at that point.

### 2.3 STEGANOGRAPHY

Steganography is one of the art and sciences that implants hidden messages into carrier signals. Unlike encrypted messages, simple steganographic messages provide security through obscurity (Parisa & Mark, 2019). Many attempts were made to devise a steganographic algorithm that minimizes interference in the cover message when the secret message is embedded in it, while allowing for the recovery of the secret message. Steganography only aims to hide the existence of messages. As such, it is almost always the case that messages are encrypted before embedding using a standard cryptographic scheme. The recipient of the steganography image will then decode to reveal the password text of the message and then decrypt it using the existing shared key (Jamie & George, 2017).

To refute information hidden in a Steganalysis container it is usually used. The stage that can distinguish images with some hidden messages from blanks is done using binary classification. Related to the basics of steganalysis based on feature extractors such as SPAM (Pevny, et al., 2010), SRM (Fridrich & Kodovsky, 2012), etc.

With the recent extraordinary confidence of deep neural networks, accessing new neural networks for steganalysis is gaining popularity (Qian et al., 2015b). For example, in (Pibre et al., 2015) the authors agreed to use deep convolution (Convolutional Neural Network) neural networks for steganalysis and show what is meant by classifications that can increase significantly when using CNN in ordinary classifiers.

## III. PROPOSED METHOD

The methods used in this study are as follows:

### 3.1 Sampling for Data Input

Input data used in this network are examples with 256 x 256 image sizes. Total sample data used is 50-100. Data training is used for the network learning process with the aim of encoding secret images into cover images through the Convolutional Neural Network.

### 3.2 Work Step

SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

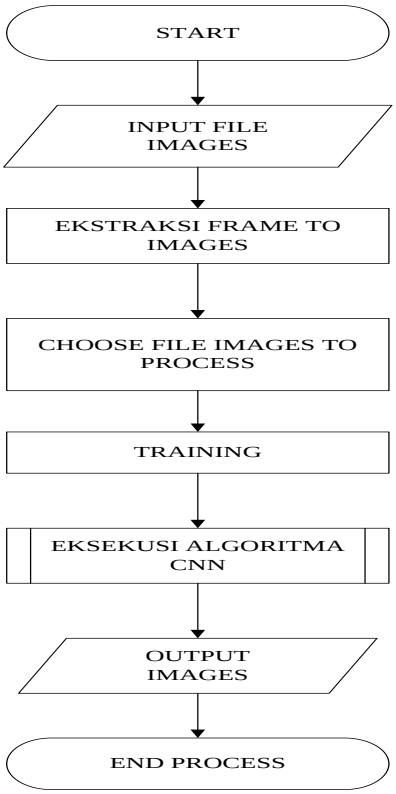



**Figure 3.1.** *Flowchart* Images Process

The flow of this research starts from inputing sample data in the form of images. Then design a network with CNN method to improve the quality of input images.

## IV. RESULT AND DISCUSSION

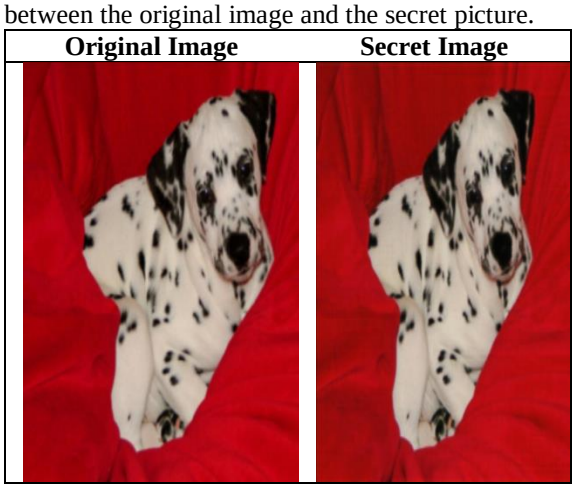
The results of applying the Convolutional Neural Network method for the insertion of messages in an image with the aim of securing the message to be conveyed, the testing process uses training data on 100 images with jpg extension, all images are resized to 256 × 256 without normalization, then implemented with intel core i5 platform specifications 2.5 GHz CPU, 8 Gb RAM and using the WIN 10 64 bits operating system.

**Figure 4.1.** Training Dataset

Testing framework by taking 2 (two) images as input, a topical image in the first row image, and a secret image in the second line image with the aim to encode the secret image into a cover image through the Convolutional Neural Network (CNN) network, then a secret message is inserted in secret image so that the secret message is not seen. The following test results are shown in Figure 3.2

**Figure 4.2.** Test results

Based on the test results, the secret image that has been inserted a secret message looks not much different from the cover image, but if an enlarged image is made it will show a slight difference between the original image and the secret picture.



SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

**Figure 4.3** Testing Results

In the picture above, the difference between the original image and the picture that has been insert message in the secret image looks a little different, in addition to the size of the original image with a secret picture there is a difference as shown in table 3.1

| No | Image | Size (KB) | |
|---|---|---|---|
| | | Original | Results |
| 1 | Image 1 | 180 | 223 |
| 2 | Image 2 | 120 | 198 |
| 3 | Image 3 | 98 | 120 |
| 4 | Image 4 | 112 | 230 |
| 5 | Image 5 | 195 | 255 |
| 6 | Image 6 | 210 | 354 |
| .. | .. | **91** | **134** |

In table 3.1 is the result of comparison of the original image size with a secret picture that has been inserted a message with a 66% increase rate for each picture, more clearly can be seen below graph.

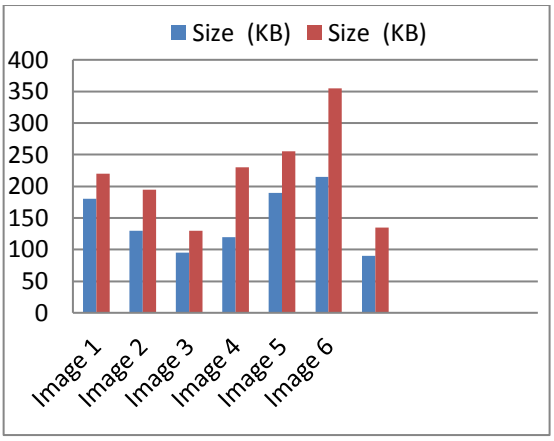



**Figure 4.4.** Graphic Comparison of Image Sizes

**DISCUSSION**

The framework that we propose to improve the security of the secret message that is inserted in the secret image with a 256x256 image size produces an image size difference of 66% from the original image, besides the secret image with the original image looks not too far apart at a glance, but if it is enlarged it will looks a little different. Our tests on JPG images have a high computational level where 10 images tested take 5 hours with a calculation of 2 hours for processing 1 image, this needs to be improved for the development of time optimization so that it is more efficient.

## V. CONCLUSION AND SUGESSTION

### 5.1 CONCLUSION

The application of the Convolutional Neural Network (CNN) method for the insertion of messages in an image with the aim of securing the proposed message produces good security, from the test results, it can be concluded as follows:

1. The Convolutional Neural Network (CNN) method requires computing time to insert messages in a secret image.
2. The model framework uses 2 (two) images with the aim of the cover image as input and the secret image where the secret image has been inserted a message so that the secret is not visible.
3. The cover image that has been inserted a secret picture that contains the message looks not much different, but the file size of the secret picture has increased by 66%.

Journal Publications & Informatics Engineering Research
Volume 4, Number 1, October 2019
DOI : https://doi.org/10.33395/sinkron.v4i1.10159
e-ISSN : 2541-2019
p-ISSN : 2541-044X

### 4.2 SUGESSTION

Some suggestions proposed for further research development are:

1. Test results on the secret image using 2 (two) proposed stages produce an increase of 66% compared to the original image, so that further research is needed to optimize the computational time.
2. In addition to the Convolutional Neural Network (CNN) approach, testing still needs to be done with other methods such as Generative-Adversarial-Networks

## VI. REFERENCES

Babaheidarian, Parisa, and Mark Wallace. *Decode and Transfer: A New Steganalysis Technique via Conditional Generative Adversarial Networks*. 2019, http://arxiv.org/abs/1901.09746.

Jamie Hayes and George Danezis "*Generating Steganographic images via adversarial training 2017*".

Zhang, Zhuo, et al. "*Generative Steganography by Sampling*." *IEEE Access*, 2019, pp. 1–1, doi:10.1109/access.2019.2920313.

S. Tan and B. Li, "*Stacked convolutional auto-encoders for steganalysis of digital images,"* Asia-Pacific Signal and Information Processing Association, 2014 Annual Summit and Conference (APSIPA), 2014, pp.1-4.

G. Xu, H. Z. Wu, and Y. Q. Shi, "*Structural design of convolutional neural networks for steganalysis*," IEEE Signal Processing Letters, 23(5):708712, 2016

S. Wu, S. Zhong, and Y. Liu, "*Deep residual learning for image steganalysis*," Multimedia Tools and Applications, pp. 1-17, 2017.

G. Xu, "*Deep convolutional neural network to detect J-UNIWARD*," arXiv:1704.08378, 2017.

Vojtech Holub and Jessica J. Fridrich "*Designing steganographic distortion using directional filters*". In WIFS, 2012.

Vojtech Holub, Jessica Fridrich, and Tomáš Denemark "*Universal distortion function for steganogra- phy in an arbitrary domain*" EURASIP Journal on Information Security, 2014(1):1–13, 2014.

Sari, Janer Irma, et al. "*Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB)*." *Jurnal Mantik Penusa*, vol. 1, no. 2, 2017, pp. 1–8, http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/253/156.

Abdul Kadir dan Adhi Susanto, "*Teori dan Aplikasi Pengolahan Citra*." Andi Yogyakarta, Yogyakarta, p.2, 2013.

Tomáš Pevny, Patrick Bas, and Jessica Fridrich "*Steganalysis by subtractive pixel adjacency matrix*" ` information Forensics and Security, IEEE Transactions on, 5(2):215–224, 2010.

Tomas Pevny, Tomas Filler, and Patrick Bas "*Using High-Dimensional Image Models to Perform Highly Undetectable Steganography*" In Information Hiding, pp. 2010, Calgary, Canada, June 2010. URL https://hal.archives-ouvertes.fr/hal-00541353.

Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan "*Deep learning for steganalysis via convolutional neural networks"* In SPIE/IS&T Electronic Imaging, pp. 94090J–94090J. International Society for Optics and Photonics, 2015b.

Lionel Pibre, Pasquet Jérôme, Dino Ienco, and Marc Chaumont "*Deep learning for steganalysis is better than a rich model with an ensemble classifier, and is natively robust to the cover sourcemis match*" arXiv preprint arXiv:1511.04855, 2015.