IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# IMAGE STEGANOGRAPHY USING CNN

Mr. Ch. Phanindra
Assistant Professor
Electronics and Communication Department
Nalla Narasimha Group of Institutions Hyderabad
Ghatkesar,India

G. Kavya
Electronics and Communication Department
Nalla Narasimha Group of Institutions Hyderabad
Ghatkesar,India

M. Nikhil
Electronics and communication Department
Nalla Narasimha Group of Institutions Hyderabad
Ghatkesar,India

K. Anjith Prasad Rao
Electrnoics and Communication Department
Nalla Narasimha Group of Institutions Hyderabad
Ghatkesar,India

**Abstract: -** These days the vast increase in the technology leads to the transmission of data over network channels which is not secure every time. So to solve this problem of security and privacy the method called Cryptography is introduced. Using this method the data to be transmitted is encrypted and given a key, to decrypt the transmitted data on the receiving end the user must give the appropriate key. If the key is given correctly the data cannot be retrieved. Even though this method provides security, due to the visibility of the encrypted data in the form of code causes suspicion and already available tools will try to exploit the privacy of data to be transmitted. To solve this problem, we propose a method called Steganography, in this we conceal and extract the information within the other data, often images after that the data will be invisible to human eyes. Now by adding the concept of Neural Networks to Steganography we can increase the capability to conceal the data, security during transmission and resistance to detect the data will be increased.

## I.INTRODUCTION

In this method the non-secret data is used to conceal the secret data within it and in such a way that the the secret data will be invisible to human eyes. This method is called Steganography. The term Steganography is the combination of two Greek words “Steganos” which means conceal or cover and “Graphia” which means Writting. The main objective of this project is to conceal a message’s existence in a way that prevents unauthorized parties or unintended receivers from noticing it. It is mainly used to secure secret data by cover the sensitive data within the innocent carriers, such as images, audio files, video clips, or even text pages. The concealing of data can be done in various techniques. One such technique involves changing of the least important digital assets of an image or an audio file to embedd or encode the secret information. The non-secret images seems to be unchanged since the changes are made in such a way that it is invisible to human eyes, because the least important parts are changed the properties of the non-secret data will not be visible. Steganography can be used for both good and bad intentions.

The process of detecting the hidden information is called “steganalyis”. This can be implemented efficiently using different algorithms. Since the machine learning algorithms work too effectively when working on larger data, Convolutional Neural Networks are used in our project.

## II.LIRATURE SURVEY

"CNN in image steganography” This survey provides an extensive examination of the integration of Convolutional Neural Networks (CNN) in the field of image steganography. It delves into the various CNN-based steganographic methods, their applications, and the challenges associated with embedding and extracting hidden data within images. This survey serves as a foundational resource for understanding the role of CNN in image steganography.

"Deep Learning Approaches for secure image hiding and extraction" This literature survey focuses on the deep learning approaches, particularly CNN, utilized for secure image hiding and extraction in the domain of steganography. It reviews state-of-the-art techniques, algorithms, and models that employ CNN to ensure the secrecy and robustness of hidden information within images. The survey offers insights

into the cutting-edge developments in deep learning-based image steganography.

"Adversarial attacks and defence in CNN based image steganography" This survey addresses the realm of adversarial attacks and defenses within CNN- based image steganography. It explores the vulnerabilities of steganographic models and the countermeasures designed to protect hidden information from detection and extraction. The survey provides a comprehensive perspective on the adversarial dynamics in this field.

“Embedding Capacity and Data Security in CNN based image steganography" This literature survey investigates the embedding capacity and data security aspects in CNN-based image steganography techniques. It discusses the trade-offs between the amount of hidden data and the security of the steganographic process, as well as the methods that balance these factors. The survey offers valuable insights into optimizing data capacity and security in CNN-based steganography.

## III.PROBLEM STATEMENT

Due to the increase in the transmission of data over insecure network channels the privacy of the data will be exploited. To solve the that we introduce image steganography, by which the data to be transmitted will be securely transmitted due to its invisible nature.

## IV.EXISTING METHOD

Conventionally, Least Significant Bits (LSB) substitution method is employed to perform image steganography. Images are usually of higher pixel quality, out of which not all the pixels are used. LSB methods works under the assumption that changing the least important pixel values would not show any visible changes. The secret information is converted into a binary form. The non secret image is scanned to determine the least significant bits in the noisy area. The binary bits from the secret image are then substituted in the LSBs of the non secret image. The substitution method has to be performed cautiously as overloading the cover image may lead to visible changes leaking the presence of the secret information. So it has less capacity to hide or conceal the information.

## V.PROPOSED METHOD

Image steganography using CNN models is heavily inspired from the encoder-decoder architecture. Two inputs – cover image and the secret image are fed as the input to the encoder to generate the stego image and the stego image is given as input to the decoder to output the embedded secret image. The basic principle is the same except different methods uses different architectures. The way the input cover image and the secret image are concatenated are also different in different approaches while the variations in the convolutional layer, pooling layer are expected. The number of filters used, strides, filter size, activation function used and loss function vary from method to method. One important point to note here is the size of the cover image and the secret image has to be same, so every pixel of the secret image is distributed in the cover image.

### Objectives

The main objective of the project is to hide image using CNN so that it is not detectable by unauthorized person.

To protect the confidentiality of the hidden image by making it difficult for unauthorized individuals to access or extract the information.

To extract hidden image from a given cover image using neural networks.

To Create and put into use a steganography system based on CNN.

To analyze the CNN-based steganography system’s performance in terms of image quality, hiding capacity, and resistance to steganalysis attacks.

## V.METHODOLOGY

The architecture of the system will consist of three components trained as a single network; however, it is easiest to describe them individually. The cover image and secret message for the hidden network are created by the prep network. The cover image and secret message are inputs, and the program outputs a preprocessed version of the cover image. The secret message and the preprocessed image are then sent across the concealed network.

The second/main network, the Hiding Network, takes as input the output of the preparation-network and the cover image, and creates the Container image. The secret message is concealed in the pre-processed cover image using the hidden network. It generates a stego image from the inputs of the secret message and the preprocessed cover image. The stego image should look identical to the cover image and also havethe secret message hidden within. The hidden network’s architecture is created to strike a balance between reducing the distortion of the cover image and increasing the hidden message’s capacity.

Finally, the right-most network, the Reveal Network, is used by the receiver of the image. The concealed secret message in the stego image must be extracted via the reveal network. It produces the concealed secret message as an output and accepts the stegoimage as input. Recovering the secret message from the stego image accurately while reducing false positives is the goal of the reveal network’s architecture.

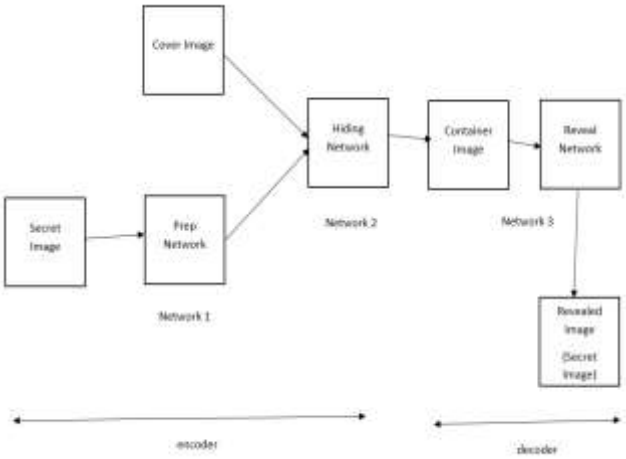


Fig 5.1 Block Diagram

## VI.IMPLEMENTATION

The user interface as shown in figure 2 of the steganography using CNN project is designed to be user-friendly and easy to navigate. It consists of a simple GUI that allows users to perform various operations related to steganography.
The main window of the interface consists of four buttons: Generate & Load Encoder-Decoder Model, Upload Cover Image, Upload Secret Image, Run Encoder_Decoder Steganography, Exit.
The button in the Interface the Encoder-Decoder Model is Generated as per the code given in the Encoder-Decoder file. This button in the Interface the cover image is uploaded which is an input in which the secret message is to be embedded. This button in the Interface the secret image is uploaded which is an input which is pre-processed and then secret message is to be embedded in the cover image. At the

end the exit button is used to clear all the results and exit the GUI Window.

Fig 6.1 GUI Window

## VII.RESULT

The results of the project shows the demonstration of the Image Steganography with encoder and decoder algorithm using Convolutional Neural Networks and four output images will be displayed secret, cover, stego and revealed images.

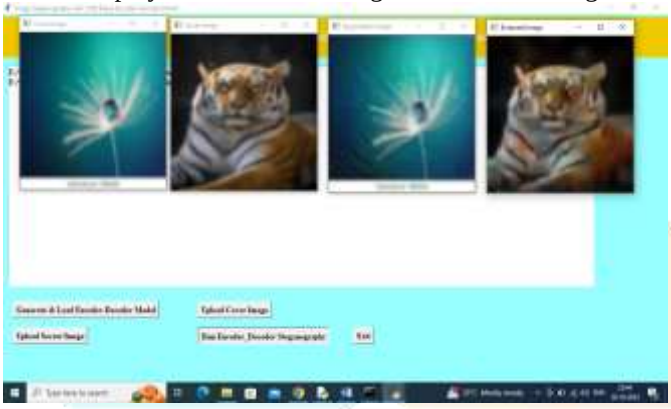

Fig. 7.1 Output Screen 1

## VIII. CONCLUSION

The networks which performs the operation of encoding and decoding are constructed and are performing well. Even though it has shown good performance encoding and decoding, it is not a full proof system as every technology has its shortcomings.

## IX.FUTURE SCOPE

As stated in the disadvantages, there is a lot of scope of improvement in this project as there is a chance that networks can be trained specifically for detecting that an image has been hidden inside a given image.

This project can be improved upon by creating a better architecture or by altering the architecture of this network and improving its performance further, making the secret image tougher to decode by any program other than the decoder and to make it more difficult to detect the presence of any secret image inside the encoded.

## REFERENCES

[1] H. Kato, K. Osuge, S. Haruta and I. Sasase, "A Preprocessing by Using Multiple Steganography for Intentional Image Downsampling on CNN-Based Steganalysis," in IEEE Access, vol. 8, pp. 195578- 195593, 2020, doi: 10.1109/ACCESS.2020.3033814.

[2] Jin, Z., Yang, Y., Chen, Y. and Chen, Y., 2020. IAS-CNN: Image adaptive steganalysis via convolutional neural network combined with selection channel. International Journal of Distributed Sensor Networks, 16(3), p.1550147720911002.

[3] Xiang, Z., Sang, J., Zhang, Q., Cai, B., Xia, X. and Wu, W., 2020. A new convolutional neural network-based steganalysis method for content-adaptive image steganography in the spatial domain. IEEE Access, 8, pp.47013-47020.

[4] Duan, X., Liu, N., Gou, M., Wang, W. and Qin, C., 2020. SteganoCNN: Image Steganography with Generalization Ability Based on Convolutional Neural Network. Entropy, 22(10), p.1140.

[5] Duan, X., Guo, D., Liu, N., Li, B., Gou, M. and Qin, C., 2020. A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access, 8, pp.25777-25788.

[6] Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., Xian, Y. and Shi, Y., 2020. A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks. IEEE Access, 8, pp.168166- 168176. [7] Tang, W., Li, B., Tan, S., Barni, M. and Huang, J., 2019. CNN-based adversarial embedding for image steganography. IEEE Transactions on Information Forensics and Security, 14(8), pp.2074-2087.

[8] Yu, X., Tan, H., Liang, H., Li, C.T. and Liao, G., 2018, December. A multi-task learning CNN for image steganalysis. In 2018 IEEE International Workshop on information forensics and security (WIFS) (pp. 1-7). IEEE.

[9] Yuan, Y., Lu, W., Feng, B. and Weng, J., 2017, June. Steganalysis with CNN using multi-channels filtered residuals. In International Conference on Cloud Computing and Security (pp. 110-120). Springer, Cham.

[10] Duan, X., Guo, D., Liu, N., Li, B., Gou, M. and Qin, C., 2020. A new high-capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access, 8, pp.25777-25788.