The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 10, October 2025
PP 135-150

Deep Learning in Steganography and Steganalysis

Bashar M. Nema[1] , Asraa S.Ahmed[2*]
[1] Mustansiriyah University, College of Science, Iraq, bashar_sh77@uomustansiriyah.edu.iq
[2] Department of Computer Sciences, College of Science, Diyala University, Diyala, Iraq.
Corresponding Author *: asraasafaa@uodiyala.edu.iq

Abstract

Steganography can be defined as a practice of concealing messages in an item that is referred to as carrier for the purpose of building a covert channel of communications where the act of communication itself is undetectable by observers with access to the channel. Steganalysis allows for discovery of hidden messages in a variety of media, including digital pictures, video les, audio _les, and plain text. The evolution of deep convolutional neural networks (DCNNs) has aided steganography and steganalysis tremendously in recent years. In the present publication, we examined current study findings from the most recent deep learning-based picture steganography and steganalysis frameworks. Our goal is to give future researchers with information on the work that is performed on the deep learning-based picture steganography and steganalysis, as well as strengths and weaknesses of current techniques. The findings of this work offer up new avenues for future research and might serve as a starting point for more substantial researches on deep learning-based picture steganography and steganalysis. Finally, technical problems of present approaches are discussed, as well as some interesting possibilities in deep learning steganography and steganalysis, to show how those obstacles might be translated to lucrative future research fields.

Keywords: Convolutional neural networks, Steganalysis, Steganography, Deep Learning.

1. Introduction

With an advent of information era, more and more people utilize mobile devices for communication, working and creation. It has brought a high level of convenience into people's lives and work. However, increasing problems of safety have been exposed. For instance, the personal privacy undergoes snooping, spreading, copyrighted ownerships, stolen works, etc. In solving such type of problems, the information hiding was given much attention for the protection of the copyright and privacy. Information hiding indicates the fact that the private information has been hidden in a cover image with the use of some cover image properties, and in the procedure of transmitting the cover image, no anomalies have been found by detectors, thus, stego image may be transmitted safely to receiver [1].

To achieve secret communication, the receiver extracts the secret information using a specific algorithm. Secret information might take the shape of a piece of text, a picture, or other media. The most common way of concealment is to transform secret information to a bit stream and then hide bit information in the cover file. Furthermore, the picture may be hidden directly in a different image, or secret information may be linked to mapping dictionary, with mapping objects being broadcast to recipient [2]. Steganography can be defined as a type of secret communications that is extremely important in military and national security matters. On the other hand, although steganography has been utilized by the individuals with good intents to protect network communication security, it is also utilized by those with bad motives. Actually, information hiding was utilized as well in the terrorist attacks, espionage, crime and other activities in the past years. In those conditions, military and security organizations in numerous nations are grappling with how to properly oversee steganography and prevent and stop its malevolent or unlawful deployment. As a result, steganalysis was commonly utilized in information hiding development. Steganalysis can be defined as the process where a detector determines whether or not a stego image includes private information after the publishing of stego image. Steganalysis and Steganography are 2 types of algorithms restricting one another and opposing one another as shown in Figure (1) [1].

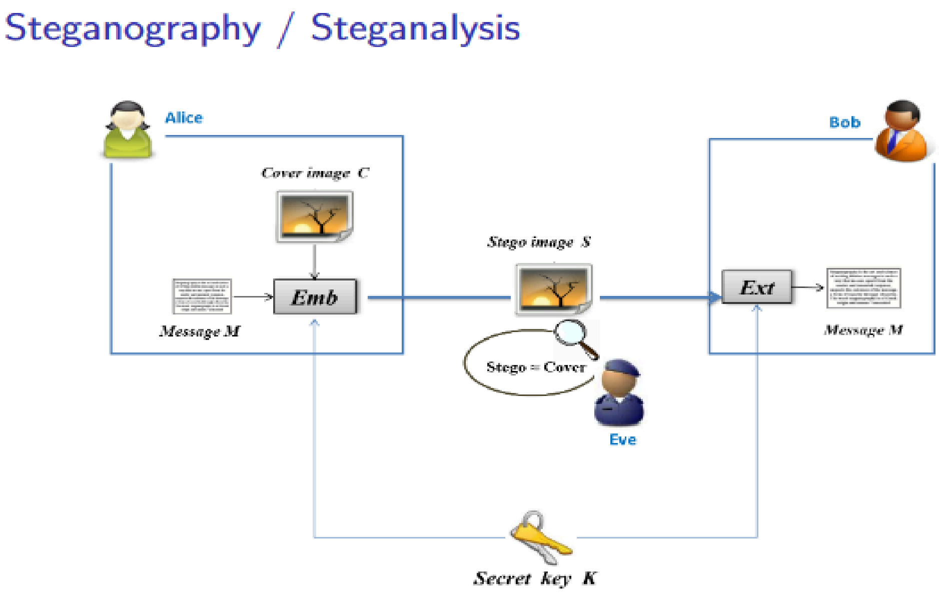

Fig 1. Steganography & Steganalysis [2]

2. Related works

2.1 Steganographic algorithms based on deep learning

In Baluja, S. (2017) [3], discussed placing a full-size colored image within a different image that has an identical size. The DNNs are trained simultaneously for the creation of the processes of hiding and revealing and have been designed for the purpose of specifically working as pair. The paper by (Baluja, 2017) talks about the way a trained system should learn compressing information from a private image within least noticeable cover image portions. However, there has been no clear attempt to purposefully disguise the existence of that data from machine detection. They used unaltered ImageNet pictures as negative examples and their containers as positive examples to train steganalysis networks as binary classifiers. The paper serves a baseline for single secret image encoding. However, it does not talk about multi-image steganography.

In Zi, H., Zhang, Q., Yang, J., & Kang, X. (2018, November) [4], suggested model is capable of generating images that are more visually convincing with a lower collapse of the model. From the comparative experimentations, it was proven that images that have been generated are of a higher security towards the steganalysis in comparison with the ones that have been produced by previously established GAN-based approaches

In Kreuk, F., Adi, Y., Raj, B., Singh, R., and Keshet, J. (2019) [5], explored the use of DNNs as steganography functions for the speech data. Which is why, they have proposed jointly optimizing 2 NNs: the first one encodes message within the carrier, whereas the other one network performs the decoding of that message from modified carrier. They have shown that this approach was effective on a number of the speech data-sets and they have also analyzed results qualitatively as well as quantitatively. In addition to that, they have shown that their method might be implemented for concealing several messages in one carrier with the use of several of the decoders or only one conditional decoder. The qualitative experiments have suggested that the modifications that have been made to carrier aren't noticeable by the human listeners and that decoded messages are quite intelligible. This paper demonstrates the capability to hide a number of the secret messages in one carrier, which aligned with their goals. In the paper, five independent speech messages have been hidden in a single speech recording. This is achieved by 2 different approaches. One approach utilizes multiple decoders, with each decoder trained to decode a different message. The other approach utilizes a conditional decoder that also takes in as input a code indicating the message index to be encoded.

Shang, Y., et al. (2020) [6], suggested an innovative approach that improves security of the DL-based steganographic approach. They have benefitted from behaviors of linear state-of-the-art CNN-based stego-analyzer and used adversarial examples' approaches for the purpose of preventing the stego from being detected. They've proven their model's effectiveness through the implementation of a variety of the experimentations. They discovered as well, single adversarial perturbation antagonism, as a result of the generation procedure. Distortion of the stego images that are produced through using adversarial approach has been assessed with the use of the PSNR and MSE. None-the-less, in the conventional steganographic approach, those indicators have not been quite sensitive to the localized distortion cases, those distortions might result in very good indicator values, however, distortions might as well get visible in stego. A different direction of the study might result in further reducing the adversarial perturbation distortion to the secret. There is an aim for investigating the likelihood of checking the post silicon technologies in which information security is an open issue; nano-fluidics and micro-fluidics device-based networks, using rather different hardware face similar issues as regards security of conventional ones.

In Koptyra, K., & Ogiela, M. R. (2020) [7], showed the way for diffusing a message then hiding it within a number of the PDF files. Their suggested approach used the de-referenced objects and secret sharing or splitting algorithms. It has been applicable to a variety of PDF file types, which include the presentations, text documents, scanned images, and so on. Due to the fact that the hiding procedure has been based upon the manipulation of the structure, the solution could be combined easily with the content-dependent steganography approaches. Hidden pages are invisible in the usual application utilization that has been tested with 7 separate programs. The PDF files were selected to the present study due to their extensive utilization use in the Internet, making them very good steganography media. The results that have been obtained had encouraged conducting more researches in this field. Future projects could be concerning new approaches of the distributed steganography in the PDF files, which incorporated cryptography as well as other security means.

Das, A., Anand, M., Wahi, J. S., and Rana, Y. (2021) [8], was utilizing the DNNs to encode and decode several private images within one cover image that has an identical resolution. perform multi-image steganography, hiding three or more images in a single cover image. The embedded secret images must be retrievable with minimum loss. The encoded cover image must look like the original cover image. To perform this, combine the idea of (Baluja, 2017) and (Kreuk et al., 2019). We take the network implementation idea of having a prep and hiding network as an encoder and a reveal network as a decoder from (Baluja, 2017). To extend this for multiple images, we pass multiple secret images via the prep network and then concatenating these resulting data with the carrier image and then finally send his via the Hiding network. We then take the idea of having multiple decoders, one per secret image, from (Kreuk et al.,2019) for retrieving all secret images from the container image. To improve security of our image retrieval model, we extend the idea presented by (Baluja, 2017) of putting secret images with noise in the original cover image instead of putting the secret images at the LSBs of the original cover image.

2.2 Steganalysis approaches that are based upon the DL

Tan & Li et al. 2014 [9], proposed first CNN structure for steganalysis of digital images in spatial domain. Although proposed model is performing better than the SPAM, but still inferior to SRM. The network is not enough deeper with only three convolutional layers and quite slow because of too large fully connected layer. Their proposed network acquired error rate of 48% with random parameter initialization against detecting HUGO at embedding rate of 0.4bpp.

Xu-NetV1 et al. 2016 [9], proposed the first deep learning framework achieved competitive performance compared with SRM [24]. In their proposed network, they used an absolute ABS activation layer for feature map generated from first convolutional layer. It can learn more resultful features that might be helpful to avoid overfitting problems. They also used BN (batch normalization) and pooling layers in their network and achieved better accuracy to SRM.

In, LU JICANG et al. 2019 [11], proposed an improved steganalysis framework based on feature selection & pre-classification techniques. First the author applies k-means algorithm to image dataset to extract images with different texture and complexities then optimal features for each cluster are selected for final decision which might improve overall performance of the stenanalysis schemes.

In Yinlong Qian et al 2015 [12], proposed a customized deep model called GNCNN for steganalysis. The proposed model can capture the complex dependencies that are useful for steganalysis, and learn feature representations with several convolutional layers. As the network goes deeper, more complex dependencies are modeled by progressively involving large input regions. Hence, higher level features are obtained. Additionally, both feature extraction and classification are unified under a single network architecture which manages to utilize the guidance of classification by jointly optimizing all the parameters.

3. Theoretical Background

3.1 Steganography

It's the art of concealing hidden messages in cover pictures by gently altering pixel values that look normal to the untrained eye. Steganography, like cryptography, is a technique for secret communication. The cryptography approach, on the other hand, is concerned with the communications' validity and integrity as shown in Figure 2, and Table (1) [13].

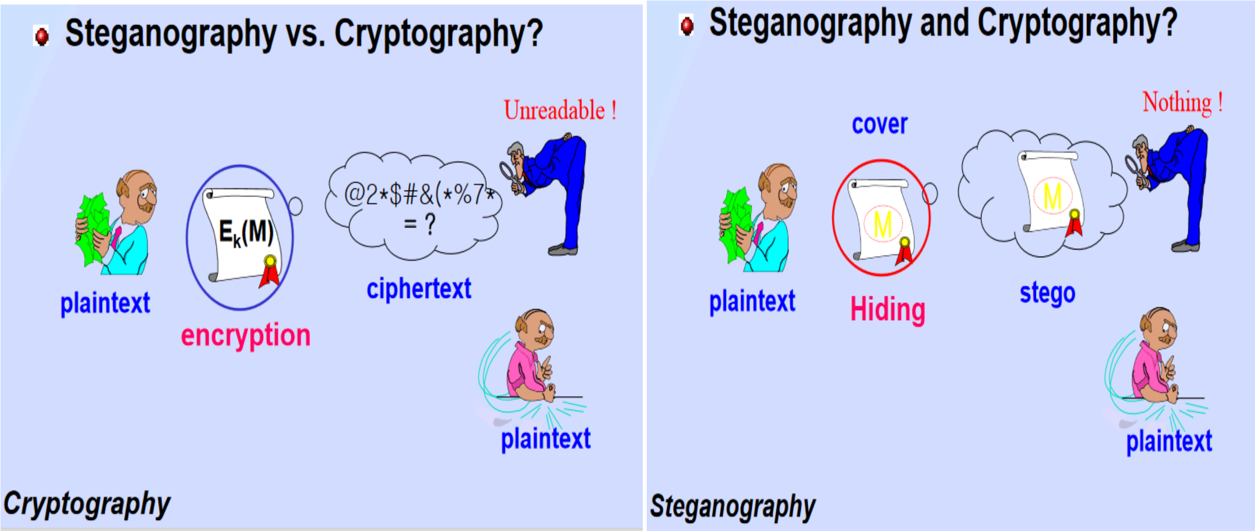

Fig 2. Steganography VS Cryptography

Table 1: Comparison Between Steganography VS Cryptography [14]

Sr. No.	Key	Steganography	Cryptography
1	Type	Steganography refers to Cover Writing.	Cryptography refers to Secret Writing.
2	Popularity	Steganography is less popular than Cryptography.	Cryptography is more popular than Steganography.
3	Integrity	Structure of data remains same.	Structure of data can be altered.
4	Attack	Attack in Steganography is termed as Steganalysis.	Attack in Cryptography is termed as Cryptanalysis.
5	Security Principles	Steganography supports Confidentiality and Authentication.	Cryptography supports Confidentiality, Authentication, Data integrity and Non-repudiation.
6	Parameter	Steganography requires a parameter like key.	Cryptography may not need any key.

The fundamental aim of the steganography approach is hiding the fact that a secret exists. Big surveillance operations had shown that even in the case where content is not known, the presence of the normal data communications could result in the leakage of the privacy. Which is why, steganography is important for the secret communications [14].

Watermarks, copyright protection, and secret communication might all benefit from steganography approaches. Typically, the sender employs a steganography technique for concealing the secret message within a cover, leaving it unaffected by external detectors. The fundamental effort in the steganography is the minimization of interferences in a cover image in the case where a secret has been embedded while permitting recovery of a private message. Then a steganographic image that has been known as the stego has been transmitted in the public channels. On the other side, the receiver receives the stego and uses the decoding algorithm and the shared key for the extraction of a private message as shown in Figure (3) [15].

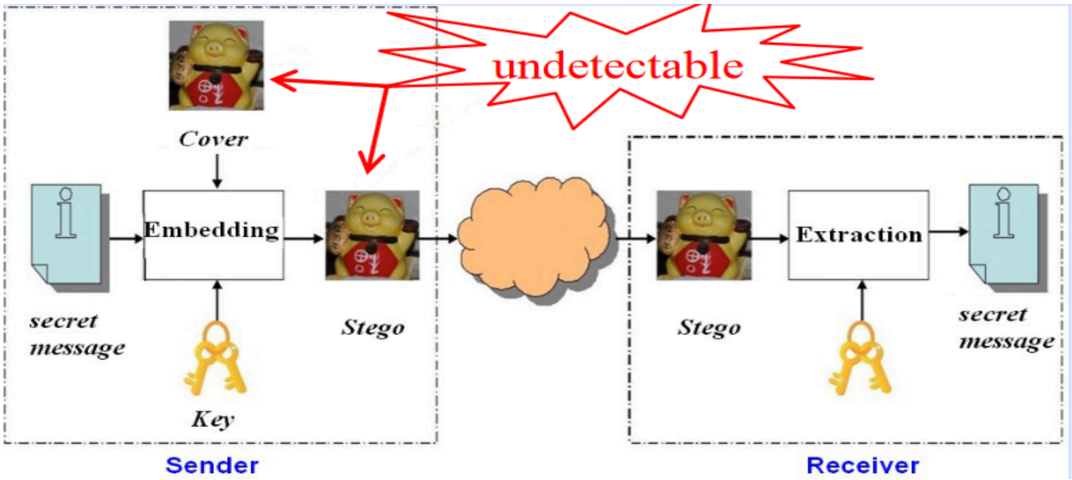

Fig 3. Embedding and Extraction of the Secret Message

With fast advancement of the field of deep learning (DL), the modification of an image turns considerably easier and automatic in the steganography. The available approaches of steganography might be divided to 2 classes, which are: STC based content-adaptive steganography and DL-based automatic steganography. Syndrome-Trellis-CodeI (STC) based content-adaptive steganography methods embedding messages in the complex areas have been considered as the most conventional approaches of the secure steganography [16].

3.2 Image Steganography Terminologies

The terminologies of the image steganography can be summarized below as shown in Figure (4):

- **Cover-Image:** which represents the original image utilized as the carrier for the hidden information.
- **Stego-Image:** following the embedding of the message in the cover image has been referred to as the stego-image.
- **Message:** which represents the actual information utilized for hiding into the image. A message could be plaintext or another image.
- **Stego-Key:** which represents a key that is utilized to embed or extract messages from the stego-images and cover-images [17].

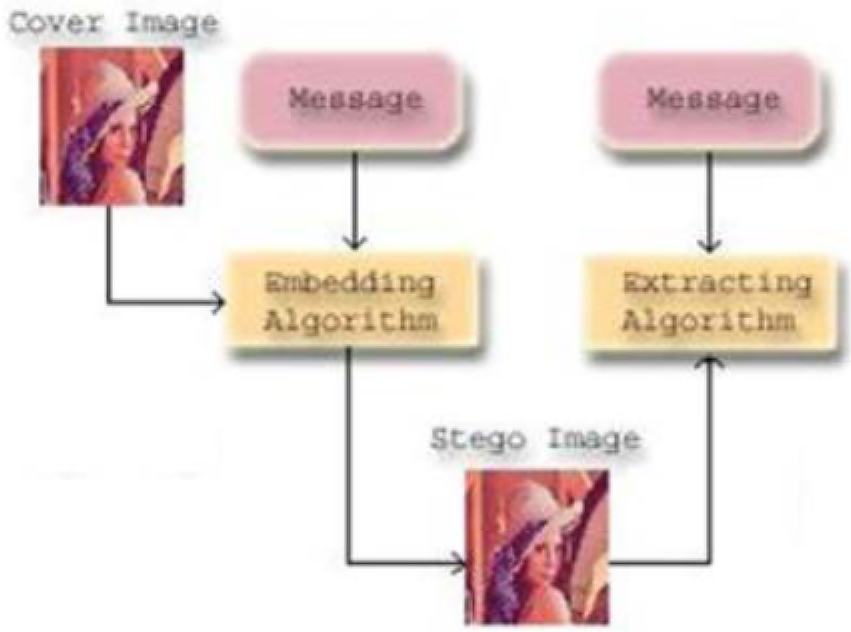

Fig 4. Image steganography

3.3 Types of Steganography

There are basically three types of steganographic protocols used. They are:

· Pure Steganography
· Secret Key Steganography
· Public Key Steganography

Pure Steganography is defined as a steganographic system which does not require the exchange of a cipher such as a stego-key. This method of is not much secure because the sender and receiver can rely only upon the assumption that no other parties are aware of the secret message.

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) previous to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more vulnerable to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. Sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a stronger way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message [18].

3.4 Steganography in the Digital Media

According to the cover object type, there is a number of the proper steganography approaches that are followed orderly for the purpose of obtaining the security. It may be seen from Figure(5).

1. **Image Steganography:** which takes a cover object as an image in the steganography, referred to as the image steganography. In general, in this approach, the intensity levels of the pixel have been utilized for hiding information.
2. **Network Steganography:** in the case of taking the cover object like a network protocol, e.g., UDP, TCP, IP, ICMP, and so on, in which the protocol is utilized as a carrier, has been referred to as the steganography of the network protocol. In the model of OSI network layers there are covert channels in which the steganography may be accomplished in the unused TCP/IP field header bits [24].
3. **Video Steganography**: which is an approach for hiding any information or file type in a digital video format. Video (stream of images) has been utilized as a carrier for the hidden information.

4. **Audio Steganography:** in the case of choosing the audio as the carrier for the hiding of information it's referred to as the audio steganography. It became a quite important medium as a result of the popularity of voice over IP (VOIP). Audio steganography utilizes the digital audio format types, like MIDI, WAVE, AVI MPEG, etc. for the steganography.
5. **Text Steganography:** which is one of the general techniques in the text steganography, like the number of the white spaces, tabs, capital letters, similar to the Morse code are utilized for achieving the task of information hiding [19].

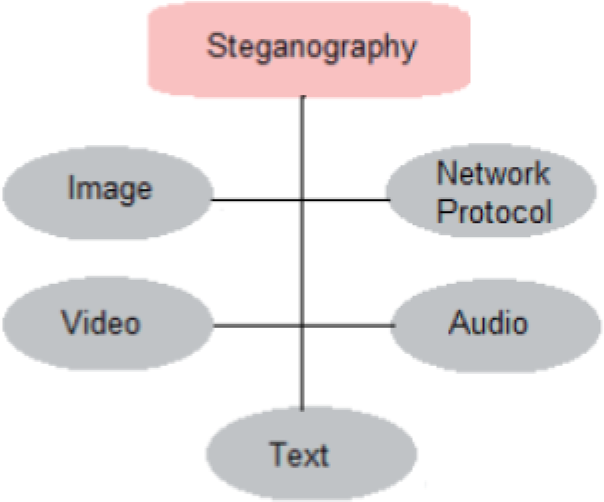

Fig 5. Steganography in the Digital Media

3.5 Steganography Techniques

1. **Spatial Domain Methods:** in this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories:

i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v) Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based.

i) **LSB:** this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii) **BPCP:** In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data.

iii) **PVD:** In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. **Spread Spectrum Technique:** The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus, it is difficult to re move the data completely without entirely destroying the cover. It is a very robust technique mostly used in military communication.

3. Statistical Technique: In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique: In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform do main techniques are broadly classified such as [1] Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv) Embedding in coefficient bits

5. Distortion Techniques: In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information whereas watermarks become a portion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-b it and grey scale images [20].

3.6 Factors Affecting a Steganographic Method

The effectiveness of any steganographic method can be determined by comparing stego image with the cover Image. There are so me factors that determines the efficiency of a technique. These factors are:

1. **Robustness:** Robustness refers to the ability of embedded data to remain intact if the stego image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.
2. **Imperceptibility:** The imperceptibility means invisibility of a steganographic algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.
3. **PSNR (Peak Signal to Noise Ratio):** It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.
4. **MSE (Mean Square Error):** It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient the image steganography technique MSE is computed pixel -by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.
5. **SNR (Signal to Noise Ratio):** It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise [21].

3.7 Application of Steganography

i) Confidential Communication and Secret Data Storing

ii) Protection of Data alteration

iii) Access Control System for Digital Content Distribution

iv) E-Commerce

v) Media

vi) Database Systems.

vii) Digital Watermarking [22].

3.8 Steganalysis

Steganalysis is the opposite procedure of steganography. Primarily, we try to detect the existence of steganographic content in a digital device and secondly discover the hidden message. From this point of view, steganalysis can be classified into two major categories i.e. passive or active. Passive steganalysis tries to classify a cover medium as stego and identify the steganographic embedding algorithm, while active steganalysis additionally tries to estimate the embedded message length and ideally extract it from the cover medium as shown in Figure (6) [23].

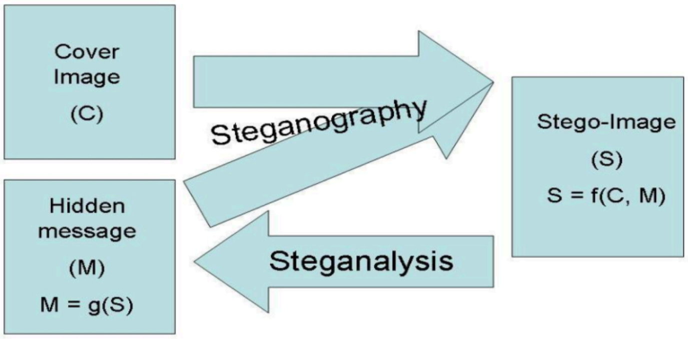

Fig 6. Complete Process of Steganography and Steganalysis

From the block diagram of complete process of steganography and steganalysis which is shown in figure 1. In brief we say that the message (M) is hiding in cover images (C), which gets converted into stego- images (S), stego-images are the function of both C and M. The whole process is called steganography. when we recovering back the hidden message (M) from stego-image called as steganalysis. Current steganalysis aims to focus more on detecting statistical anomalies in the stego images which are based on the features extracted from typical cover images without any modifications. Steganalysis can be classified into two broad categories based on prior information [2]

a) Specific/Targeted steganalysis

b) Blind/Generic/Universal steganalysis

A) **specific/targeted steganalysis:** Specific steganalysis, also called as targeted steganalysis, it is designed to attack one particular type of steganography algorithm. The steganalyst is aware of the embedding methods and statistical trends of the stego image if it is embedded with a known algorithm. This attack method is most effective when tested on images with the known embedding techniques, whereas it might fail considerably if the algorithm is unknown to the steganalyst.

B) blind/generic/universal steganalysis: The more general class of steganalysis techniques independently can be designed to work with any steganographic embedding algorithm, even an unknown algorithm. Such techniques have been called as Universal Steganalysis techniques or Blind Steganalysis Techniques. Blind steganalysis also known as universal steganalysis is the modern and more powerful approach to attack a stego media. Since this method does not depend on knowing any particular embedding technique. This method can detect different types of steganography content even if the algorithm is not known. However, this method cannot detect the exact algorithm used to embed data if the training set is not trained with that particular stego algorithm. The method is based on designing a classifier which depends on the features or correlations existing in the natural cover images. The most current and popular methods include extracting statistical characteristics also known as features from the given set of images [24]

3.8 Deep learning in Steganalysis

Deep learning frameworks achieved excellent performance in many fields. Researchers in image steganography and steganalysis also demonstrated to explore the capability of deep learning algorithms in various key areas of multimedia security. The design of steganalysis based on convolutional neural networks, especially deep learning has achieved amazing performance. Absolutely, a deep learning based steganalysis allows us to automatic feature extraction and classification steps in a distinctive network architecture, beyond any prior feature selection. Inspired by successful approaches based on CNNs, it’s has fascinated the attention of many scholars and made great development. After all, recent development on deep leaning steganalysis is still facing numerous challenges. [25].

4. Discussion and Conclusion

This study examines and presents deep learning-based picture information concealment methods from two perspectives: steganography and steganalysis. Although significant study has been done in these sectors, there are still certain issues that may be improved. Some steganography-based techniques, for example, are quite resilient, but their extraction approach still require being improved. Furthermore, current methods can be improved by the addition or employment of a DL model that is appropriate for the algorithm, or through the introduction of new function of optimization, which is suitable for this algorithm. The aim of the present work on the DL in the steganalysis and image steganography are: a) encapsulation of what was accomplished till now; b) State-of-the-art DL-based image steganography and steganalysis approaches were evaluated then compared. Identification of the unique as well as the common techniques and difficulties, that have been utilized by the scholars for the representation of those issues; c) identification of a few questionable methods for future, in terms of the applications as well as the practical enhancements. In addition to that, important problems and considerations that are involved in the image steganalysis and steganography have been discussed for the purpose of illustrating the way those issues may be transformed to prolific future study avenues. It has been concluded that considerable improvements are going to be accomplished in the case of considering all the advantages and drawbacks of the available models in the case where the DL approaches have been implemented to image steganalysis and steganography.

References

1. Zhang, R., Dong, S., & Liu, J. (2019). Invisible steganography via generative adversarial networks. *Multimedia tools and applications*, *78*(7), 8559-8575.
2. Yang, J., Liu, K., Kang, X., Wong, E. K., & Shi, Y. Q. (2018). Spatial image steganography based on generative adversarial network. *arXiv preprint arXiv:1804.07939.*
3. Baluja, S. Hiding images in plain sight: Deep steganography. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R. (eds.), Advances in Neural Information Processing Systems 30, pp. 2069–2079. Curran Associates, Inc., 2017.
4. Zi, H., Zhang, Q., Yang, J., & Kang, X. (2018, November). Steganography with convincing normal image from a joint generative adversarial framework. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* (pp. 526-532). IEEE.
5. Kreuk, F., Adi, Y., Raj, B., Singh, R., and Keshet, J. Hide and speak: Deep neural networks for speech steganography, 2019.
6. Shang, Y., Jiang, S., Ye, D., & Huang, J. (2020). Enhancing the Security of Deep Learning Steganography via Adversarial Examples. *Mathematics*, *8*(9), 1446.
7. Kodovský, J.; Fridrich, J. (2012): Steganalysis of JPEG images using rich models. *International Society for Optics and Photonics on Media Watermarking, Security, and Forensics*, vol. 8303.
8. Das, A., Wahi, J. S., Anand, M., & Rana, Y. (2021). Multi-Image Steganography Using Deep Neural Networks. *arXiv preprint arXiv:2101.00350*.
9. W. Tang, H. Li, W. Luo and J. Huang, (2014) "Adaptive steganalysis against WOW embedding algorithm", Proc. 2nd ACM Information Hiding and Multimedia Security Workshop (IH&MMSec‘ 14), pp. 91-96.
10. G. Xu, H.-Z. Wu, (2016) “Structural design of convolutional neural networks for steganalysis,” IEEE Signal Processing Letters, vol. 23, pp.708–712.
11. J. Lu, G. Zhou, C. Yang, Z. Li,(2019) “Steganalysis of content-adaptive steganography based on massive datasets pre-classification and feature selection,” IEEE Access, vol. 7, pp. 21 702–21711.
12. Qian, Yinlong, Dong, (2015)“Deep learning for steganalysis via convolutional neural networks” , SPIEDigitalLibrary.org/conference-proceedings-of-spie..
13. Chang, C. C.; Fan, Y. H.; Tai, W. L. (2008): Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, vol. 41, no.2, pp. 654-661.
14. Dutta, S.; Murthy, A. R.; Kim, D.; Samui, P. (2017): Prediction of compressive strength of self-compacting concrete using intelligent computational modeling. *Computers, Materials & Continua*, vol. 53, no. 2, pp. 157-174.
15. Feichtenhofer, C.; Fan, H.; Malik, J.; He, K. (2018): SlowFast networks for video recognition. *Computer Vision and Pattern Recognition*.
16. Fridrich, J.; Kodovsky, J. (2012): Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868-882.

17. Fu, H.; Gong, M.; Wang, C.; Batmanghelich, K.; Tao, D. (2018): Deep ordinal regression network for monocular depth estimation. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2002-2011.
18. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D. et al. (2014): Generative adversarial nets. *Advances in Neural Information Processing Systems*, pp. 2672-2680.
19. Gautam, C.; Tiwari, A.; Leng, Q. (2017): On the construction of extreme learning machine for online and offline one-class classification-an expanded toolbox.
20. Gurusamy, R.; Subramaniam, V. (2017): A machine learning approach for MRI brain tumor classification. *Computers, Materials & Continua*, vol. 53 no. 2, pp. 91-108.
21. Holub, V.; Fridrich, J. (2013): Random projections of residuals for digital image steganalysis. *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996-2006.
22. He, K.; Zhang, X.; Ren, S.; Sun, J. (2016): Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770-778.
23. Konstantinos Karampidis , " A review of image steganalysis techniques for digital forensics" , Journal of Information Security and Applications 2018
24. PevnyT.andFridrichJ, "Merging Markov and DCT features for Multiclass JPEG Steganalysis,Steganography, and watermarking of Multimedia Contents",vol. 6505, pp1-13,Springer 2007
25. T. Pevny, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix", *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215-224, 2010.

.