National College of Ireland

Image Steganography on Cryptographic text using Neural Networks

MSc Research Project
Cyber Security

Aarsh Bararia
Student ID: x19215045

School of Computing
National College of Ireland

Supervisor: Prof. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Aarsh Rajesh Baraia
Student ID:	x19215045
Programme:	MSc in Cyber Security **Year:** 2020-2021
Module:	MSc Research Project
Supervisor:	Prof. Imran Khan
Submission Due Date:	16th August, 2021
Project Title:	Image Steganography on Cryptographic text using Neural Networks
Word Count:	4872 **Page Count:** 14

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: .....

Date: .....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Image Steganography on Cryptographic text using Neural Networks

Aarsh Bararia
Student ID: x19215045

Abstract

This paper is an effort to design and implement a data securing technique using both Cryptography and Steganography together. Using both these techniques together gives multiple layers of security to the message and help to transmit confidential information securely. For encryption and decryption of message AES-256 encryption technique along with password based key derivation function PBKDF2 is used. The encrypted text is then encoded inside the image pixels. This encoded image is further encrypted inside another image using multi-image steganography. This paper is an effort to implement multi-image steganography in combination with Deep Neural Networks. This technique is designed to take the encoded image and a random cover image from image dataset and then train the neural network to hide the encoded image in the cover image.

Index Terms: **Cryptography, Steganography, Deep Neural Networks**

1. Introduction

1.1 Background Overview

Transferring data has become one of the most important aspect of communication and with the advancements in technology, transferring data securely has become the most important aspect of the communication chain. Usually, Cryptography is used to encrypted data and transfer over a communication channel. This is a very secure method to use but the minor issue with this method is the resulting text after the encryption doesn't make any sense and if this text is transmitted, it makes it obvious suspicions over the message and the interceptor gets confirmation that this data is confidential. But if this encrypted text is hidden inside an image and then image is transmitted it can dodge a lot of trouble from the interceptors. This is the basic idea of the paper and in an effort to make the technique more efficient and secure the encoded image is hidden inside another cover image using Deep neural networks. Two networks are trained, first is Hiding network and the other is Revealing network. Hiding network will take the take the encoded image and a random image from the image dataset and train itself to hide the encoded image inside the cover image with minimum distortions and peak-signal to noise ratio.

1.2 Motivation

Cryptography and Steganography are two different techniques for data encryption and decryption. Both these techniques have had significant impact in the field of networking where the need for data transmission is particularly important and transferring data securely is one of the most important aspect of it. The idea in this paper takes both these techniques and intend to design a hybrid technique that takes the perks of both these techniques and implement them together using Deep neural networks. There have been techniques that have

used Convolution neural networks (CNN) or General Adversarial neural networks (GANs) for the purpose of data security or image steganography. But most of the models face on multi-image steganography only. This attempt to design a robust and secured data encryption technique in the age where the advancements in technology daily are commodifying the data transmission.

1.3 Research Question

"How Image Steganography over encrypted text or images can be achieved using Neural Networks to enhance data security?"

1.4 Research Objective

In the presented research technique, a bridge is intended to be build between cryptography and steganography by combining these two techniques and implanting a new hybrid method for data encryption with multiple layers of encryption involved in the process. The cryptographic technique used for the data encryption is AES-256 encryption technique along with password based key derivation function (PBKDF2). This function helps the users to protect the message from tools that are used for cracking the passwords. This generates a random string of encrypted text, and this encrypted text is then hidden inside and image. This is the second layer of encryption where the data is converted into an eight-bit binary code by using the ASCII values. After that these binary converted values are stored in the pixels of image. Three pixels are taken together that gives in total of nine RGB values, out of these nine values eight are used to hide the eight-bit binary converted code and last value is made one if the value of RGB is odd and it is made zero if the value is even. This image is then fed to the neural network which is designed with combination of three networks first is preparation network, hidden network and last is reveal network. These networks work in harmony with each other. The methodology approach carried out for this project is Cross-Industry Standard Process for Data Mining (CRISP-DM).

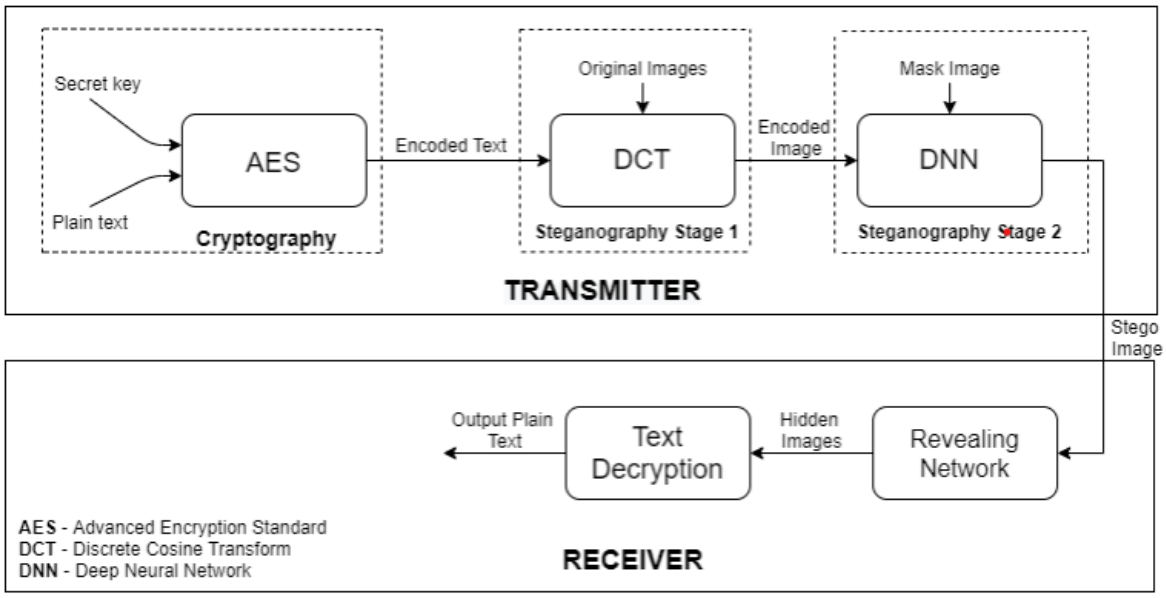


Figure 1: Research Flow

The report structure follows like this, Section 2 of the report comprises of a detailed literature review about the previous works over steganography, cryptography, understanding different

neural networks, implementation of steganography using different neural networks. The next section i.e., Section 3 describes the methodology followed for the research to get the desired results. The results and evaluations are covered on Section 4 and the last two sections 5 and 6 focus on depicting the learning outcomes, Conclusion and limitations of the proposed techniques and future work that can be done to overcome them.

2 Literature Review

Various cryptography and steganography techniques have been around since they were introduced. Also, there are many hybrid techniques proposed for combining cryptography and steganography and in addition to that in the recent years techniques to implement steganography using neural networks are also published A deep and detailed review was performed. This literature review section is divided into 5 sub-sections New Cryptography techniques, Steganography techniques, learning different neural networks, Combination of Cryptography and Steganography and the last one is implementing steganography using neural networks.

2.1 Cryptography techniques

Cryptography has been around since a long time and there have been many good techniques and in the following paper (Emori, 1973) author performs an experiment on three encryption techniques namely AES, DES and RSA, these three techniques are widely used for end-to-encryption in most of the applications. Authors performed a thorough analysis on all three techniques with their designed experiment and compared the results in the paper and determined that AES algorithm is much better than the other two techniques.
(Rothke, 2007) AES was officially announced as Federal information Processing Standards Publications by NIST in the year 2001. The paper explains in detailed specification, implementation, and applications of the AES encryption standard and (Daemen and Rijmen, 1999)shows the math behind the techniques. This paper explains every part of AES working along with the calculations included with it. These two papers clearly explained the AES technique. (Bidhuri and Heffernan, 2019)author describes a hybrid technique of AES encryption and SCrypt. Scrypt is a password based key derivative function which helps to enhance the strength of a password to withstand against the attacks.

2.2 Steganography

In (Altaay, Sahib and Zamani, 2012) author gives an in-depth explanation steganography. The paper covers all the aspects of steganography starting from important measurements such as the capacity of an image to hide data without getting distortions these can be defined by the Mean square error(MSE) or Peak Signal to Noise Ratio (PSNR); Robustness, which is strength of any image to keep hidden data undistorted against the disturbances and distortions while being transmitted and lastly the authenticity of image.
(Bansal *et al.*, 2015)author gives a detailed idea of multiple steganography techniques used for the purpose of hiding data in Images.
(Khan and Jeoti, 2010) author proposed a novel technique to blind watermark an image using the bit plane of DC component in an image. In this paper the author used DC component in the bit plane of an image to watermark the image. The image is watermarked at random positions on the DC components in Bit-plane. These random positions are generated by a scrambler. The best feature of the technique is that it does not require the original image to

check for the watermark and hence this is what makes the technique a blind watermarking technique making it unique.

2.3 Understanding the Neural Networks

(Canziani, Paszke and Culurciello, 2016)author performs a detailed analysis of all the necessary metrics of multiple deep neural networks models and compares and explains the architecture, power consumption, accuracy of the particular models. The paper provides some significant set of data which definitely helps in choosing a perfect model for any application.
(Wei *et al.*, 1998)author describes Artificial neural networks very well, starting from the basic question "What is Artificial neural network. Author clearly depicts the working of an ANN and how it can be put to use in various filed with an example of ANN being used in the medical field.
similar to the previous paper this is also a research paper to understand the basic working of (Albawi, Mohammed and Al-Zawi, 2018)Convolution Neural Network. Author very well describes all the aspects of a CNN right from it meaning, idea, technologies used, working and the mathematical approach taken to design a CNN. After carefully reviewing these three types of Neural network it was pretty obvious the CNN has most applications in field of image processing and image recognition, face generations and many more.

2.4 Combination of Steganography and Cryptography

(Pujari and Shinde, 2016) proposes a technique to enhance steganography along with cryptography, here the author designed a hybrid encryption technique using more than one cryptographic scheme such as AES, RC2, Blowfish. To make this more secured author adds a second layer of security; this second layer is to use image steganography technique LSB in addition with the parity check. The architecture of the proposed method is such that it is divided in three steps. First it takes the message and encrypts using multiple hybrid cryptographic schemes, second is that it hides all the encrypted text inside an image using LSB and parity checker steganography techniques. The final step is that author evaluated all the encrypted images with different techniques based on their Peak-Signal-to-Noise ratio PSNR and the technique with best PSNR gets transmitter.
(Atee, Ahmad and Noor, 2014) author has focused on the most important drawback of cryptography and steganography techniques. The biggest drawback of cryptography is that once a text is encrypted with a cryptographic technique it gets converted into random stream of alphabet, number, and symbols and the drawback with steganography is that it mostly encrypts the data in plaintext. Which makes it very easy to break and get the data from inside. Therefore, author proposes a technique which flows like using AES encryption to encrypt the data and then hiding this encrypted text inside an image using Pixel value differencing. The proposed technique achieves the double layer of security, but the technique inly implemented on grey scale images.
(Oo and Aung, 2020)Author purported a secured method comprising of combination of both cryptography and steganography for the for the communication over multimedia channels. The writer makes use of AES algorithm in combination with CBC which is then encoded inside and image achieving coloured image steganography.
In the sphere of wireless communication, (Eyssa, Abdelsamie and Abdelnaiem, 2020)has recommended a robust Steganography approach. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are used to encrypt three images into a single mask image, increasing the hiding capacity (DWT). Cover photos have been subjected to a variety

of permutations and transformations in order to improve image deterioration tolerance. This method is done using Orthogonal Frequency Division Multiplexing (OFDM), and the results outperform existing techniques using the Least Significant Bit (LSB) and PSNR as assessment metrics.

This paper (Pradhan *et al.*, 2016) focuses on three specific parameters considered for performing evaluation for various Image Steganography techniques. Hiding Capacity within an Image, Distortion Measure of Images and Security implemented for Encryption are the parameters specified in the paper. Evaluation Metrics such as MSE, PSNR, quality index, correlation, SSIM, etc. are considered to measure distortion within images and the security for the resultant container images have been displayed using Histograms focusing on pixel differences. Using these parameters, authors have successfully evaluated different steganographic algorithms and focuses to explore different areas such as LSB, PVD, etc.

In this study (Shaik, Thanikaiselvan and Amitharajan, 2017), different Data Hiding strategies based on Cryptography and Steganography are discussed. The author focuses on several properties of Data Hiding with Steganography and assesses them using a variety of criteria such as Bit Error Rate (BER), PSNR, SSIM, and others to get satisfactory results. . Using these evaluation factors, the paper also directs on Spatial Image Hiding and Steganalysis. The features of Hiding are being studied in order to increase Robustness and Accuracy in the future.

2.5 Steganography using Neural Networks

(Das *et al.*, 2021) showcases a unique technique of Steganography which comprises of three neural networks which work together to encode images within images and the reveal back the hidden image. Deep neural networks are used in all the three phases of the paper to hide and reveal the images. The author further extends work from single images to multiple images using same network. This was done after remarkable results were achieved in terms of Peak Signal to Noise ratio and Accuracy. Author intends to overcome the limitations of the techniques in terms of colour regeneration for hidden images in the future work of the research. To tackle the problems of hiding multiple images into one carrier.

To deal with the problems of concealing more than one image inside a single carrier, (Duan, Liu, *et al.*, 2020) came up with a solution by using a convolution neural network (CNN). The paper depicts two ML models each dedicated for encoding and decoding images at a same time. To negate the issue of image regeneration both of these models are trained with a large number of images. Authors successfully achieved the execution of image steganography using convolution neural network and compared this model with ResNet and Unet on the basis of PSNR ratio. Authors described the future scope of the paper as their intentions to overcome time and space constraints in relation with decryption process and the process of hiding image.

With a goal to accomplishing better and improved image visualisation in the field of steganography,(Duan, Guo, *et al.*, 2020) puts forwards a novel technique of using Discrete Cosine Transform (DCT) for the purpose of conversion of original images into secret image. This particular technique uses multi-level steganography after the conversion of first layer of steganography and after that the Elliptical curve cryptography. (ECC) to encrypt the image and the make use of the hiding network to create a container image. This particular technique is double layer data security along with the improvised image visuality by using deep neural network named SegNet in the hidden network section. The results of this technique are evaluated on the basis of Structural Similarity Index and the peal-signal-to-noise ratio.

This research paper () focused on mentioning various implementation procedures in the field of steganography and steganalysis using CNN deep convolution neural networks. Author has

beautifully pointed of advantages and disadvantages of multiple techniques in the field. Author had done a perfectly good job of guiding new aspiring researchers in right direction by supplying with proper resources and hypothesis by optimizing results and thereby optimizing neural networks.

To uncover secret information and check for steganographic images (Oplatková *et al.*, 2009) proposed a novel technique, making use of neural network-based image steganography method of displaying encoded message. OutGuess and Steghide were used to program the model and to train itself to produce maximum output. These models provided considerably high accuracy in comparison to the traditional revealing network. Evaluation of these model was performed on the basis of root mean square error (RMSE). Even though the proposed models performed excellent in accuracy, but these models did not perform well in terms of alterations of hidden layers and improving that was the main focus on authors in future works.

(Hussain *et al.*, 2020) used four Artificial Neural networks (ANN) to implement steganography over sensitive information inside an image. The main reason to choose ANN in place of any other neural network is to implement Scaled Conjugate Gradient (SCG) technique. This technique helped in perfecting the hiding of secret image in container image without leaving any errors. Evaluation of this method was performed by MSE and PSNR.

A strong method of image steganography by () in respect to the field of wireless communication. The proposed method uses DCT and DWT to hide three secret images in a single cover image thus, increasing the hiding capacity of and image. The technique was employed over Orthogonal Frequency Division multiplexing and the output of this technique surpassed the results of previously used LSB based methods.

3. Research Methodology

For the proposed research technique, the CRISP-DM methodological approach is being taken into consideration and it is strictly being followed. All the work for the technique was performed as per the steps mentioned by the methodology.

The steps followed are displayed in the flow chart below:

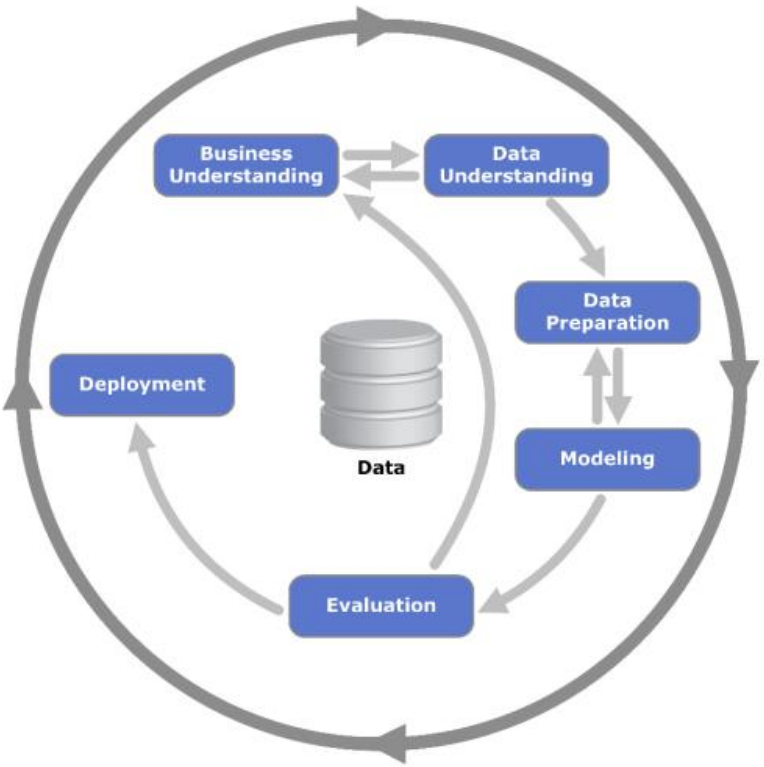


Figure 2: CRISP-DM Methodology flow

3.1 Business Understanding

The main purpose of this phase is to achieve the knowledge of the process of Cryptography, Steganography and Neural Networks. Also, to comprehend the necessity of a data encryption technique that provide multiple layers of encryption to sensitive data. Keeping this particular need in mind the proposed technique is an attempt to provide three layers of encryption; first by encrypting the data with AES technique, second is by hiding the AES encrypted data into an image using text to image steganography and last by hiding the encoded image into another image using multi-image steganography implemented with the help of convolution neural network.

3.2 Data Understanding

The second most important thing for any research after understanding the needs is to understand and choose correct data for the experiment. Because data contributes to the maximum information for the technique, it is critical to know what kind of data are most appropriate. Choosing correct data is a very crucial stage before the implantation begins. Data sets used for this research are text dataset consisting of all alphabets, numbers, and symbols for the AES encryption. For the sake of text to image steganography and multi-image steganography using neural network image dataset of google images of art piece, places, food and cultures of all around the world are included in it is being used.

4. Design Plan

This section particularly concentrates on planning the flow of the research. The proposed research has been performed as per the steps mentioned below

- Multiple Image data sets were researched and out of those one dataset was selected based on its specifications which perfectly matched with the need of project.
- The first step is to use AES encryption to encrypt the secret message using PBKDF2 function.
- After encryption is performed the encrypted text is then encoded into an image by converting the text into 8-bit binary code and the hiding it inside the pixels of the secret image.
- After this, there are two sets of images with us. First set is the cover image, and second set is the encoded images. These two sets of images become input to our image steganography convolution neural network.
- Designing of neural network, dividing both the image datasets into test and train data by the ratio of 70 to 30.
- After this the datasets are provided to the convolution neural network. The CNN is divided in three networks prep network, hidden network and reveal network.
- The last step is to evaluate the output of the CNN used for multi-image steganography.

5. Implementation

5.1 Data Pre-processing

Proper data is important for any experiment and hence pre-processing the data properly is one of the most important tasks of any research to be performed properly. After the downloading the data set following steps were performed for the pre-processing the data and making it ready to use for neural networks.

The dataset downloaded had many folders and inside those folders there were multiple subfolders, and these subfolders then contained the images that we wanted to use for the processing. So, the very first thing done as the part of pre-processing of data was that a new folder was created and then the images from all the sub-folder were then transferred into the new folder using python code. Also, these images were not named properly and thus it was difficult to identify a particular image. Therefore, all the images were renamed as Image_00,01,02 and so on.

Following to this, the dataset was divided into two equal halves, first half was used as secret images and second half was used as cover images. The secret images were transferred to a new folder. Thus, the data was divided into two subsets for the ease of use.

These were the pre-processing steps performed before the start of the implementation. Once the first part of the proposed method was implemented, there was again need for the data pre-processing as there were some changes made in the data set. A new folder of images was created, named “encoded_images”. This set of images contained the output of the text to image steganography step of the experiment. These images contained the AES encrypted message inside them. Following operations were performed on these images: all the images were resized and made of same size so that they can be hidden inside the cover images uniformly. Both the datasets, cover images and the encoded images were split into two different datasets for the neural network these datasets were test and train datasets. The

datasets were split in 70:30 which gave 70% of images to training and 30% images for testing.

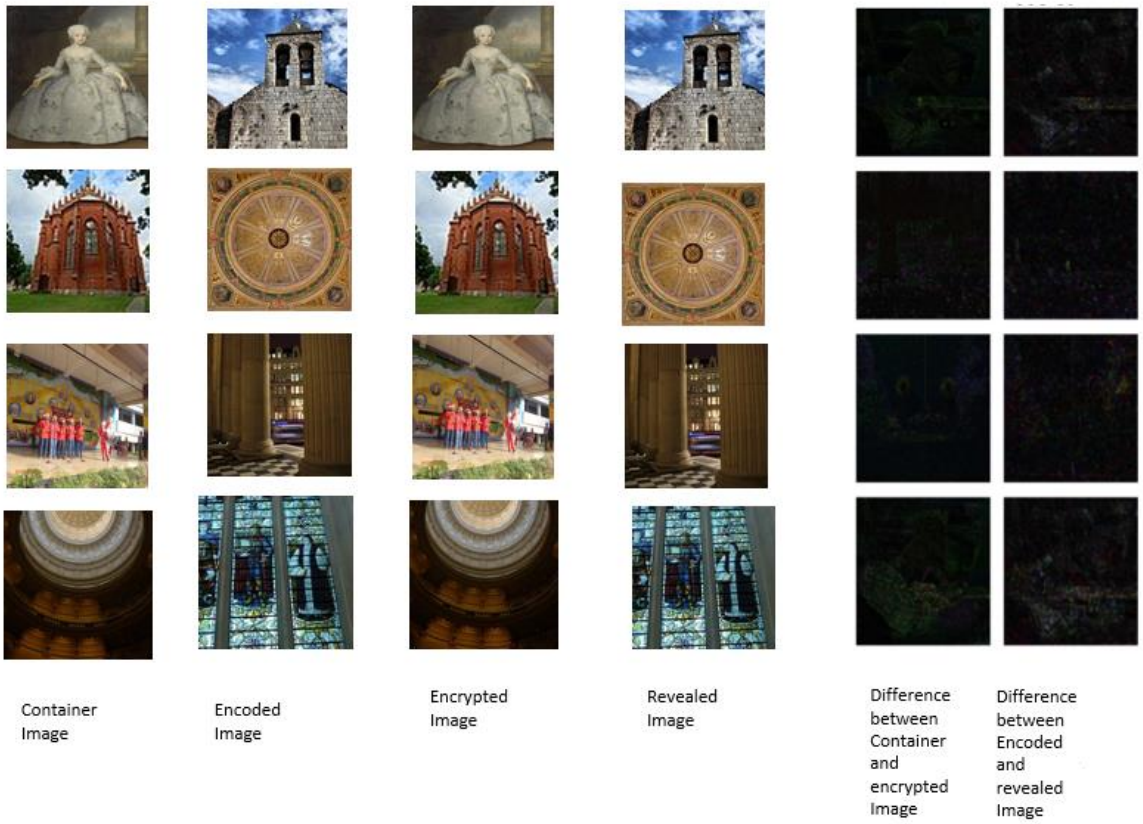
5.2 Data Modelling

This is of the most important phase of the research, where the data model is designed and implemented. The structure of the Data model is divided into three different networks.
Deep Convolution neural network is designed here with a goal of encoding an AES encrypt secret image into a cover image and then reveal the encoded image. The CNN comprises of three networks working together to achieve the mentioned goal. The three networks are prep network, hiding network and revealing network.

- Preparation network or prep network is specially designed for the secret images only. The main motive in designing this prep network is to properly prepare the secret images that are to be hidden inside cover image. The prep network is assigned two important tasks; the first task is to match the size of secret image with the size of cover image. For example, if the size secret image is smaller than the size of cover image then the prep network has the task of bringing the secret image to the size of cover image. The reason to do this is that as we are using LSB technique for image steganography the data will be kind of hidden in the edges of the cover image. So, now if the image is smaller than cover then it will not be distributed uniformly across the edges if the image. Hence, some parts will contain images and other will not and this will cause unevenness in the pixels. To avoid this the secret image is resized. The second task of prep network is to convert the coloured pixels are converted to grey scale so that it can make optimal use of the regions in image which have high frequency such as the edges of the shapes and image or the textures in image.
- The second phase or the second important network of the designed CNN is the Hiding Network, this network is placed after the prep network and it takes inputs from there. The main function of the hiding network is as the name suggests hiding the secret image into the cover image. Thus the hiding network gets two inputs first is the cover or container image and the second input is the transformed image from the prep network. The container image is an RGB image and the secret image is the image with the transformed channel. The hiding layer is designed with 5 convolution layers or hidden layers and it has 50 filters [3*3, 4*4 and 5*5]
- The last layer or network of the designed CNN is the Revealing Network. As the name suggest, the function of this network is to pull out and reveal the secret image from the container image received as the input from the hiding network.
- There is another layer added to the network for a the purpose of ensuring that all the image are not being encoded in the LSB's. This layer is famous Gaussian noise layer and the gaussian noise layer flips the LSB randomly to create a forced error during the training phase of the network. The impact of this is that the network gets trained to deal with the error and it doesn't hide all the information in just LSB to avoid errors.

6. Evaluation

From below, it can be seen that our deduction from the metric visualization was correct: in the coded image created by the activation function relu and higher learning rate, both the cover and the hidden image are gone. The networks have not optimised, is reasonable to claim. The strange quality of data in the diff cover and diff secret rows can further confirm this.



7. Conclusion

Deep neural network steganography improves existing digital steganography procedures because traditional techniques were easy to decode and there is a relatively limited amount of information that can be buried. This strategy compresses and distributes all available bits of the secret imaging contrary to many of the popular steganographic approaches, that encode the secret message in the least significant bits of the carrier image. Also, adding AES encryption to the technique gives a pretty secure approach to the technique.

8. References

Albawi, S., Mohammed, T. A. and Al-Zawi, S. (2018) 'Understanding of a convolutional neural network', *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, 2018-Janua, pp. 1–6. doi: 10.1109/ICEngTechnol.2017.8308186.

Altaay, A. A. J., Sahib, S. Bin and Zamani, M. (2012) 'An introduction to image steganography techniques', *Proceedings - 2012 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2012*, pp. 122–126. doi: 10.1109/ACSAT.2012.25.

Atee, H. A., Ahmad, R. and Noor, N. M. (2014) 'Combining Cryptography and Steganography for Data Hiding in Images', *conference of Applied Computer and Applied Computational Science (ACACOS)*, 5(12), pp. 128–134.

Bansal, N. *et al.* (2015) 'Comparative analysis of LSB, DCT and DWT for Digital Watermarking', *2015 International Conference on Computing for Sustainable Global Development, INDIACom 2015*, pp. 40–45.

Bidhuri, V., Heffernan, N. and Heffernan, N. (no date) 'Enhancing Password Security Using a Hybrid Approach of SCrypt Hashing and AES Encryption MSc Internship Cyber Security National College of Ireland Supervisor ':

Canziani, A., Paszke, A. and Culurciello, E. (2016) 'An Analysis of Deep Neural Network Models for Practical Applications', pp. 1–7. Available at: http://arxiv.org/abs/1605.07678.

Daemen, J. and Rijmen, V. (1999) 'AES proposal: Rijndael', (December).

Das, A. *et al.* (2021) 'Multi-Image Steganography Using Deep Neural Networks', pp. 1–9. Available at: http://arxiv.org/abs/2101.00350.

Duan, X., Guo, D., *et al.* (2020) 'A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network', *IEEE Access*, 8, pp. 25777–25788. doi: 10.1109/ACCESS.2020.2971528.

Duan, X., Liu, N., *et al.* (2020) 'SteganoCNN: Image steganography with generalization ability based on convolutional neural network', *Entropy*, 22(10), pp. 1–15. doi: 10.3390/e22101140.

Emori, R. I. (1973) 'Scale models of automobile collisions with breakaway obstacles - Investigation indicates that scale models can be used to show the motion of breakaway signposts and lightposts after being struck by automobiles', *Experimental Mechanics*, 13(2), pp. 64–69. doi: 10.1007/BF02322384.

Eyssa, A. A., Abdelsamie, F. E. and Abdelnaiem, A. E. (2020) 'An Efficient Image Steganography Approach over Wireless Communication System', *Wireless Personal Communications*, 110(1), pp. 321–337. doi: 10.1007/s11277-019-06730-2.

Hussain, I. *et al.* (2020) 'A survey on deep convolutional neural networks for image steganography and steganalysis', *KSII Transactions on Internet and Information Systems*, 14(3), pp. 1228–1248. doi: 10.3837/tiis.2020.03.017.

Khan, M. I. and Jeoti, V. (2010) 'A blind watermarking scheme using bitplane of DC component for JPEG compressed images', *Proceedings - 2010 6th International Conference on Emerging Technologies, ICET 2010*, pp. 150–154. doi: 10.1109/ICET.2010.5638498.

Oo, B. B. and Aung, M. T. (2020) 'Enhancing Secure Digital Communication Media Using Cryptographic Steganography Techniques', *Proceedings of the 4th International Conference on Advanced Information Technologies, ICAIT 2020*, pp. 1–6. doi: 10.1109/ICAIT51105.2020.9261790.

Oplatková, Z. *et al.* (2009) 'Detection of steganography inserted by outguess and steghide by means of neural networks', *Proceedings - 2009 3rd Asia International Conference on Modelling and Simulation, AMS 2009*, pp. 7–12. doi: 10.1109/AMS.2009.28.

Pradhan, A. *et al.* (2016) ‘Performance evaluation parameters of image steganography techniques’, *International Conference on Research Advances in Integrated Navigation Systems, RAINS 2016*. doi: 10.1109/RAINS.2016.7764399.
Pujari, M. A. A. and Shinde, M. S. S. (2016) ‘Data Security using Cryptography and Steganography’, *IOSR Journal of Computer Engineering*, 18(04), pp. 130–139. doi: 10.9790/0661-180405130139.
Rothke, B. (2007) ‘A look at the Advanced Encryption Standard (AES)’, *Information Security Management Handbook, Sixth Edition*, pp. 1151–1158. doi: 10.1201/9781439833032.ch89.
Shaik, A., Thanikaiselvan, V. and Amitharajan, R. (2017) ‘Data security through data hiding in images: A review’, *Journal of Artificial Intelligence*, 10(1), pp. 1–21. doi: 10.3923/jai.2017.1.21.
Wei, J. T. *et al.* (1998) ‘Understanding artificial neural networks and exploring their potential applications for the practicing urologist’, *Urology*, 52(2), pp. 161–172. doi: 10.1016/S0090-4295(98)00181-2.