IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Deep Learning Technique In Steganography With Multimedia Network Security For Health Care

Anupama A Kori[1], P. I. Basarkod[2] , Veena. K. N[3]

[123] School of Electronics and Communication Engineering,

[1,2,3] REVA UNIVERSITY, Bengaluru-560064, India

Abstract: Information breach in today's world has become major setback in technological advancements. To secure such confidential information steganography is used. In this experiment, the secret image is covered by cover image which involves hiding process of the information and in the later stage the secret image is separated from the cover image which involves the recovery process of the information. Three deep learning models namely Preparation Network, Hiding Network and Reveal Network were designed to perform as a pair and are simultaneously trained on images randomly selected from Tiny Image Net Database and it performs well on natural images from a variety of sources. This paper blends image-into-image steganography with recent deep convolutional neural network methods

Keywords: Steganography, Deep Convolution Neural Network, Image based Analysis, Audio based Analysis, Video based Analysis, Network Security.

1. Introduction

The art of veiled or concealed writing is known as steganography, and it dates back to the 15th century when messages were physically hidden. The aim of modern steganography is to communicate a digital message invisibly. The steganographic method embeds a secret message in a carrier, which is a transport medium [1]. The carrier can be noticeable to the general public. The secret message may also be encrypted for added protection, enhancing perceived randomness and reducing the probability of content discovery even if the message's presence is identified. Introductions to steganography and steganalysis that are easy to understand (the process of discovering hidden messages).

The amount of medical data in health care domain stores electronically, so does the need to improve its security. The inability to access patient records at the appropriate time will result in a high death toll as well as a decline in the quality of health care services provided by medical professionals. Since 2010, criminal attacks on social security have increased by 125 percent, making them the leading cause of medical data breaches [3].

The goal of traditional and non-traditional steganography is to communicate a digital message or a secret information invisibly by hiding it or encrypting it. The steganographic method inserts a secret message in a carrier, which is a transport medium [6]. The carrier can be visible to the general public. The secret message may also be encrypted for added protection, enhancing perceived randomness and reducing the probability of content discovery even if the message's presence is identified.

The objective of this work is to visually cover up a complete H* W* C pixel secret multimedia data in another H* W* C cover multimedia data with as little noise as possible (each colour channel is 8 bits). We follow the method that the hidden multimedia data to be collected losslessly, unlike previous studies in which a secret multimedia message must be transmitted with complete reconstruction. Instead, we're willing to consider reasonable trade-offs in carrier and hidden picture quality. Secret message bit rates as low as 0.1bpp have been discovered in previous studies; our bit rates are 10*- 40* higher.

2. Literature Review

Steganography is a collection of techniques for hiding the presence of knowledge by encasing it in a cover. With the advancement of deep learning [2], new steganography approaches based on autoencoders or generative adversarial networks have emerged. While the advantages of deep learning-based steganography methods include automatic generation and capability, the algorithm's protection needs to be improved. Easy methods like LSB manipulation have been used to encode a lower resolution image into a higher resolution image using steganography over the years.

In this application [1] we use deep neural networks to encode and decode multiple hidden images within a single high-resolution cover image. In 2017 Shumeet et al. [4] tried to fit a full-size color image into another image of the same size, where deep neural networks are built to operate as a pair and are simultaneously trained to construct the hiding and revealing processes.

According to [6] the accessories to provide protection in healthcare systems should be reviewed. The aim of this report is to summarise the findings of a literature review on the protection of health-care systems supported by information-hiding techniques such as cryptography, steganography, and watermarking. As a result, we share our perspectives on open research problems and point to future directions in this field.
Steganography model will be trained on large number of multimedia data such as image, audio and video so that information can be hided in a more effective way and can be revealed or decoded in an effective way. This paper blends image-into-image steganography with recent deep convolutional neural network methods.

3. Research methodology

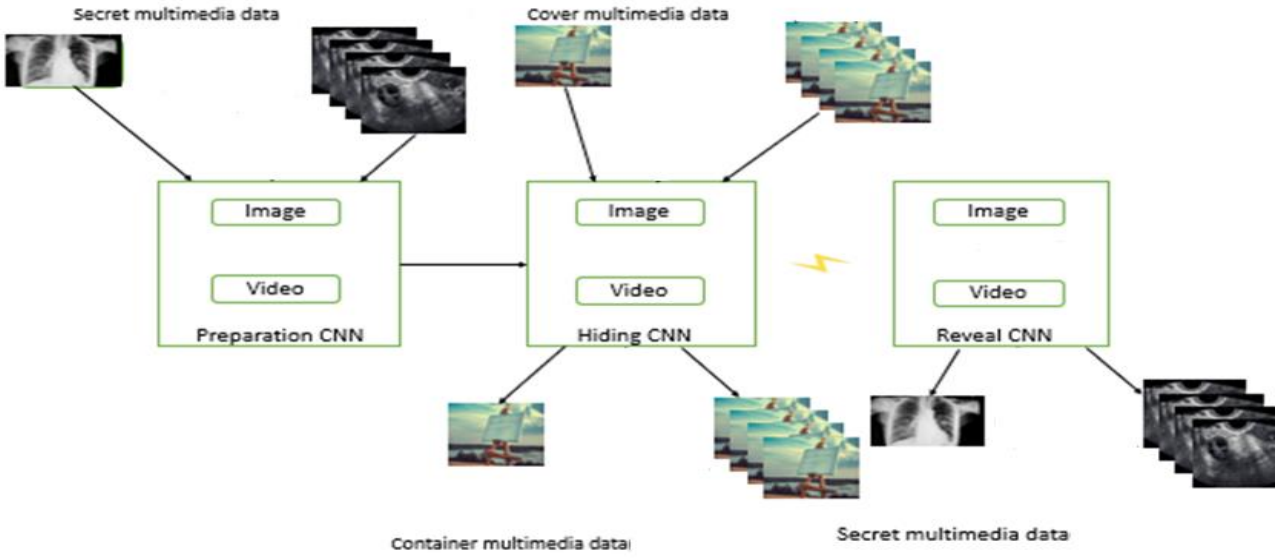


Fig 1. Block Diagram

The cover image, cover audio frames, and cover video frames in Figure 1 cover confidential information that must be transmitted, while the secret image, secret audio frames, and secret video frames are hidden outside the cover image, cover audio frames, and cover video frames. The secret multimedia data is prepared in the Preparation Network by extracting certain features from the secret multimedia data using Deep Neural Networks, and then concealed beyond the cover multimedia data by the hidden network, which is made up of different layers of Deep Neural Networks.

3.1 Data collection

The data set was collected from Kaggle the online platform for data collection. The secret image consist of various medical images like brain tumour images, knee osteoarthritis and chest x-ray Pneumonia images. The cover image was collected from ALASKA Steganography photographs. There were total 500 data which were collected for training 250 data for testing and validation.

3.2 Data pre-processing

The input secret image and cover image was resized to 224x224 pixel value and reshaped to 1,224,224,3 where 1 indicates number of images, 224 indicates pixel width of image, 224 indicates pixel height of the image and 3 indicates number of channels (RGB).Then input secret and cover image were normalized by 255, as image pixel size ranges from 0 to 255.The output secret and cover image were denormalized by 255 to obtain the original data.

3.3 Model architecture

The Preparation Network for medical steganography analysis. In preparation network the secret image is passed through three different architectures, each architecture consist of four layers and each layer consist of convolution layer with 50 number of filters, kernel size of 3, same padding and with activation function as relu. Next the output of all the three architecture present in the preparation network is concatenated and passed through three different convolution layers which consist of 50 number of filters, same padding and same activation function as relu but each convolution layer consist of different kernel size, 1st convolution layer have kernel size of 5, 2nd convolution layer have kernel size of 4, 3rd convolution layer have kernel size of 3.
The generated filtered secret image from the preparation network and the cover image where secret image to be hided were concatenated and passed through three different architectures, each architecture consist of four layers and each layer consist of convolution layer with 50 number of filters, kernel size of 3, same padding and with activation function as relu. Next the output of all the three architecture present in the hiding network is concatenated and passed through three different convolution layers

which consist of 50 number of filters, same padding and same activation function as relu but each convolution layer consist of different kernel size, 1st convolution layer have kernel size of 5, 2nd convolution layer have kernel size of 4, 3rd convolution layer have kernel size of 3.
The Reveal Network for medical steganography analysis. In reveal network the container image is passed through three different architectures, each architecture consist of four layers and each layer consist of convolution layer with 50 number of filters, kernel size of 3, same padding and with activation function as relu. Next the output of all the three architecture present in the reveal network is concatenated and passed through three different convolution layers which consist of 50 number of filters, same padding and same activation function as relu but each convolution layer consist of different kernel size, 1st convolution layer have kernel size of 5, 2nd convolution layer have kernel size of 4, 3rd convolution layer have kernel size of 3.

3.4 Model training

The model architecture consists of three networks namely Preparation network, Reveal network and Hiding network. The data which was collected was trained on built architecture on various parameter such as Adam as a optimizer, loss as a mean squared error, no of epochs should was 100 and batch size is 12. The model took around 4 hours for training on google colab GPU and model was saved on those epochs which had improvement in mean squared error loss.

4. RESULT

The result was calculated from mean squared error loss which is one of the best measurement parameters for regression type of task where output is in the form of continuous values. In our paper there are 3 types of loss namely preparation loss, reveal loss and hidden loss which was calculated using mean square error.
As we can see that from the below graph figure 2 the loss was decreased as number of epochs increases for all the three networks namely Preparation Network, Hidden Network and Reveal Network.

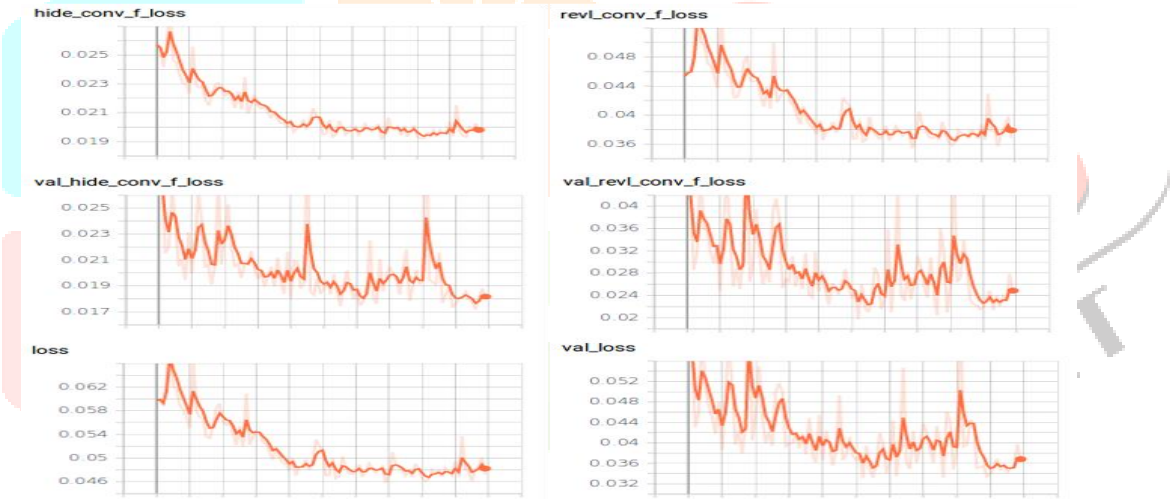
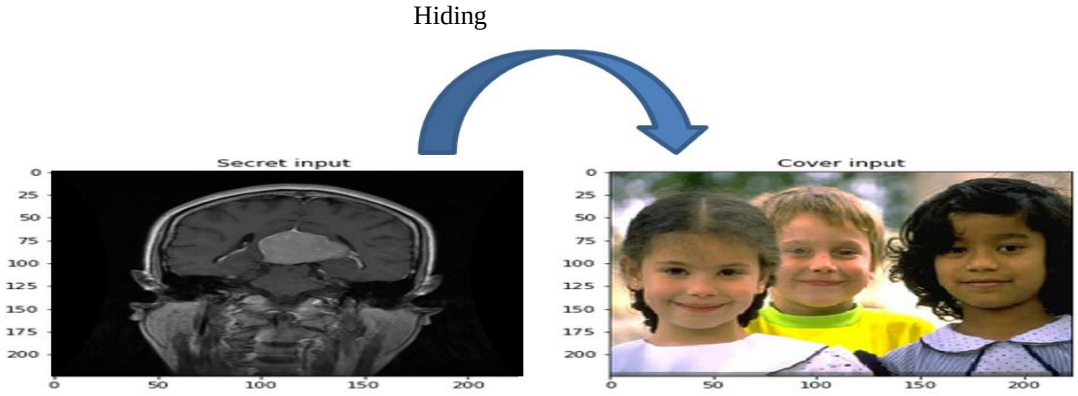


Fig 2. Graph Analysis of Proposed Work

Image Steganography: The below Fig 3 shows the output generated by the model in image steganography. For testing purpose unseen secret image and cover image was selected as shown below. The secret input consist of brain tumor image and cover image consist of some random image. The secret image will be hided beyond the cover image in such a way that nobody can see the secret image.

Input Image:



Output Image:

The secret output consist of brain tumor image and cover image consist of some random image. The secret image will be revealed which is hided beyond the cover image by Reveal Network.

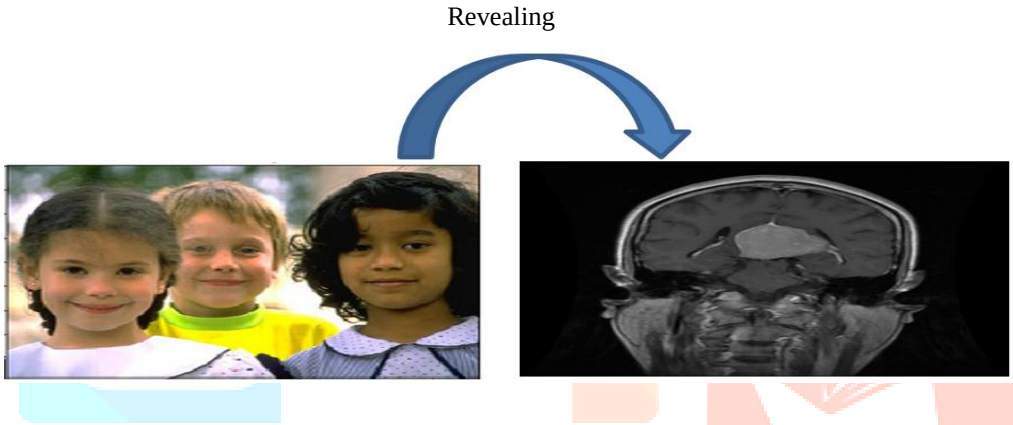


Fig 3. Image Steganography

Video Steganography: The Fig 4 shows the output generated by the model in video steganography. For testing purpose unseen secret video and cover video was selected as shown below. The secret input consist of ultrasonic video and cover image consist of some random video. The secret video will be hided beyond the cover image in such a way that nobody can see the secret video.

Input video:

Output Video:

The secret output consist of ultrasonic video and cover video consist of some random image. The secret video will be revealed which is hided beyond the cover video by Reveal Network.

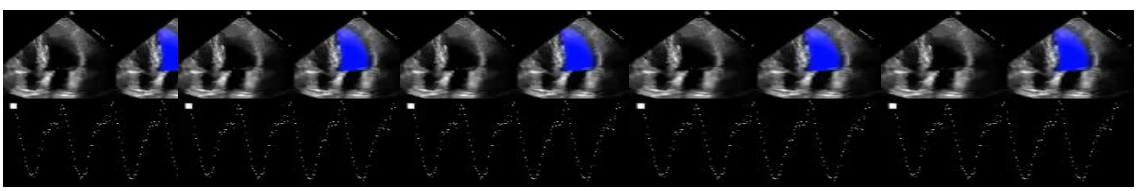


Fig 4. Video Steganography

5. CONCLUSION

This project uses deep learning to exhibit multimedia steganography. On various input images and text messages, Adam's algorithm was utilised to implement it. The hidden picture media was embedded into a cover picture file using a hidden network in the first part. The reveal network at the receiving end then reverses this process, ensuring the safe transmission of the secret message. The model was trained using Adam's algorithm. A text message is overlapped onto the visual media in the second section, with non-noticeable alterations perceptible to the human eye. To recover the secret text message, steganalysis must be performed on the other end. Other steganography programmes will not be able to decode and expose the secret message hidden in the cover material. As a result, this application is more secure. Regardless of the multiple cover images and secret messages used as inputs, the network is only trained once. This procedure has numerous applications, including the concealment of secret military information, the use of watermarking techniques to conceal identification, and increased security through fingerprinting and biometrics.

6. FUTURE SCOPE

Steganography is the most effective method of communicating sensitive information because it is undetectable by merely looking at the image. However, developing a steganography that meets both the criteria of high robustness and high security will be a difficult undertaking. By solving the aforementioned problem, existing steganography tools can be improved. The usage of numerous passwords can improve the content's security. Despite the fact that the image has been recovered and one password has been identified, there will be additional passwords to identify, making the job difficult for the intruder.

REFERENCES

[1] Meng, Ruohan & Cui, Qi & Yuan, Chengsheng. (2018). A Survey of Image Information Hiding Algorithms Based on Deep Learning. Computer Modeling in Engineering & Sciences. 117. 425-454. 10.31614/cmes.2018.04765.

[2] Shang, Yueyun & Jiang, Shunzhi & Dengpan, Ye & Huang, Jiaqing. (2020). Enhancing the Security of Deep Learning Steganography via Adversarial Examples. Mathematics. 8. 1446. 10.3390/math8091446.

[3] Das, Abhishek & Wahi, Japsimar & Anand, Mansi & Rana, Yugant. (2021). Multi-Image Steganography Using Deep Neural Networks.

[4] Shumeet Baluja. 2017. Hiding images in plain sight: deep steganography. In Proceedings of the 31st International Conference on Neural Information Processing Systems Curran Associates Inc., Red Hook, NY, USA, 2066–2076.

[5] Chahar, Vijay & Laddha, Saloni & Sharma, Aniket & Dogra, Nitin. (2020). Steganography Techniques Using Convolutional Neural Networks. Review of Computer Engineering Studies. 7. 10.18280/rces.070304.

[6] Johnson, Neil F., Duric, Zoron, Jajodia, "Information Hiding steganogarphy and watermarking- Attacks and Countermeasures" , Kluwer Academic Publishers., 2001.

[7] Katzenbeisser S. and petitcolas F., "Information Hiding Techniques for . steganograhpy and Digital Watermarking ",Artech House, USA 2000.

[8] Stevens, Roger T. "Graphics Programming in C",BPB Publications, 1993.

[9] Rodriguez-Colin Raul, Feregrino-Uribe Claudia, Trinidad-blas Gershom de J. "Data Hiding Scheme for Medical Images", Luis Enrique Erro No. 1 Sta . Maria Tonantzintla, Puebla, Mexico C. P. 72840 , 2008.

[10] Shuliang Sun1,2 , ―A New Information Hiding Method Based on Improved BPCS Steganography‖ , Volume 2015 , Article ID 698492, 2015.

[11] Pevny, T.; Filler, T.; Bas, P. Using high-dimensional image models to perform highly undetectable steganography. In Proceedings of the International Workshop on Information Hiding, Calgary, AB, Canada,28–30 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 161–177.

[12] Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain,2–5 December 2012; pp. 234–239.

[13] Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain.EURASIP J. Inf. Secur. **2014**.

[14] Li, B.;Wang, M.; Huang, J.; Li, X. A new cost function for spatial image steganography. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014.

[15] Jamie, H.; Danezis, G. Generating steganographic images via adversarial training. In Proceedings of the Annual Conference on Neural Information Processing Systems 2017, Long Beach, CA, USA, 4–9 December 2017.