

Steganography using Deep Learning

Banjot Singh Kullar (21BCE5169), Ayush Pathak(21BCE5322), Shekhar Chhaba (21BCE6008)(21BCE6008) and Anmol Sehgal (21BCE5984)

GITHUB LINKS:

21BCE5322 Ayush Pathak

21BCE5984 Anmol Sehgal

21BCE6008 Shekhar Chabba <https://github.com/Shekhar-2309/DIP>

21BCE5169 Banjot Singh Kullar

***Abstract- For safe information transfer, steganography has long been a necessary technology, particularly in contemporary communication when information privacy is of utmost importance. Image-to-image steganography has gained popularity as digital media has grown because it integrates easily into a wide range of platforms and applications. Although it is commonly employed, the Least Significant Bit (LSB) method, one of the basic techniques for image-image, and text-image steganography, is neither very secure nor imperceptible. Therefore, it's now essential to investigate more sophisticated methods.***

***This study explores the application of Convolutional Neural Networks (CNNs) in Deep Learning (DL) to improve the security and performance of image-to-image steganography. Our technique seeks to provide high imperceptibility and resilience against steganalysis while encoding and decoding hidden information in pictures by utilizing CNNs. To assess the state-of-the-art in this field, a thorough literature study was carried out, with a particular emphasis on different DL models such as CNNs and Generative Adversarial Networks (GANs).***

***The main objective of this work is to present a new technique for secret message transmission that combines DL with image-to-image steganography, making it more effective and safe. The objective is to showcase the latest developments in the field and illustrate how DL models may improve image-to-image and text-image steganography performance. The research findings will aid in the creation of more complex and safe digital environment communication systems.***

**I. Introduction**

In today's landscape of information security and multimedia, the protection of confidential data has become increasingly critical due to escalating security threats in areas such as personal privacy, trade secrets, and national security. Information steganography has emerged as a crucial field of study aimed at addressing these challenges by enabling the covert embedding of sensitive information within benign digital images, referred to as steganographic images or stegos. This method ensures secure data transmission by concealing critical data while rendering it undetectable to unintended observers.

Historically, conventional image steganography methodologies have relied on techniques like Least Significant Bit (LSB) embedding, HUGO, and transform domain-based approaches such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). These techniques have been utilized to hide data within images while balancing considerations of security, data capacity, and imperceptibility.

Security concerns in steganography primarily center around the threat of unauthorized access and detection of concealed information by malicious entities. Traditional steganographic methods face challenges in ensuring robust security and imperceptibility, as advancements in steganalysis techniques have raised the bar for effective data concealment. Adversaries may utilize sophisticated algorithms to analyze steganographic images and uncover hidden information, posing risks to the confidentiality and integrity of sensitive data.

The incorporation of Convolutional Neural Networks (CNN) in image steganography offers a promising avenue to bolster security and address concerns related to data concealment. By leveraging CNNs, researchers can develop advanced embedding techniques that enhance the efficacy of concealing information within images while preserving imperceptibility. CNNs possess the capability to understand intricate patterns and structures in images, facilitating the creation of steganographic systems that are resilient to detection by steganalysis techniques.

Utilizing CNNs, image steganography can elevate security levels by integrating sophisticated encryption and embedding algorithms that thwart detection efforts. CNNs enable the generation of steganographic images that seamlessly blend with unaltered images, ensuring imperceptibility while safeguarding sensitive information. Furthermore, CNN-based steganographic systems can adapt to evolving threats, fortifying the overall resilience of information concealment mechanisms.

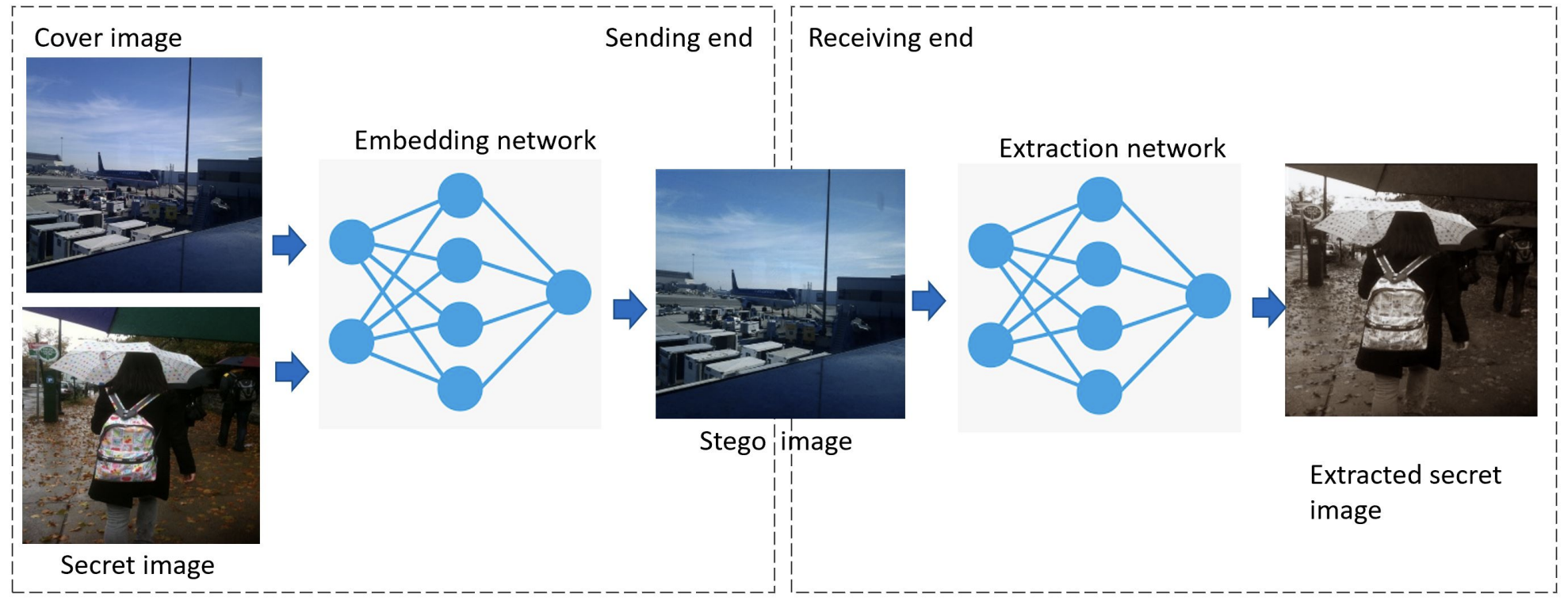


Figure 1. The overall block-diagram of the proposed image steganography scheme.

**2. Related Work**

This section is intended to provide a literature review of some of the numerous digital image steganography methods. There are three main categories that image steganography techniques fall under, which are spatial domain techniques, transform domain techniques, and neural networks.. It should be noted, however, that image steganography techniques may fall into several categories by using a combination of different techniques.

*2.1 Steganography using Combined DCT, ECC, and SegNet CNN Approach*

The authors in this study [1] devised a novel approach by utilizing a combination of the Discrete Cosine Transform (DCT), Image Elliptic Curve Cryptography (ECC), and the SegNet Convolutional Neural Network (CNN) to achieve a hiding capacity of around 23 bits per pixel (bpp). ECC, an asymmetric encryption algorithm commonly employed in security applications like the Diffie-Hellman key exchange, played a crucial role in this technique. Their method employed a network architecture similar to a previous study, incorporating a pre-processing network, an encoding network, and a decoding network to facilitate steganography. The pre-processing network was responsible for normalizing the secret image and extracting significant features through DCT and ECC processes to yield a secret image and an encrypted image. Subsequently, the encoding network was tasked with aligning the hidden and cover images to the same dimensions and embedding the hidden image within the cover image. Finally, the decoding network was utilized to extract the hidden image from the cover image, resulting in the generation of the steganographic image. To retrieve the original hidden information, one would need to decrypt the steganographic image further using inverse DCT and ECC techniques.

2.2 Text in image steganography

In this study [4] we have text in image steganography, the format and encoding of the text is altered to make it hide more efficiently. The task can be achieved by various methods some of which are namely,Random generation method, Linguistic and format based method. Different coding techniques are implemented

2.2.1

Line shift coding

In this study [4]the technique is used to modify the text by shifting the lines vertically. The shifting of lines led to a specific pattern in the text which is used to generate a cover text. Shifting is incorporated by moving the lines of the plain text by some degree in the vertical direction. Bits like 0, 1 and -1 can be used to denote the unmoved, shifted up and shifted down lines. At the decoders end either baseline shifting is found or the centroid shifting is found. Baseline shifting includes the hidden message in the baseline of the adjacent lines in text. If centroid shifting is done then the decoder searches for the hidden message in the centroids of the adjacent lines of the cover text.

2.2.2

Word shift coding

In this work[4] method introduces the idea of shifting the words of the text in a horizontal manner to hide a meaningful message. The distance in between the words is altered so that information is hidden. The spaces within the words should be different in order to generate a cover text. The decoder should also know about how to shift the words to extract a message hidden using steganography. If there are variable places involving the word shifting method then the decoder should be given the original text so that detection of correct information at the decoder's end is possible.

2.2.3

Feature encoding

The feature encoding deals with the change in the features of the text in such a manner that a meaningful message is hidden to produce a cover text. Features like height of the text, color of the text, font of the text are some of the ways which are used.

2.3.1

**Training Image Processing Generation Model**

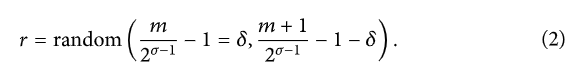
First, (referencing [7]) the image processing generation model needs to be trained in order to put our idea of embedding hidden information during image processing into practice. Two sophisticated GAN variants, DCGAN and WGAN-GP, are utilized in this model. Two processed image sets are produced from the original image set by applying histogram equalization and sharpening procedures prior to starting the training of the generation model. The DCGAN and WGAN-GP models are then trained independently using these two processed image sets, and the training procedure is continued until both models converge and generate high-quality images.

2.3.2 **Training the Extraction Model**

The extraction model's objective is to extract the noise vector from the stego image that has been processed by the generation model and then use pre-established mapping methods to reassemble the hidden data. As seen, the extraction model's architecture, which combines fully connected and convolutional neural networks, is quite similar to that of the discriminator D in DCGAN [33]. Each layer of the extraction model's convolutional neural network includes batch normalization and a Leaky ReLU activation function to improve nonlinear learning capabilities and hasten network convergence. The network's output layer function is set to tanh in order to guarantee that the extraction model's output noise values lie between -1 and 1.

2.3.3 **Communication of Secret Information**

As in reference [7], the sender splits up the secret information into segments and applies rules to map each segment to a noise vector.

**** As a result, secret information is mapped to noise values within a given interval, and these noise values are used to generate processed stego images, which are then sent to the receiver, who uses a trained extraction model to retrieve the noise vectors and reverse-maps them to restore the original secret information, allowing for a small amount of deviation. The extraction process is based on Formula (2) and its parameters.

##### 2.4 Steganography techniques that are based on traditional methods

##### In the work[11]Image steganography is traditionally done using the Least Significant Bits (LSB) substitution method. The pixel quality of images is normally higher, but not all of the pixels are used. The LSB approach is based on the notion that changing a few pixel values will not result in noticeable changes. The secret data is transformed into a binary format. The least significant bits in the noisy area are determined by scanning the cover image. The LSBs of the cover picture are then replaced with the binary bits from the secret image. The substitute approach must be used with caution, as overloading the cover picture may result in noticeable alterations that reveal the secret information's presence.

2.5 StegNet: Mega Image Steganography Capacity with Deep Convolutional Network

This paper [14] combines recent deep convolutional neural network methods with image-into-image steganography. It successfully hides the same size images with a decoding rate of 98.2% or bpp (bits per pixel) of 23.57 by changing only 0.76% of the cover image on average

2.6 Image Steganography: A Review of the Recent Advances

The main goal of this paper [15] is to explore and discuss various deep learning methods available in image steganography field. Deep learning techniques used for image steganography can be broadly divided into three categories - traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods. Along with the methodology, an elaborate summary on the datasets used, experimental set-ups considered and the evaluation metrics commonly used are described in this paper

**III. Proposed Method**

Instead of using the classical data concealment algorithms such as LSB substitution algorithm and its improved versions, the authors in [5] proposed an image steganographic model that uses deep learning based on generic encoder-decoder architecture. The location where to hide data is selected by ingenious networks of neurons; the network structure of this deep model is composed of three sub-networks: Pre-network, Hiding network and Reveal network. CNN layers are used to learn the hierarchy of image features, a hierarchy ranging from low-level generic features to high-level specific features. Thus, the encoder network learns the features of the two images which allows it to hide the details of the image to be hidden in the features of the cover image. In other words, the objective is to compress and distribute the bits of the secret image on all the bits available on the cover image.

**Hiding network Architecture**

The encoder network of our method is designed as a plain network receiving as input the cover image and the secret image, both are concatenated into a 6-channel tensor. It is made up of two phases. The first phase of the network is designed with a sequence of 3 x 3 convolution layers, each convolution is followed by a BN operation

to accelerate learning and a ReLU activation function.

**Reveal network Architecture**

The reveal network is also designed as a plain network, it receives as input the stego image produced by the encoding network. We apply to this image a sequence of layers of 3 x 3 convolution; each convolution is followed by a BN operation to accelerate the training and a ReLU activation function. But, in the last layer, a Sigmoid activation is applied to compress the convoluted features channels into 3-channel features to calculate the secret image (output).

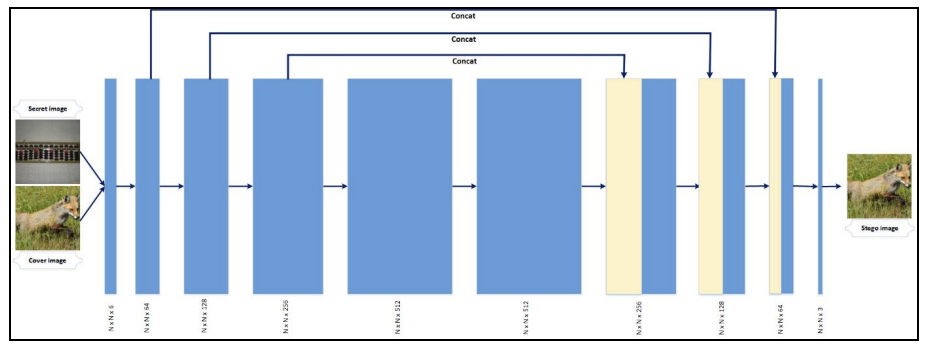


Fig : Hiding network Scheme

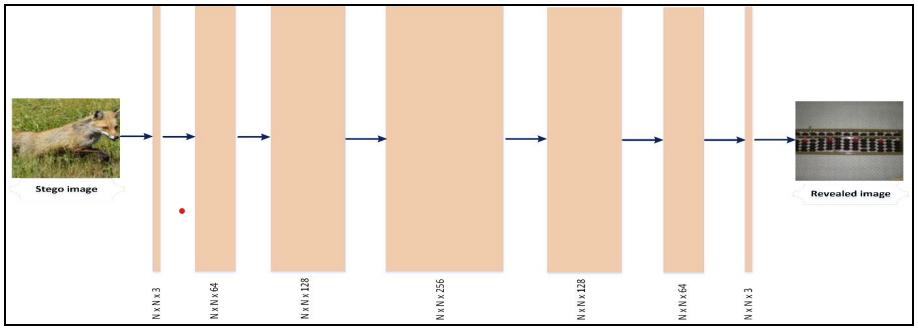


Fig : Reveal Network Scheme

**IV. Dataset**

For the scope of this project we will be using the dataset Linnaeus 5. Linnaeus 5 is a dataset that contains 6000 square images of five different types of objects. The images in the Linnaeus 5 dataset are saved in a JPG format, with each image having a height and width of 256 pixels.

The link for the dataset is <https://chaladze.com/l5/#:~:text=Overview&text=Images%20are%20256x256%20pixels%2C%20color,400%20test%20images%20per%20class>.

**References**

[1] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, "A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," *IEEE Access,* pp. 25777-25788, 2020.

[2] Nandhini Subramanian, Ismahane Cheheb, Omar Elhlarrouss, Somaya Al-Maadeed, Ahmed Bouridane, “End-to-End Image Steganography Using Deep Convolutional Autoencoders,”*10.1109/ACCESS.2021.3113953, IEEE Access*

[3]Akram Abdel Qader and Fadel AlTamimi, “A novel image steganography approach using multi-layers discrete cosine transform (DCT) features based on support vector machine (SVM) classifier,”The International Journal of Multimedia & Its Applications (IJMA) Vol.9, No.1, February 2017

[4] Vijay Kumar\* , Saloni Laddha, Aniket, Nitin Dogra “steganography, Convolutional Neural Network (CNN), Rectifier Linear Unit (ReLU)” 20 August 2020

[5] Ismail Kich 1 , El Bachir Ameur1 , Youssef Taouil1 , Amine Benhfid1 ”Image Steganography by Deep CNN Auto-Encoder Networks” Volume 9,No 4 July - August 2020

[6] Seyed Hesam Odin Hashemi, Mohammad-Hassan Majidi\* , Saeed Khorashadizadeh “Image steganography, Deep neural networks, Autoencoder, ResNet”

[7] Mingjie Li , Zichi Wang, Haoxian Song, and Yong Liu :

[8] Ofoegbu, C. I. a\* , Nwokorie, E. C. a , Onyemauche, U.C. a , Okolie S. A a , Amadi, C.O “Image steganography, Deep neural networks, Autoencoder, ResNet, CIFAR dataset”

[9] Zhangjie Fu1,2, Fan Wang1 and Xu Cheng1\* “Steganography, Information hiding, Generative adversarial networks, Deep learning”

[10] B. Li, M. Wang, J. Huang, and X. Li, “A new cost function for spatial image steganography,” in *Proceedings of the Image Processing (ICIP) 2014 IEEE International Conference on 2014*, pp. 4206–4210, IEEE, Paris, France, October,2014.

[11] Shourya Chambial1, Dhruv Sood “IMAGE STEGANOGRAPHY USING CNN “ International Research Journal of Engineering and Technology (IRJET) Volume: 09 Issue: 02 | Feb 2022

[12] Pin Wu1 , Yang Yang1 , and Xiaoqiang Li1,

“Image-into-Image Steganography Using Deep Convolutional Network” (2017).

[13] Vijay Kumar\* , Pankaj Rao, Ashish Choudhary “Image Steganography Analysis Based on Deep Learning” Vol. 7, No. 1, March, 2020

[14] Pin Wu 1,Yang Yang 1 andXiaoqiang Li 1,2,\* “[**convolutional neural network**](https://www.mdpi.com/search?q=convolutional+neural+network); [**image steganography**](https://www.mdpi.com/search?q=image+steganography); [**steganography capacity**](https://www.mdpi.com/search?q=steganography+capacity)”

[15] NANDHINI SUBRAMANIAN 1 , (Member, IEEE), OMAR ELHARROUSS1 , SOMAYA AL-MAADEED 1 , (Senior Member, IEEE), AND AHMED BOURIDANE 2 , (Senior Member, IEEE)

“Image steganography, GAN steganography, CNN steganography, information hiding, image data hiding. ”