COMPARISON OF LSB AND CNN FOR IMAGE STEGANOGRAPHY

A PROJECT REPORT

Submitted By

MUKILAN.A.R. 312215104062

NIKHIL NEROOR 312215104064

SHARAJ J 312215104701

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

SSN COLLEGE OF ENGINEERING

KALAVAKKAM 603110

ANNA UNIVERSITY :: CHENNAI - 600025

April 2019

ANNA UNIVERSITY : CHENNAI 600025

BONAFIDE CERTIFICATE

Certified that this project report titled **"COMPARISON OF LSB AND CNN FOR IMAGE STEGANOGRAPHY"** is the *bonafide* work of "**MUKILAN A.R. (312215104062)**, **NIKHIL NEROOR (312215104064)**, and **SHARAJ J (312215104701)**" who carried out the project work under my supervision.

Dr. CHITRA BABU
HEAD OF THE DEPARTMENT
Professor,
Department of CSE,
SSN College of Engineering,
Kalavakkam - 603 110

Ms. S. MANISHA
SUPERVISOR
Assistant Professor,
Department of CSE,
SSN College of Engineering,
Kalavakkam - 603 110

Place:
Date:

Submitted for the examination held on. . . . . .

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENTS

We thank GOD, the almighty for giving me strength and knowledge to do this project.

We would like to thank and deep sense of gratitude to our guide **Ms. S. MANISHA**, Assistant Professor, Department of Computer Science and Engineering, for her valuable advice and suggestions as well as her continued guidance, patience and support that helped us to shape and refine our work.

My sincere thanks to **Dr. CHITRA BABU**, Professor and Head of the Department of Computer Science and Engineering, for her words of advice and encouragement.

We express our deep respect to the founder **Dr. SHIV NADAR**, Chairman, SSN Institutions. We also express our appreciation to our **Dr. S. SALIVAHANAN**, Principal, for all the help he has rendered during this course of study.

We would like to extend our sincere thanks to all the teaching and non-teaching staffs of our department who have contributed directly and indirectly during the course of our project work. Finally, I would like to thank our parents and friends for their patience, cooperation and moral support throughout our life.

MUKILAN A.R. **NIKHIL NEROOR.** **SHARAJ J**

ABSTRACT

Securing data over wireless transmissions is an urgent need in the field of data communication. The protection of information over the wireless networks is done by encrypting the information with the use of Cryptographic Algorithms. But due to advancements in computing techniques the cipher messages can be easily detected and the algorithms used for Cryptographic encryption and decryption are well known to all in the computer field. So to avoid attacks from the unintended users, the presence of secret information must be masked. It helps the recipient to protect the message from the hackers. When it comes to image data, it is more susceptible to attacks because there aren't many unknown methods available to encrypt it and transmit it safely over a network. However, in this project we have focussed on one of the methods for hiding the presence of the secret image data which is known as Steganography. This project focuses on hiding an image using another image known as Cover Image and encrypting a message within that image. The experiment is done using various flavours of Least Significant Bit approach (1-Bit, 4-Bit) and Deep Steganographic method of using CNN for the same experiment, and the results are compared.

TABLE OF CONTENTS

LIST OF FIGURES vii

LIST OF TABLES viii

1 INTRODUCTION 1

1.1 Types of Steganography 2

1.1.1 Text Steganography 3

1.1.2 Image Steganography 3

1.1.3 Audio Steganography 3

1.1.4 Video Steganography 4

1.1.5 Protocol Steganography 4

1.2 Applications of Steganography 4

1.2.1 Secret Communications 4

1.2.2 Feature Tagging 4

1.2.3 Copyright Protection 5

1.3 Methods for Steganographic Implementations 5

1.4 Problems with existing methods 5

2 LITERATURE SURVEY 7

2.1 1 Bit LSB 7

2.1.1 An Overview 7

2.1.2 Characterizing Data Hiding 9

2.2 4 Bit LSB 11

2.2.1 An Overview 11
2.2.2 Secure Data Hiding 14
2.3 The Neural Network 14
2.3.1 Introduction to Neural Network 14

3 LEAST SIGNIFICANT BIT 17
3.1 1 Bit LSB 17
3.1.1 LSB Encoder 17
3.1.2 LSB Decoder 18
3.2 4 Bit LSB 19
3.2.1 LSB Technique 19
3.2.2 Basic Architecture 23
3.2.3 Algorithm : Image Encoding 24
3.2.4 Data Extraction 25
3.2.5 Problems with existing methods 26

4 CNN FOR DEEP STEGANOGRAPHY 27
4.1 CNN Architecture Overview 27
4.1.1 Convolution Layer 27
4.1.2 Non-Linearity Layer 28
4.1.3 Pooling Layer 28
4.1.4 Fully Connected Layer 29
4.2 Proposed system 29
4.3 Error Propagation 30
4.4 Performance Evaluation 32
4.5 Limitations 33

5 CONCLUSION AND FUTURE WORK 34

REFERENCES 35

LIST OF FIGURES

2.1 LSB Steganography 13
2.2 Block Diagram of Steganographic Process 14

3.1 Sample of LSB Steganography 20
3.2 LSB Steganography Algorithm 21
3.3 Cover Image 22
3.4 Secret Image 22
3.5 Stego Image 23
3.6 Extracted Image 23
3.7 4 bit LSB 24

4.1 Basic Architecture 27
4.2 Proposed System 30
4.3 Design Parameters 30
4.4 Error 31
4.5 Deep Steganography using CNN for NIPS 2017 dataset 32

LIST OF TABLES

3.1 Comparison of Steganographic features between 1 bit, 4 bit LSB Techniques 25

4.1 Comparison of Steganographic features between 1 bit, 4 bit and Deep Steganography using CNN 33

CHAPTER 1

INTRODUCTION

The word “Steganography” is of Greek origin and means “covered or hidden writing”. The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography and cryptography are counter parts in digital security the obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. Also, the last decade has seen an exponential growth in the use of multimedia data over the Internet. These include Digital Images, Audio and Video files. This rise of digital content on the internet has further accelerated the research effort devoted to steganography.

The initial aim of this study was to investigate steganography and how it is implemented. Based on this work a number of common methods of steganography could then be implemented and evaluated. The strengths and weaknesses of the chosen methods can then be analysed. To provide a common frame of reference all of the steganography methods implemented and analysed used GIF images. To make a steganographic communication even more secure the message can be compressed and encrypted before being hidden in the carrier.

Cryptography and steganography can be used together. If compressed the message will take up far less space in the carrier and will minimise the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography.

Steganography refers to the science of “invisible” communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding some information in digital content has a wider class of applications that go beyond steganography.

In order to defeat the steganalytic attacks, algorithms have been proposed which try to restore the statistics which get distorted during the embedding procedure and which may be used for steganalysis.

While Cryptography does encrypt any given data, it does not hide the fact that classified information is being transmitted to another source. Furthermore, the cryptographic algorithms used to encrypt and decrypt data are well known to all who work in the field of computers and it simply takes knowing which algorithm has been used for encrypting that particular data, which in turn will allow hackers and the like to simply perform the reverse process and illegally obtain the information. Hence, Cryptography is at a disadvantage. Hence, this system attempts to secure classified data by using the concept of Steganography, which does not encrypt the data like in Cryptography, rather, it hides the existence of any secret information by hiding the data in another media entity, such as an image.

1.1 Types of Steganography

In modern approach, depending on the cover medium, steganography can be divided into five types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography 5. Protocol Steganography

1.1.1 Text Steganography

Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

1.1.2 Image Steganography

Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but cant see the existence of the hidden message.

1.1.3 Audio Steganography

Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information [2]. Existing audio steganography software can embed messages in WAV and MP3 sound files.

1.1.4 Video Steganography

Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.

1.1.5 Protocol Steganography

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

1.2 Applications of Steganography

1.2.1 Secret Communications

The use of steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

1.2.2 Feature Tagging

Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

1.2.3 Copyright Protection

Copy protection mechanisms that prevent data, usually digital data, from being copied.The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

1.3 Methods for Steganographic Implementations

There are many available methods to implement Steganography, such as Spiht Based Method, LSB replacement technique, MSB replacement technique, Spatial Domain Technique etc. However, the best technique to use has always been LSB replacement technique, which is being used in this project. It has been explained in detail in the forthcoming chapters. The current existing methods have some discrepancies, which have been mentioned below.

1.4 Problems with existing methods

Current methods that hide images in other images already exist, but there are a few problems associated with these. They are very easy to decode, as the way information is encoded, is fixed. The amount of information that can be hidden is generally less. Hiding an image of the same size will probably lose a fair bit of information. In the case of Images, the algorithms dont exploit the structure of images. They dont use the patterns found in natural images.

The best way to solve these problems is to perform Steganography using Deep Learning, by means of a Convolutional Neural Network. This will be discussed in further detail later.

In layman's terms, Steganography can be defined as "masking the existence of secret information." There are many algorithms available to perform Steganography. In this project, we will be using the Least Significant Bit(abbreviated as LSB) technique to perform Steganography. In addition, we will be designing a Convolutional Neural Network to perform the same Steganography and perform a comparative study of the results obtained from the LSB technique and the CNN.

CHAPTER 2

LITERATURE SURVEY

2.1 1 Bit LSB

2.1.1 An Overview

With the growth of computer network, security of data has become a main concern and thus data hiding technique has concerned people around the world. Steganography techniques are used to deal with digital copyrights management, protect information, and conceal secrets. Data hiding techniques provide a motivating challenge for digital forensic investigators[5]. Data is the backbone of todays communication. To ensure that data is secured and does not go to unplanned destination, the concept of data hiding came up to protect a part of information. Digital data can be delivered over computer networks with little errors and often without interference.

The Internet provides a communication method to distribute information to the masses. Therefore, the privacy and data reliability are required to protect against unauthorized access and use. Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between recognized parties. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a considerably larger object so that the change is undetectable by the human eye. All digital file formats can be used for steganography, but the formats those

are with a high scale of redundancy are more suitable. The redundant bits of an object are those bits that can be distorted without the alteration being detected easily[16].

The most popular cover objects used for steganography are digital images. Digital images often have a huge amount of redundant data, and this is what steganography uses to hide the message. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited[17]. To conceal a message inside an image without changing its perceptible properties, the cover source can be altered in noisy areas with many color variations, so less concentration will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image.

These techniques can be used with unreliable degrees of success on different types of image files. The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the paper is to hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the intention securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data encryption into an image and decryption and steganography plays an important role in this paper. Since, from the first written communication secrecy is the ultimate goal for men to maintain their integrity and confidentiality.

In the past, messages could easily be intercepted and there were no secrecy devices, so the third party was able to read the message. During the time of the Greeks, around 500 B.C., when Demaratus first used the technique of steganography. The word Steganography derived from two Greek words steganos, meaning covered, and graphein, meaning to write. As the name says steganography has a cover medium to hold the secret message without showing its explicit it passes the message from one end to another end[6]. The goal of Steganography is to avoid drawing suspicion to the transmission of a hidden message.

Steganography encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as covers or carriers to hide secret messages.

2.1.2 Characterizing Data Hiding

Steganography is a kind of technique which can embed a message inside a cover object. There are a number of features that characterizes the merits and demerits of the embedding techniques. The way they are applied decides the importance of

each and every feature. A set of criteria are proposed to define the invisibility of an algorithm. The criteria are as follows:

2.1.2.1 Invisibility

The imperceptibility of a Steganography technique is the most important necessity, since the quality of Steganography lies in its capacity to be unseen by the naked eyes.

2.1.2.2 Payload Capacity

Steganography techniques used aim at hiding the embedded secret data and also maximize the amount of information embedded. The amount of information that is hidden is called payload capacity.

2.1.2.3 Hiding Capacity

Concealing capacity is nothing but the size of data that could be concealed with respect to the size of the cover object. A vast concealing capacity permits the use of smaller cover images and thus decreases the data transmission needed to broadcast the Stego image.

2.1.2.4 Perceptual Transparency

The inability of an eavesdropper to detect hidden data is referred by Perceptual transparency.

2.2 4 Bit LSB

2.2.1 An Overview

Data hiding techniques provide a motivating challenge for digital forensic investigators. Data is the backbone of todays communication. To ensure that data is secured and does not go to unplanned destination, the concept of data hiding came up to protect a part of information. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Therefore, the privacy and data reliability are required to protect against unauthorized access and use. Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between recognized parties. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a considerably larger object so that the change is undetectable by the human eye.

All digital file formats can be used for steganography, but the formats those are with a high scale of redundancy are more suitable. The redundant bits of an object are those bits that can be distorted without the alteration being detected easily. The most popular cover objects used for steganography are digital images[9]. Digital images often have a huge amount of redundant data, and this is what steganography uses to hide the message. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To conceal a message inside an image

without changing its perceptible properties, the cover source can be altered in noisy areas with many color variations, so less concentration will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image[10]. These techniques can be used with unreliable degrees of success on different types of image files.

The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the paper is to hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the intention securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data encryption into an image and decryption and steganography plays an important role in this paper. Since, from the first written communication secrecy is the ultimate goal for men to maintain their integrity and confidentiality. In the past, messages could easily be intercepted and there were no secrecy devices, so the third party was able to read the message. During the time of the Greeks, around 500 B.C., when Demaratus first used the technique of steganography. The word Steganography derived from two Greek words steganos, meaning covered, and graphein, meaning to write[3].

As the name says steganography has a cover medium to hold the secret message without showing its explicit it passes the message from one end to another end. The goal of Steganography is to avoid drawing suspicion to the transmission of a hidden message. Steganography encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very

existence of the embedded messages is undetectable[20]. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages[11]. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as covers or carriers to hide secret messages.

The basic working of LSB Steganography is shown by the following Figures 2.1 and 2.2.

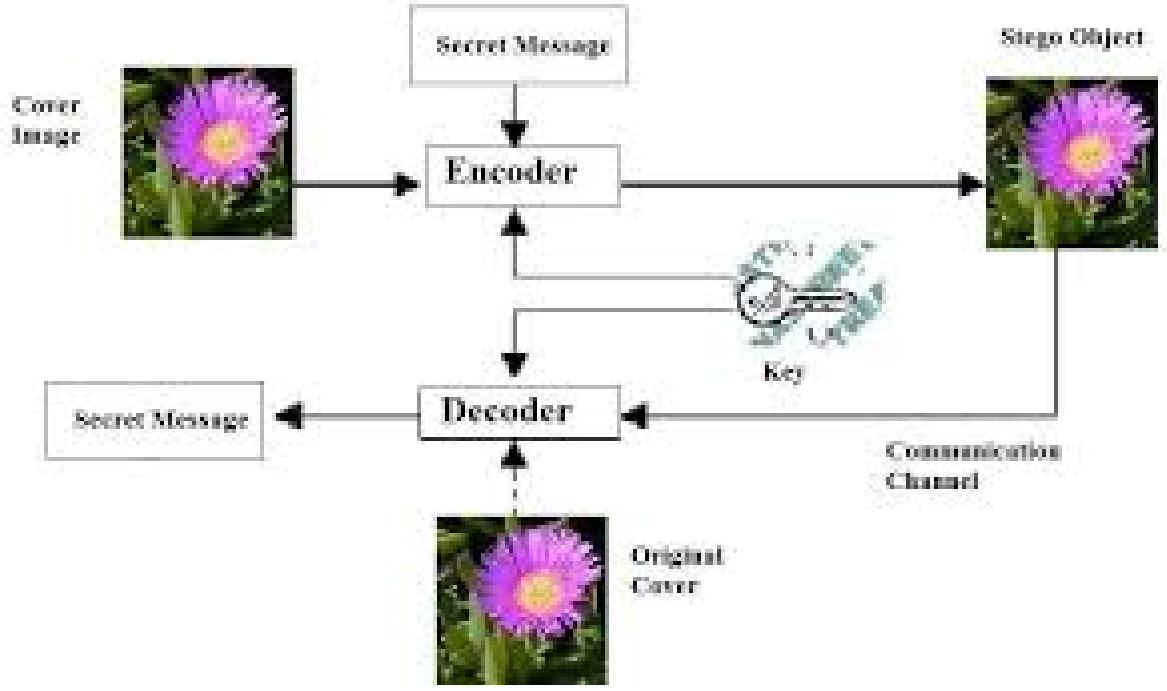

FIGURE 2.1: LSB Steganography

Note that the secret key shown in both diagrams is optional and only needed if the developer wishes to perform a combination of Steganography and Cryptography. This will be highly beneficial but extremely tough to implement and will also have insanely high complexity.

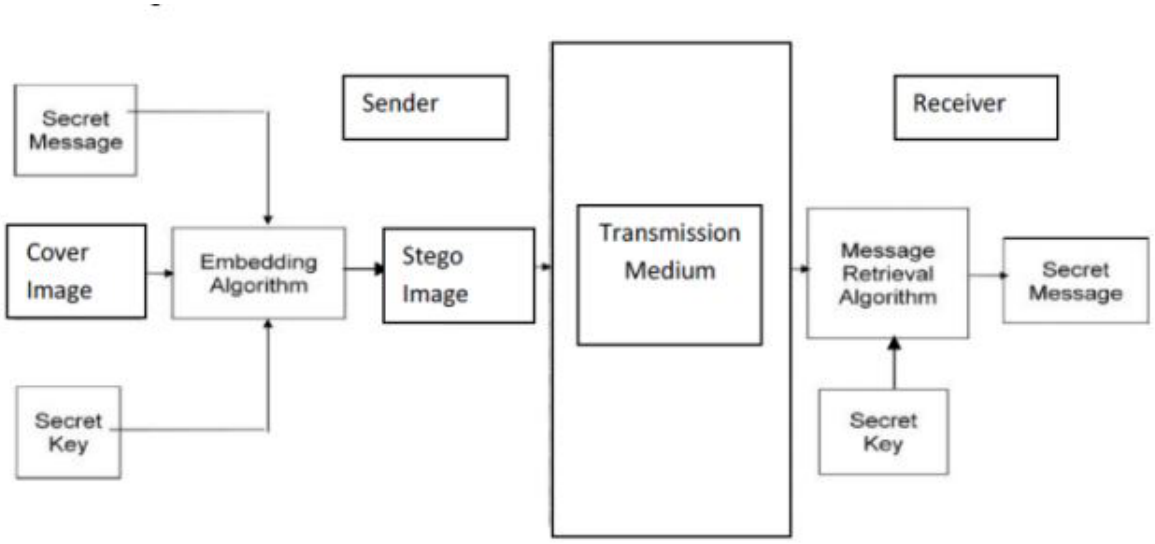

FIGURE 2.2: Block Diagram of Steganographic Process

2.2.2 Secure Data Hiding

An information hiding system has been developed for confidentiality. However, in this chapter, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image. The implementation of system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below.

2.3 The Neural Network

2.3.1 Introduction to Neural Network

Convolutional Neural Network (CNN) is a deep learning architecture which is inspired by the structure of visual system. In 1962, Hubel and Wiesel [1] in their classic work on cats primary visual cortex found that cells in the visual cortex are

sensitive to small sub-regions of the visual field called as receptive field. These cells are responsible for detecting light in the receptive fields. Neocognitron proposed by Fukushima was the first model which was simulated on a computer and was inspired from the works of Hubel and Wiesel. This network is widely considered as a predecessor of CNN and it was based on the hierarchical organization between neurons for the transformation of image. LeCun et al.[4] established the framework of CNNs by developing a multi-layer artificial neural network called as LeNet-5.

LeNet-5 was used to classify handwritten digits and could be trained with the backpropagation algorithm which made it possible to recognize patterns directly from raw pixels thus eliminating a separate feature extraction mechanism. But even with all these advantages, due to the lack of large training data and computational power at that time, LeNet-5 failed to perform well on complex problems such as video classification. Since the advent of GPGPUs and their use in machine learning, the field of CNN has gone through a renaissance phase. Several publications have established more efficient ways to train convolutional neural networks using GPU computing[7,8]. Krizhevsky et al. proposed a deep CNN architecture called as AlexNet[10] which demonstrated significant improvement in image classification task. AlexNet is very similar to the classic LeNet-5 albeit a deeper structure.

Following the success of AlexNet several publications such as GoogleNet, VGGNet[12], ZFNet[13] and ResNet[14] have shown to improve its performance. Recurrent Neural Networks (RNN) are generally applied to solve Natural Language Processing (NLP) problems[15] since RNNs resemble how human beings process language. But recently, CNNs which seem less intuitive in solving

such problems than RNNs have been applied to solve NLP problems such as sentiment analysis, spam detection or topic categorization. CNNs have achieved state-of-art or competitive results. CNNs have also been applied to the problem of speech recognition which essentially is a major researched task in NLP.

Speech which is the spectral representation of spoken words consists of several hundred variables and generally face problems of overfitting when trained using fully connected feed-forward networks[18]. They also do not have built-in invariance with respect to translations[19]. These architectures also entirely ignore the topology or hierarchy of the input. On the other hand, in CNN, shift variance is automatically obtained and it also forces the extraction of local features thus improving the performance with respect to traditional architectures.

CHAPTER 3

LEAST SIGNIFICANT BIT

3.1 1 Bit LSB

3.1.1 LSB Encoder

The easiest way to embed secret information within the cover file is called LSB insertion. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used, then the quantity of modification will be small. As an example, supposing that we have three neighbouring pixels (nine bytes) with the following RGB encoding:

Now if we wish to embed the following 9 bits of compressed secret information: 010010011. If we insert these 9 bits over the LSB of the 9 bytes above, we get the following sequence of bits:

The LSB Encoding Algorithm works as follows.

- Step-1: Read the cover image and secret image which is to be embedded in to the cover image.

01101010	11110010	00110110
01101001	11110000	00110101
01100000	11101111	00110100

01101010 11110011 00110110
01101000 11110001 00110100
01100000 11101111 00110101

- Step-2: Compress the secret image.

- Step-3: Convert the pixel block values compressed secret image into binary form.

- Step-4: Find LSBs of each RGB pixels of the cover image.

- Step-5: Embed the bits of the secret information into least significant bits of RGB pixels of the cover image.

- Step-6: Continue the procedure until the secret image is fully hidden into the cover image.

3.1.2 LSB Decoder

First, Stego-Image is taken and single array of bytes are generated as it was done at the time of encoding. The total number of bits of encrypted secret information and the bytes representing the pixels of stego-image are taken. Counter is initially set to 1, which in turn gives the index number of the pixel byte where secret message bit is available in LSB. The process is continued till final count of secret message bit is reached. After this, the bit stream of the message shall be generated. Available bits are grouped to form bytes such that each byte represents single ASCII character. Characters are stored in text file which represents the

encrypted embedded message. After that the decryption and decompression are to be performed. The Algorithm for extracting the secret file from the Stego Image is given below.

- Step-1: Read the stego image.
- Step-2: Find LSBs of each RGB pixel of the stego image.
- Step-3: Find and retrieve the LSBs of each RGB pixel of the stego image.
- Step-4: Continue the process until the message is fully extracted from stego image.
- Step-5: Decompress the extracted secret data.
- Step-6: Reconstruct the secret information.

Figure 3.1 gives the basic idea of how the output for LSB Steganographic Technique will look.

3.2 4 Bit LSB

3.2.1 LSB Technique

The least significant bits (in other words, the 4 rightmost bits) of some or all of the bytes inside an image are changed to bits of the secret message.Digital images

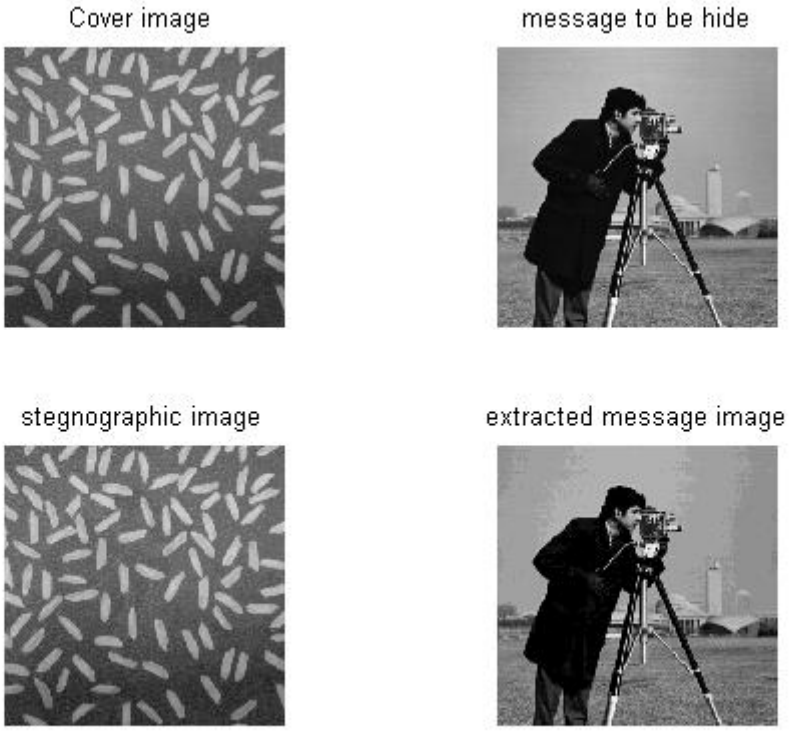

FIGURE 3.1: Sample of LSB Steganography

are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed 12 bits of information in each pixel, four in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, 4 bits of information can be hidden. The procedure how LSB Steganography Algorithm work is depicted in Figure 3.2.

The Cover Image and Secret Image have been shown in the figures below. A Stego Image is obtained by applying LSB Encoding technique on both the Cover and Secret Image. The secret is extracted by applying LSB Decoding Technique on the Stego Image. If the LSB of the pixel value of cover image C(i,j) is equal to the

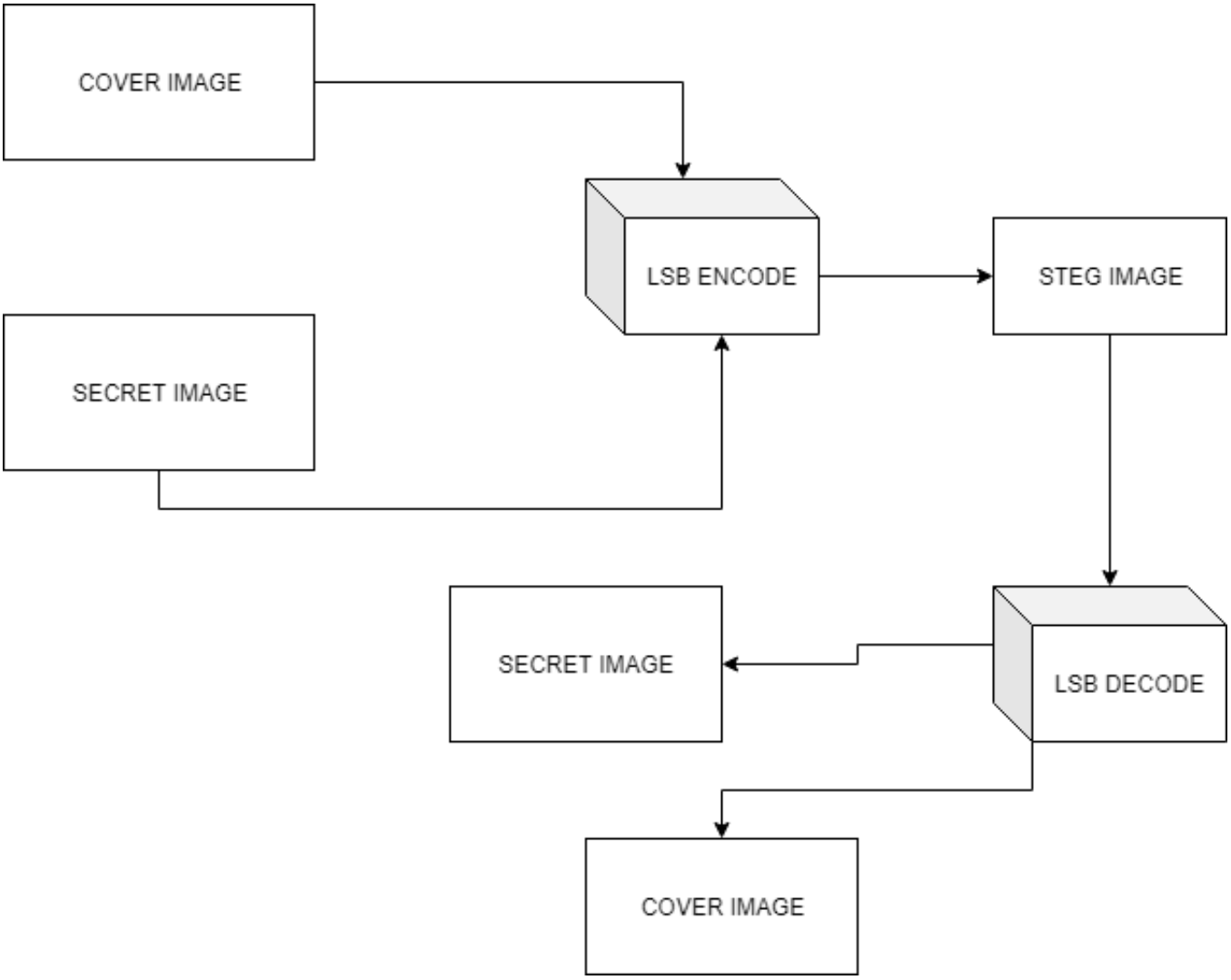

FIGURE 3.2: LSB Steganography Algorithm

message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below.

- S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0
- S(i.j) = C(i,j), if LSB(C(i,j)) = m
- S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded. S(i,j) is the stego image. Figure 3.5 represents the Stego Image.

FIGURE 3.3: Cover Image

FIGURE 3.4: Secret Image

FIGURE 3.5: Stego Image

FIGURE 3.6: Extracted Image

3.2.2 Basic Architecture

A sample input output has been shown below along with the basic architecture of the system in Figure 3.7.

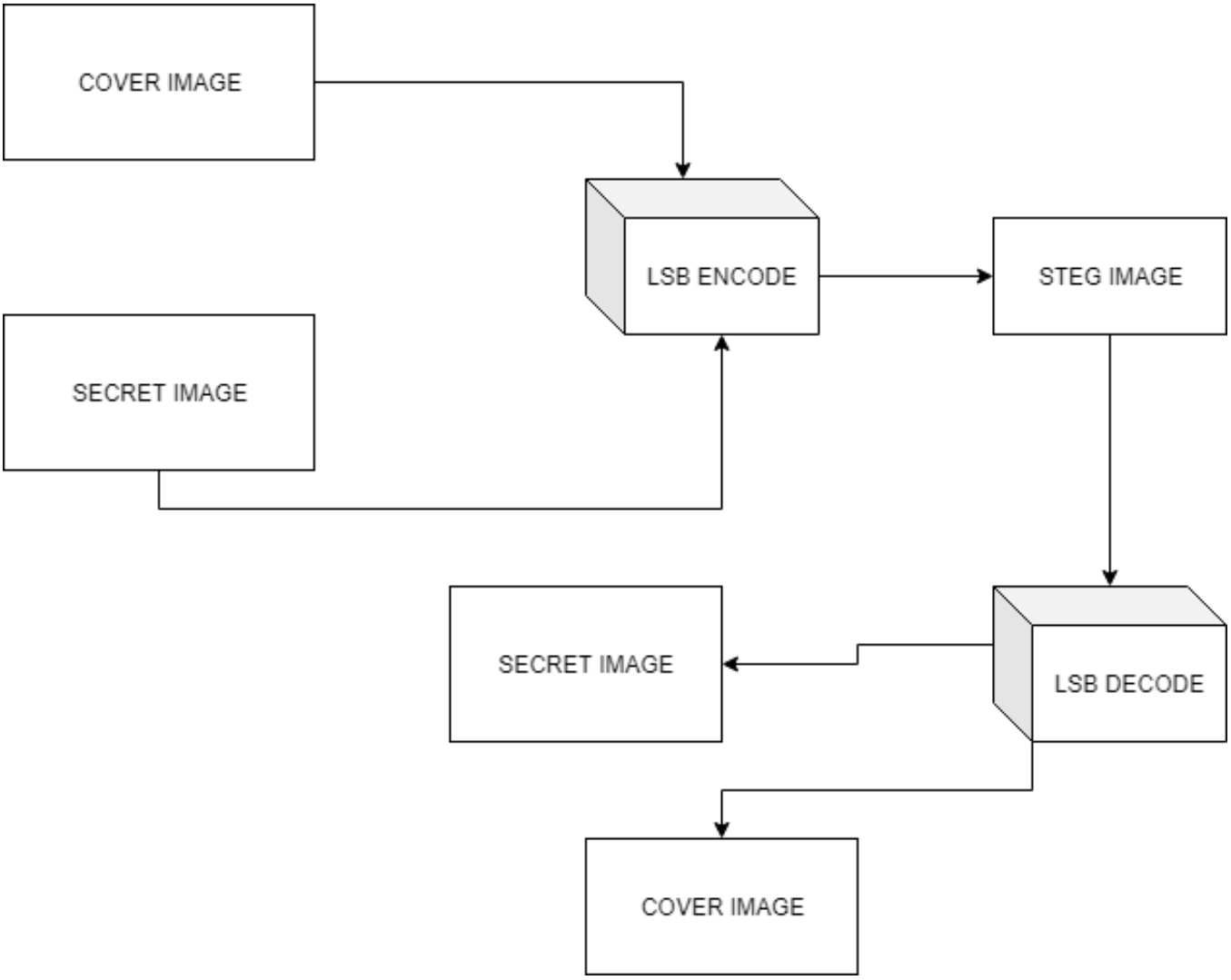

FIGURE 3.7: 4 bit LSB

3.2.3 Algorithm : Image Encoding

Inputs: Image file(cover) and image file(secret); **Output:** Stego image.

The cover and secret images are read and converted into the unit8 type. The numbers in secret image matrix are conveyed to 8-bit binary. Then the matrix is reshaped to a new matrix a. The matrix of the cover image given in Figure 3.3 is also reshaped to matrix b Perform the LSB technique as described for 1 bit lsb. The stego-image, which is very similar to the original cover image, is achieved.

While extracting the data, the LSB of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image as given in Figure 3.4.

3.2.4 Data Extraction

Inputs: Stego-image file

Output: Secret image

Firstly, extract the pixels of the Stego Image in Figure 3.5. Next, extract the 4 LSBs of all the pixels until the terminating sign comes up. Using the extracted LSB values, the secret image Figure 3.6 can be obtained.

The 4 bit LSB algorithm works in exactly the same manner as the 1 bit LSB algorithm, except for the fact that in this case, instead of replacing just the rightmost bit of the cover with the secret data, we will be replacing the four rightmost bits with the secret data. The below Table 3.1 gives comparison between 1 bit and 4 bit LSB techniques.

Type	**Imperceptibility**	**Robustness**	**Capacity**	**Tamper Resistance**
1 bit LSB	High	Low	High	Low
4 bit LSB	High	Low	Higher	Low

TABLE 3.1: Comparison of Steganographic features between 1 bit, 4 bit LSB Techniques

3.2.5 Problems with existing methods

Current methods that hide images in other images already exist, but there are a few problems associated with these. They are very easy to decode, as the way information is encoded , is fixed. The amount of information that can be hidden is generally less. Hiding an image of the same size will probably lose a fair bit of information. In the case of Images, the algorithms dont exploit the structure of images. They dont use the patterns found in natural images.

Hence, we propose using deep learning in Steganography with the use of a Convolutional Neural Network, by which we will attempt to eliminate these discrepancies.

CHAPTER 4

CNN FOR DEEP STEGANOGRAPHY

4.1 CNN Architecture Overview

CNN architecture differs from the traditional multi-layer perceptrons (MLP) to ensure some degree of shift and distortion invariance [16]. They combine three architectural ideas to do the same: Local Receptive Fields, Shared weights and Spatial and Temporal Sub-sampling. We have mentioned many CNN architectures in the literature but their basic components are very similar. Let us consider the typical convolutional network architecture for recognizing characters given in Figure 4.1.

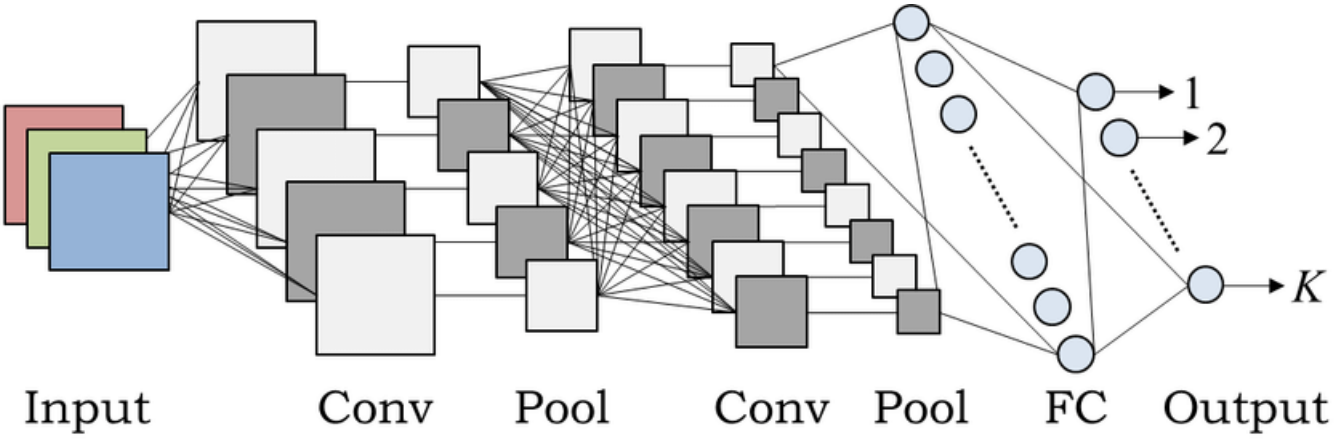

FIGURE 4.1: Basic Architecture

4.1.1 Convolution Layer

This layer is the core building block of a CNN. The layers parameters consist of learnable kernels or filters which extend through the full depth of the input. Each

unit of this layer receives inputs from a set of units located in small neighbourhood in the previous layer. Such a neighbourhood is called as the neurons receptive field in the previous layer. During the forward pass each filter is convolved with input which produces a map. When multiple such feature maps that are generated from a multiple filters are stacked they form the output of the convolution layer. The weight vector that generates the feature map is shared which reduces the model complexity.

4.1.2 Non-Linearity Layer

This is a layer of neurons which apply various activation functions. These functions introduce nonlinearities which are desirable for multi-layer networks. The activation functions are typically sigmoid, tanh and ReLU. Compared to other functions Rectified Linear Units (ReLU)[17] are preferable because neural networks train several times faster.

4.1.3 Pooling Layer

The Convolution layer may be followed by the pooling layer which takes small rectangular blocks from the convolution layer and subsamples it to produce a single maximum output from the block[19-21]. Pooling layer progressively reduces the spatial size of the representation, thus reducing the parameters to be computed. It also controls overfitting. Pooling units apart from the maximum function can also perform other functions like average[18] or L2-norm pooling.

4.1.4 Fully Connected Layer

There maybe one or more fully-connected layers that perform high level reasoning by taking all neurons in the previous layer and connecting them to every single neuron in the current layer to generate global semantic information.

4.2 Proposed system

Convolutional Neural Networks have shown to learn structures that correspond to logical features. These features increase their level of abstraction as we go deeper into the network. Using a ConvNet will solve all the problems mentioned above. Firstly, the ConvNet will have a good idea about the patterns of natural images, and will be able to make decisions on which areas are redundant, and more pixels can be hidden there. By saving space on redundant areas, the amount of hidden information can be increased. Because the architecture and the weights can be randomised, the exact way in which the network will hide the information cannot be known to anybody who does not have the weights.

The entire network architecture is surprisingly similar to Auto Encoders. In general, auto-encoders are made to reproduce the input after a series of transformations. By doing this, they learn about the features of the input distribution. In this case, the architecture is slightly different. Instead of merely reproducing images, the architecture has to hide an image , as well as reproduce another image.

The neural network being designed for this system contains the following parameters as shown in the Figure 4.2 and 4.3.

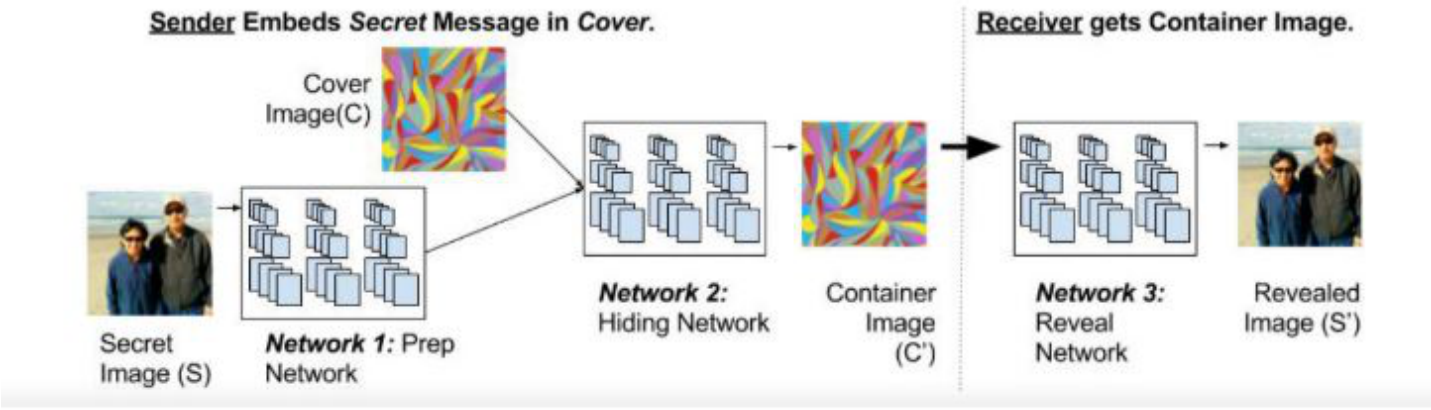

FIGURE 4.2: Proposed System

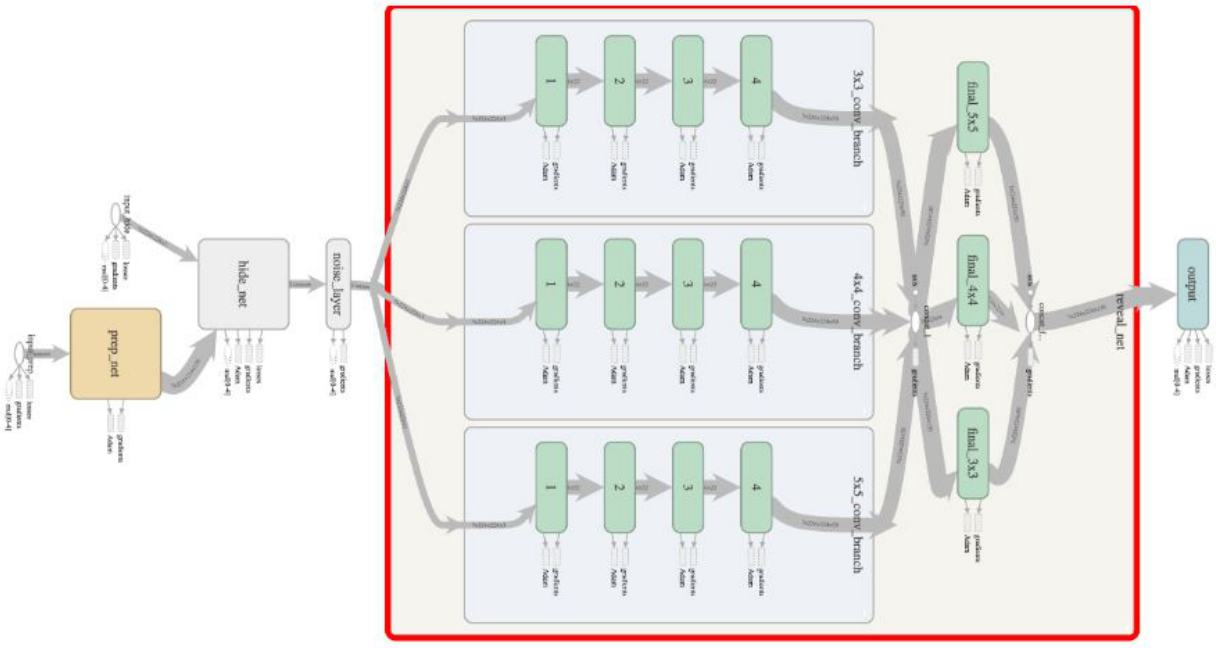

FIGURE 4.3: Design Parameters

4.3 Error Propagation

As mentioned earlier, our approach borrows heavily from auto-encoding networks; however, instead of simply encoding a single image through a bottleneck, we encode two images such that the intermediate representation (the

container image) appears as similar as possible to the cover image. The system is trained by reducing the error shown in Figure 4.4 below (c and s are the cover and secret images respectively, and is how to weigh their reconstruction errors):

L(c, c0, s, s0) = (c c')+ (s s')

It is important to note where the errors are computed and the weights that each error affects, see Figure 4.3. In particular, note that the error term ——c c—— does not apply to the weights of the reveal network that receives the container image and extracts the secret image. On the other hand, all of the networks receive the error signal (s s') for reconstructing the hidden image. This ensures that the representations formed early in the preparation network as well as those used for reconstruction of the cover image also encode information about the secret image.

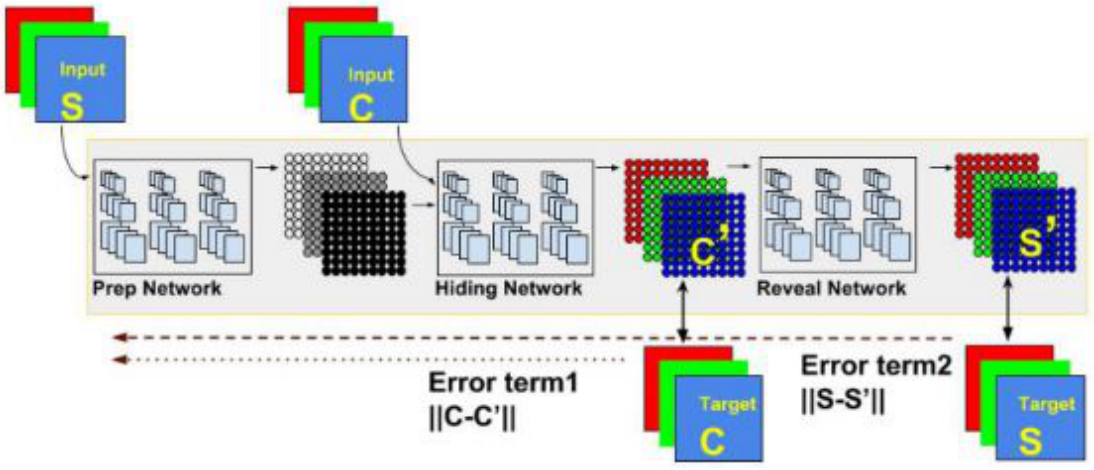

FIGURE 4.4: Error

The three networks are trained as a single, large, network. Error term 1 affects only the first two networks. Error term 2 affects all 3. S is the secret image, C is the cover image.

4.4 Performance Evaluation

The neural network causes almost no distortion in the edited and extracted images. Furthermore, the distortion is practically invisible to the naked eye, as shown in the following Figure 4.5.

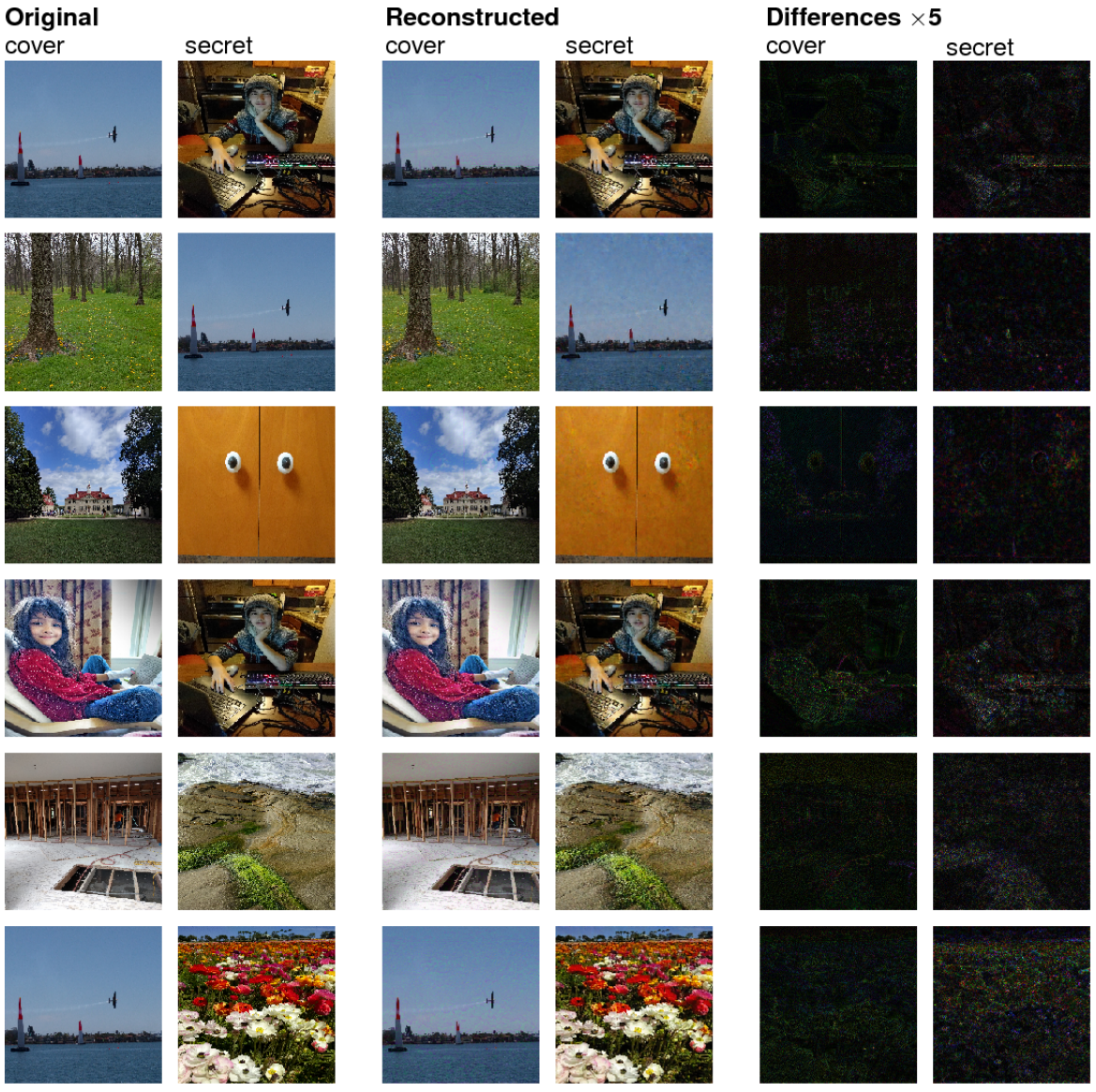

FIGURE 4.5: Deep Steganography using CNN for NIPS 2017 dataset

The following Tabe 4.1 gives the comparison between 1 bit, 4 bit LSB Steganography and Deep Steganography using CNN.

Type	**Imperceptibility**	**Robustness**	**Capacity**	**Tamper Resistance**
1 bit LSB	High	Low	High	Low
4 bit LSB	High	Low	Higher	Low
Neural Network	Very High	Low	Highest	High

TABLE 4.1: Comparison of Steganographic features between 1 bit, 4 bit and Deep Steganography using CNN

4.5 Limitations

Unfortunately, there is a limitation to this method, although it is extremely unlikely to occur. Like all CNNs, no matter how much training is done, the output will never be 100 percent perfect and there will always be one odd image which will not respond as it should to the system. However, the more you train the Neural Network, the less likely this is to happen.

CHAPTER 5

CONCLUSION AND FUTURE WORK

In this thesis, we have explained and compared the working and benefits of 1 bit LSB Steganography, 4 bit LSB Steganography, and Deep Steganography using a Convolutional Neural Network(CNN). This study opens a new avenue for exploration with steganography and, more generally, in placing supplementary information in images. Several previous methods have attempted to use neural networks to either augment or replace a small portion of an image-hiding system. We have demonstrated a method to create a fully trainable system that provides visually excellent results in unobtrusively placing a full-size, color image into another image. Although the system has been described in the context of images, the same system can be trained for embedding text, different-sized images, or audio.Additionally, by using spectrograms of audio-files as images, the techniques described here can readily be used on audio samples. There are many immediate and long-term avenues for expanding this work.

Three of the most immediate are listed here. (1) To make a complete steganographic system, hiding the existence of the message from statistical analyzers should be addressed. This will likely necessitate a new objective in training (e.g. an adversary), as well as, perhaps, encoding smaller images within large cover images. (2) The proposed embeddings described in this paper are not intended for use with lossy image files. If lossy encodings, such as jpeg, are required, then working directly with the DCT coefficients instead of the spatial domain is possible. (3) For simplicity, we used a straightforward SSE error metric

for training the networks; however, error metrics more closely associated with human vision, such as SSIM, can be easily substituted.

REFERENCES

1. Ali, K., Hamid, A., Kasirun, Z.M., Zaidan, A.A. and Zaidan, B.B. (2010) 'On the capacity and security of Steganography approaches: An overview', Journal of Applied Sciences, Vol. 10, pp. 1825-1833.

2. Baluja, S. (2017) 'Hiding images in plain sight: Deep steganography'. Advances in Neural Information Processing Systems, Vol. 30, pp. 2069-2079.

3. Bandyopadhyay, B., Das, S., Das, S. and Sugata, S. (2008) 'Steganography and Steganalysis: Different Approaches', International Journal of Computers, Information Technology and Engineering, Vol. 2, No. 1, pp.312-318.

4. Behal, S. and Kaur, N. (2014) 'A Survey on various types of Steganography and Analysis of Hiding Techniques', International Journal of Engineering Trends and Technology, Vol. 11, No. 8, pp. 388-392.

5. Bengio, Y., Courville, A., Goodfellow, I., Mirza, M., Ozair, S., Pouget-Abadie, J., Warde-Farley, D. and Xu, B. (2014) 'Generative adversarial nets', In Proceedings of Conference on Neural Information Processing Systems, pp. 2672-2680.

6. Bin, L., Donghui, H., Liang, W., Zheng, S. and Zhiang, W. (2018) 'A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks', IEEE Access, Vol. 6, pp. 38303-38314.

7. Chang, C., Li, L., Liu, Z. and Wang, A., (2017) 'A secret image sharing with deep-steganography and two-stage authentication based on matrix encoding', International Journal of Network Security, Vol. 19, pp. 327-334.

8. Danezis, G. and Hayes, J. (2017) ‘Generating steganographic images via adversarial training’, In Proceedings of Conference on Neural Information Processing Systems, pp.1954-1963.

9. Devi, K. J. (2013) ‘Secure Image Steganography Using LSB Technique’ B.Tech. Thesis, NIT Rourkela.

10. Devi, S. and Thangadurai (2014) ‘An analysis of LSB based image steganography techniques’, In Proceedings of International Conference on Computer Communication and Informatics, pp. 1-4.

11. Dipti, S. and Rashmi, A. S. (2017) ‘Reversible Texture Synthesis Using Three Level Security in Steganography’, International Journal of Scientific Research in Science and Technology, Vol. 3, pp. 105-109.

12. Gagnani, L., Joshi, R. and Pandey, S. (2013) ‘Image Steganography With LSB’, International Journal of Advanced Research in Computer Engineering and Technology, Vol. 2, No. 1, pp. 228.

13. Guanshuo, X., Han-Zhou, W. and Yun-Qing, S. (2016) ‘Structural Design of Convolutional Neural Networks for Steganalysis’, IEEE Signal Process Letters, Vol. 23, pp. 708-712.

14. Han-Zhou, W., Hong-Xia, W. and Yun-Qing, S. (2016) ‘Can Machine Learn Steganography’, Computing Research Repository (CoRR), arXiv:1606.05294.

15. Haripriya, R. and Mishra, B.K. (2004) ‘Pros and Cons of Cryptography, Steganography and Perturbation techniques, IOSR Journal of Electronics and Communication Engineering, Vol. 3, pp. 76-81.

16. Kakde, V and Sagar, S.P. (2015) ‘Review on Steganography for Hiding Data’, International Journal of Computer Science and Mobile Computing, Vol. 3, No. 4, pp. 225-229.

17. Pin. W., Xiaoqiang, L. and Yang, Y. (2018) 'StegNet: Mega Image Steganography Capacity with Deep Convolutional Network', Future Internet, Vol. 10, No. 6, pp. 54-72.

18. Sandhu, P.S. and Juneja, M. (2015) 'An improved LSB based image steganography technique for RGB images' in International Journal of Computer and Communication Engineering, Vol. 2, No. 4, pp. 513-517.

19. Schmidhuber, J. (2014) 'Deep learning in neural networks: An overview', Vol. 61, No. 1, pp. 85-117.

20. Sheng-hua, Z., Songtao, W. and Yan, L. (2017) 'A Novel Convolutional Neural Network for Image Steganalysis with Shared Normalization', IEEE Transactions on Multimedia, arXiv:1711.07306.