VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI - 590018

A Technical Seminar Report on

HIGH-CAPACITY IMAGE STEGANOGRAPHY BASED ON IMPROVED FC-DENSENET

Submitted in partial fulfillment of the requirements as per VTU curriculum of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE & ENGINEERING

By

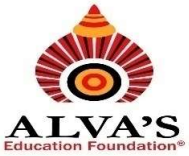
JAYALAKSHMI M

4AL17CS035

Under the Guidance of

HEMANTH KUMAR N P

SENIOR ASSISTANT PROFESSOR



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

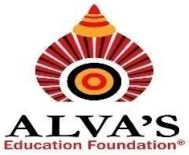
MOODBIDRI-574225, KARNATAKA

2020– 2021

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that **JAYALAKSHMI M** (**4AL17CS035**) has submitted Technical Seminar Report on "**HIGH-CAPACITY IMAGE STEGANOGRAPHY BASED ON IMPROVED FC-DENSENET**" for the VIII semester B.E. in Computer Science & Engineering during the year 2020-21

Mr. Hemanth Kumar N P	**Mr. Harish Kunder**	**Dr. Manjunath Kotari**
Seminar Guide	**Seminar Coordinator**	**Professor and Head**

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany a successful completion of any task would be incomplete without the mention of people who made it possible, success is the epitome of hard work and perseverance, but steadfast of all is encouraging guidance.

So, with gratitude I acknowledge all those whose guidance and encouragement served as beacon of light and crowned the effort with success.

I thank my project guide **Mr. Hemanth Kumar N P, Senior Assistant Professor** in Department of Computer Science & Engineering, who has been my source of inspiration. He has been especially enthusiastic in giving his valuable guidance and critical reviews.

The selection of Technical Seminar Topic as well as the timely completion is mainly due to the interest and persuasion of my seminar coordinator **Mr**. **Harish Kunder,** Associate Professor, Department of Computer Science & Engineering. I will remember his contribution for ever.

I sincerely thank, **Dr. Manjunath Kotari**, Professor and Head, Department of Computer Science & Engineering who has been the constant driving force behind the completion of the seminar.

I thank Principal **Dr. Peter Fernandes,** for his constant help and support throughout.

I am also indebted to **Management of Alva's Institute of Engineering and Technology, Mijar, Moodbidri** for providing an environment which helped me in completing the seminar.

Also, I thank all the teaching and non-teaching staff of Department of Computer Science & Engineering for the help rendered.

Finally, I would like to thank my parents and friends whose encouragement and support was invaluable.

JAYALAKSHMI M 4AL17CS035

ABSTRACT

The Fully Convolutional Dense Connection Network (FC-DenseNet) is proposed to target the problem of low steganographic capacity on using traditional steganography based on carrier modification. Since FC-DenseNet can effectively overcome the problems of gradient dissipation and gradient explosion, and a large number of features are multiplexed, the cascaded secret image and carrier image can reconstruct good image quality after entering the network. Effectively improve steganographic capacity. First, we reset the number of input channels of the first convolution block of FC- DenseNet and the number of output channels of the last convolution block and deleted the LogSoftmax() function. On the sender side, after the concatenated secret image and carrier image pass through the hidden network FC-DenseNet, the secret image is embedded in the carrier image to obtain a stego-image. At the receiving side, the extraction network reconstructs the secret image from the stego-image. Experimental results show that our proposed steganography scheme not only has a high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM) but also can realize large-capacity image steganography, with an average image payload capacity of 23.96 bit per pixel.

TABLE OF CONTENTS

CHAPTER NO.	DESCRIPTION	PAGE NO.
	DECLARATION	i
	ACKNOWLEDGEMENT	ii
	ABSTRACT	iii
	TABLE OF CONTENT	iv
	LIST OF FIGURES	v
1.	**INTRODUCTION**	
1.1	PROBLEM STATEMENT	4
1.2	OBJECTIVE	5
1.3	BACKGROUND AND SCOPE	5
1.4	TRADITIONAL IMAGE STEGONOGRAPHY	7
2.	**METHODOLOGY**	
2.1	NETWORK ARCHITECTURE	10
2.2	HIDE ENCODER OF THE SECRET IMAGE	11
2.3	REVEAL DECODER OF THE STEGO-IMAGE	12
2.4	LOSS FUNCTION	12
2.5	EXPERMIENTS	13

3. ADVANTAGES AND DISADVANTAGES

3.1 ADVANTAGES 20

3.2 DISADVANTAGES 20

3.3 APPLICATIONS 21

4. CONCLUSION AND FUTURE ENHANCEMENT

4.1 CONCLUSION 22

4.2 FUTURE ENHANCEMENT 22

REFERENCES 23

BASE PAPER 26

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
1.1	Random samples from the Encoder-Decoder	4
1.2	A 4-layer dense block with hyperparameter k 4	6
1.3	Flow chart to hidden information into cover image	8
1.4	Data of changed bit after encoding	8
1.5	Flow chart to stego-image into hidden information	9
2.1	Framework for steganography model diagram	10
2.2	A Dense connection Block has four layers	12
2.3	Carrier image, Secret image, the stego-image	14
2.4	Starting stego-image	15
2.5	Experimental images of CT images, remote sensing images, and images captured by aerial cameras	17
2.6	The first line is the carrier image, the second line is the secret image, the third line is stego-image, and the fourth line is the secret image extracted. The carrier image and the secret image in the first column are the original images. The carrier image and the secret image in the second, third, fourth, and fifth columns are the images processed by the JPEG high-quality compression factor.	18
2.7	Get ROC curve with StegExpose analysis tool.	19

CHAPTER 1

INTRODUCTION

Cyberspace security has always attracted people's attention. While the number of global netizens continues to grow, net- work security is in a cycle of decreasing and increasing. How to effectively ensure that information is not intercepted by attackers in the process of Internet communication is crucial. In addition, personal privacy leakage is also an important issue today. For example, the photographed electronic ID cards and bank cards were stolen by criminals and used for illegal purposes. It not only endangers people's property safety, but also violates personal privacy.

The most common steganography is to embed secret information into the Least Significant Bits(LSB) of natural images, LSB digit of the pixel is easily replaced by secret information, which is easy to produce visual artifacts. In the case of known carrier images and stego-image, it is very easy for an attacker to find secret information in stego-image. Cheonshik Kim et al. proposed a lossless data hiding method for Absolute Moment Block Truncation (AMBTC) images. In order to increase the steganographic capacity, the coefficients of the bit planes in each 4 4 block are calculated, and then the histogram modification is effectively expanded, which improves the steganography effect to a certain extent. In order to further optimize the results of Dongkyoo Shin et al. in added Hamming codes and lookup tables to optimize codewords, which are mainly used to reduce the distortion of image pixels and improve image quality. Vinodhini RE et al. used DNA algorithms to insert secret information into DNA sequences to complete image steganography. Lin Weixiong et al. proposed a blind watermarking algorithm based on the significant differ- ence between wavelet coefficient quantization and copyright protection. Each of the seven non-overlapping wavelet syner- gies of the carrier image is grouped into a block, which mainly quantizes the local maximum coefficient to determine the position of the watermark insertion. Tomáš et al. pro- posed an adaptive steganographic lattice code quantization method that minimizes the embedding impact. STC is usually used in combination with the cost. STC coding and cost calculation are divided into two processes. The cost is calcu- lated first (Assuming the effect of distortion after embedding information), STC coding is performed. Currently, based on the method of modifying the carrier image, it mainly includes modifying the spatial domain of the image and

modifying the frequency domain of the image. The change of the image spatial domain is to directly modify the pixel value of a certain area or a certain area to achieve expected goals, and the image frequency domain changes by modifying the transform domain coefficients to achieve information embed- ding. We are different from traditional image steganography. Traditional image steganography is a cost function designed by hand and embedded with STC class. The cost function is designed by ourselves based on our own experience. This is a difficulty in STC coding. Due to the great potential of deep learning, it has achieved great success in pattern recognition, natural language processing, data mining, etc., and it has also penetrated and developed in the field of information security and forensics. Therefore, introducing deep learning into the field of steganography and using artificial intelligence to design the cost function is a novel solution to the difficulty of manually designing the cost function.

Text information is hidden into the image. In the generative adversarial network of the stego-image, image generated by the generator makes the discriminator unable to distinguish between the carrier image and the stego-image. At the same time, it is impossible to accurately distinguish whether the image is a carrier image or a stego-image in our human vision, so it is difficult for us to find that the image contains secret information. The secret information is segmented and converted into random noise. The noise enters the generator and the output result is a secret image, and the secret image is extracted by the extractor and the output result is a noise vector. Finally, according to the mapping of secret information and noise vector relation- ship, reconstruct the secret information. To increase security, the attention model and the generative adversarial net-work are combined to realize the embedding and extraction of secret images. Nowadays, there are relatively few attempts to hide images using the deep neural network itself. The convolutional network has an encoder and a decoder. The encoder is mainly used to hide the color secret image, and the decoder is mainly used to extract the secret image. The convolutional network implements the hiding and extraction of secret images, but after hiding the stego-image, we can easily see the distortion of setgo-image. Most of them are steganographic text. The number of bits per pixel occupied by the text is relatively small in the image, so these methods have the advantages of steganalysis good resistance, but low payload capacity. A good information hiding challenge arises because the appearance and underlying statistical changes of the carrier image are easily caused by embedding the message. There are two main reasons for the change in the appearance of the carrier

image and the statistics of the basic data. First, the amount of information that will be hidden. The most common is to hide relatively few bits of text information hidden. Second, the extent of the visible change in the image of the carrier depends on the image of the carrier itself. Hiding secret information in the high-frequency region of the image is better than hiding the information in artificially detectable low-frequency regions. The capacity for estimating information hiding can be found.

In March 2020, China's Internet penetration rate was 64.5% and the number of Internet users was 904 million. The problem of personal privacy leakage continues to arise. For example, for some private photos stored by the user, the user can embed the private photos into a natural picture through the scheme we designed. The text is converted to binary data, and then the position of the LSB is automatically selected by the neural network for embedding. In contrast, in our work, the difference between us and is that the preparation network is removed, and the hidden network uses Full Convolution Dense Connection Network (FC-DenseNet). In our work, first, the secret image and the carrier image are encoded as a stego-image via a hidden network, and secondly, the stego-image is decoded into a secret image via a decoding network. Ultimately, our proposed solution not only improves steganographic capacity but also has a high Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM).

Perhaps the best neural network is used at the same time as the work presented here. In addition, in standard steganography studies, these methods encode small amounts of information but are visual of good quality. As a summary, our work consists of the following three parts:

The image is segmented by semantics, and the segmentation effect is very good. Unlike, we applied FC-DenseNet for information hiding for the first time. The number of input channels of the first convolution block of FC-DenseNet and the number of output channels of the last convolution block is reset. In addition, we did not use the object tag category and deleted LogSoftmax().

Hidden secret information does not need to be perfectly coded and can accept small errors. It can clearly balance the reconstruction quality of the carrier image and the secret image, as shown in Figure 1.1.

Unlike an encrypted noise image or an image that is obviously visually impacted after adding secret information. Instead of the images we transmit are meaningful images,

and large orders of secret information are hidden, the ratio of the magnitude of the secret image to be hidden to the image of the carrier is 1:1, payload capacity reaches 23.96bpp.

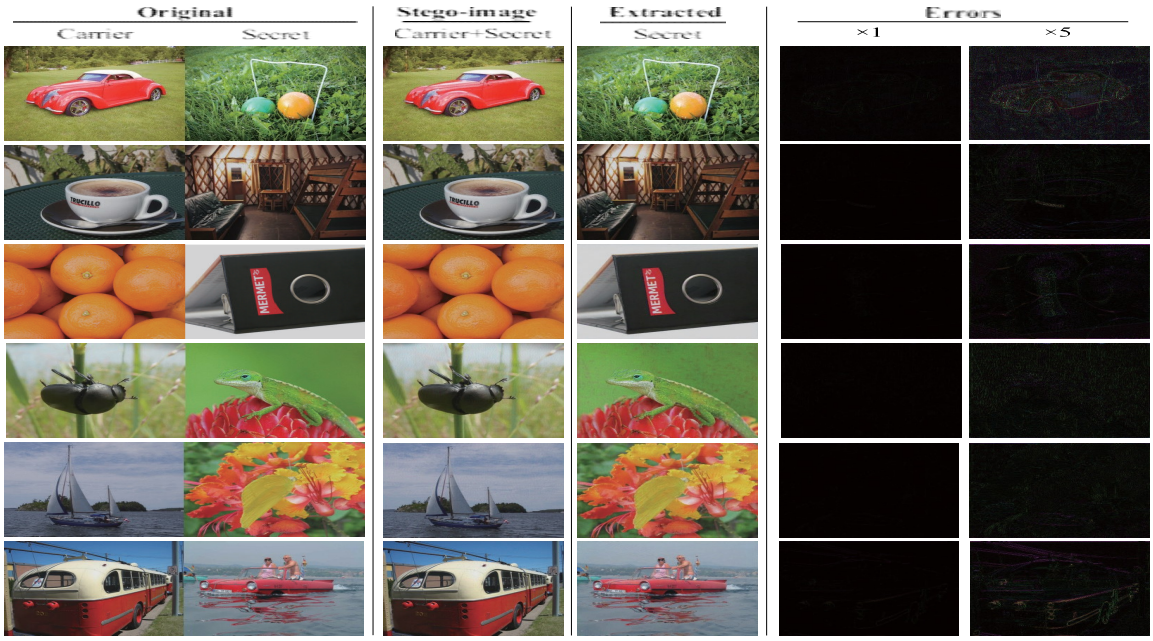


FIGURE 1.1: Random samples from the Encoder-Decoder (hidden and extracted) system. Starting from the left: carrier image, secret image, the stego-image (It not only looks like a carrier image, but also hides the secret image in it), and the recovered secret image—this is extracted from only the stego-image. Columns 5 and 6 are the errors for the stego-image vs. carrier (enhanced ×1, ×5).

1.1 Problem Statement

How can we send message/image secretly to the destination?

Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmission. In this study, I proposed a new framework of an image steganography system to hide a digital text of a secret message. An issue of gradient dissipation and gradient explosion, and a large number of features are multiplying when carrier modification-based steganography method is used. This paper proposes fully convolutional Dense Connection Network (FC-DenseNet) in order to improve reconstruction of good quality image after entering network.

1.2 Objective

In the project, its primarily concentrated on the data security issues when sending the data over the network using steganographic techniques. Requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings. The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. The FC-DenseNet method is about image classification and sending the convoluted stego-image over the network by upsampling and down sampling to realize large-capacity image steganography. The improved Network parameter is more specific and improves the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM).

1.3 Background and scope

Deep networks have achieved unprecedented success in many image segmentations tasks. In this article, we mainly apply FC-DefnsNet to our hidden network to hide information. FC-DenseNet is extended from Densely Connected Convolutional Networks (DenseNet). To utilize deep networks in image steganography, we will briefly introduce the application of DenseNet and FC-DenseNet to lay the foundation for the next section.

1.3.1 DENCE CONVOLUTION NETWORK (DenseNet)

DenseNet is not only used for the classification of data but also for the super-resolution of images and image segmentation. Tong Tong al. proposed a method to apply DenseNet to image super-resolution. After the image passes DenseNet, it is followed by deconvolution and reconstruction, which have achieved good results. In view of the fact that the traditional convolutional network has an L layer, there is an L number of connections. However, there is a connection between each layer of the DenseNet network and each subsequent layer, and the total number of connections is L(L 1)/2. The advantage of DenseNet is to eliminate the vanishing- gradient problem, enhance feature propagation, a large number of features are multiplexed, and can effectively reduce the parameters of the model. The structure of DenseNet is shown in Figure 1.2. Figure 1.2 briefly depicts the layout of DenseNet. Consequently, the l^{th} layers accept all

layers in front of feature maps, $X_0, X_1, \ldots, X_{l-1}$ as input:

$$X_l = Y_l([X_0, X_l, \ldots, X_{l-1}]) \quad (1)$$

where $[X_0, X_1, \ldots, X_{l-1}]$ represents the concatenation of the feature maps generated in the 0 to l 1 layers. Com- bine multiple tensors into one tensor for better applica- tion. is a composite function with three operations: namely Batch Normalization (BN) and Rectified Liner Unit (ReLU), Convolution (Conv).

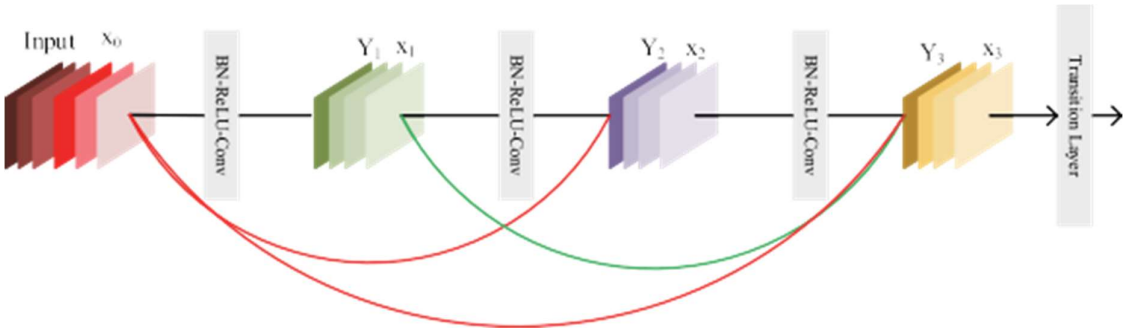


FIGURE 1.2: A 4-layer dense block with hyperparameter k 4. The hyperparameter determines how much information each layer contributes globally.

1.3.2 APPLICATION AND DEVELOPMENT OF FC-DenseNet

FC-DenseNet is a dense convolutional neural network. It is derived from DenseNet, FC-DenseNet is mainly used for semantic segmentation, according to the label, it can segment the sky, tree, vehicle, pedestrian, road, etc. in the picture, and also applies to the segmentation in the video. The main process is to add a downsampling and upsampling function behind the Dense Block. The down- sampling is a 2x2 convolution block used to extract the maximum value of the feature map to reduce the image and simplify the calculation. The upsampling is composed of a 3x3 transposed convolution, and the convolution kernel has a step size of 2 to compensate for the pooling operation. Finally, the classification is done by 1x1 convolution and the number of categories. More straightforward, the number of output feature-maps is the number of different categories, and the effect of the segmentation is attractive.

Based on FC-DenseNet, it is not necessary to split different objects in the image but to hide information in our work. We did not mark the different objects in the image, deleted the label category and the 1- 1 convolution to achieve perfect hiding of the information.

1.4 Traditional Method of Image Steganography

In a gray scale image, each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone has considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bit of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types.

1.4.1 LSB ALGORITHM

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8-bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24-bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless.

LSB ENCODING: LSB encoding algorithm consist of counter to check whether all the message text is inputted. It gets LSB of red band-image and one bit of the message and performs XOR operation on it, depending on the result it replaces left most 1-bit hidden information from either Green or Blue until the complete message is covered shown in

Fighure 1.3 and 1.4. Finally, it converts the formed matrix into a stego-image.

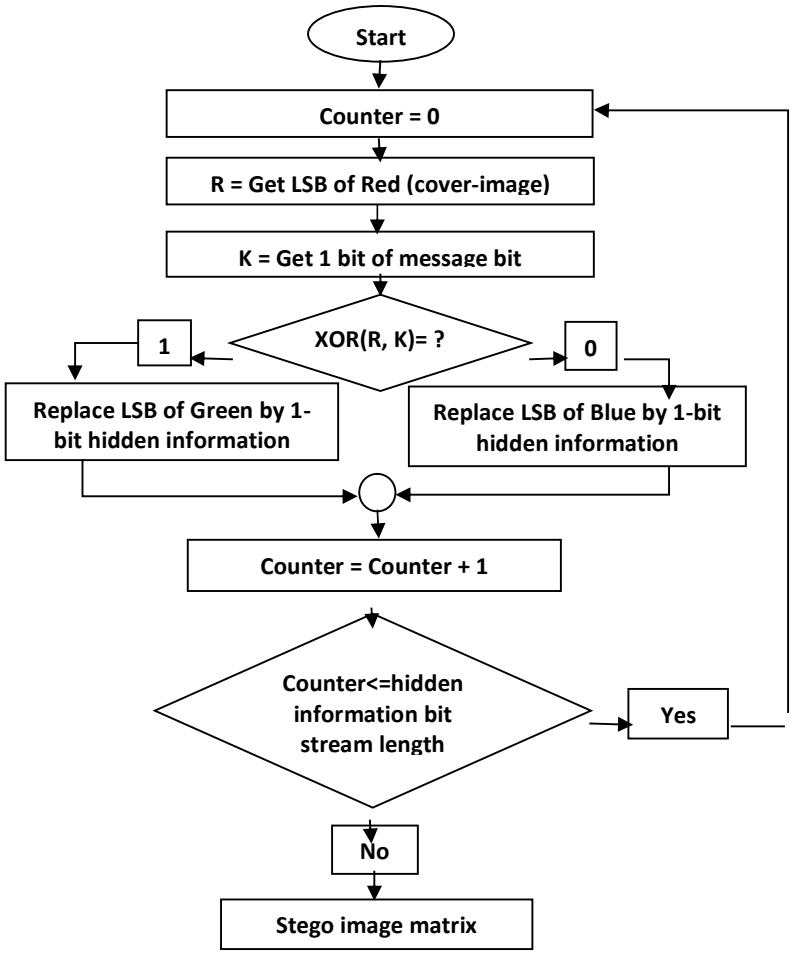


FIGURE 1.3: Flow Chart to hidden information into cover image

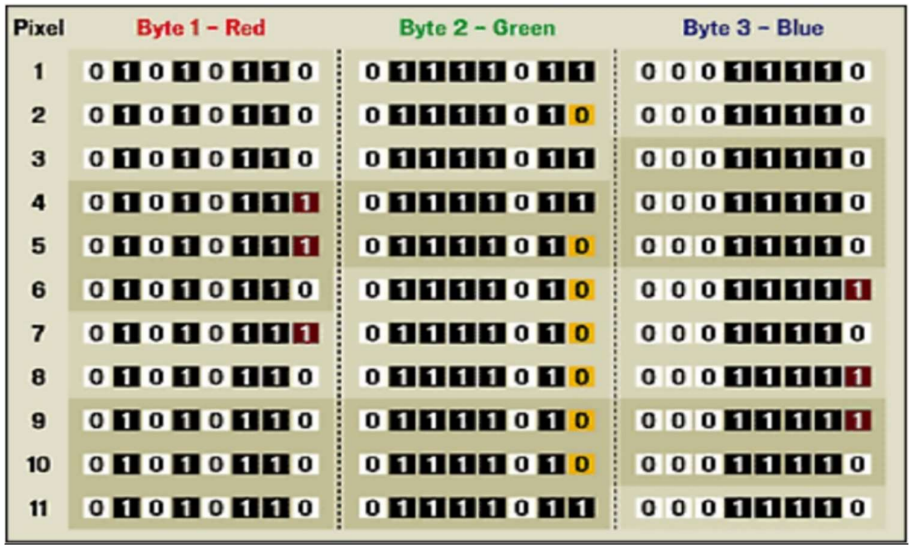


FIGURE 1.4: Data of changed bit after encoding

LSB DECODING: LSB decoding algorithm consist of counter to check whether all the message text is read. It gets LSB of red band-image and one bit of the message and performs XOR operation on it, depending on the result it picks LSB hidden information from either Green or Blue and stores that bit into 1D array until the complete message is read. Finally, it we get a 1D array of hidden message shown in Figure 1.5.

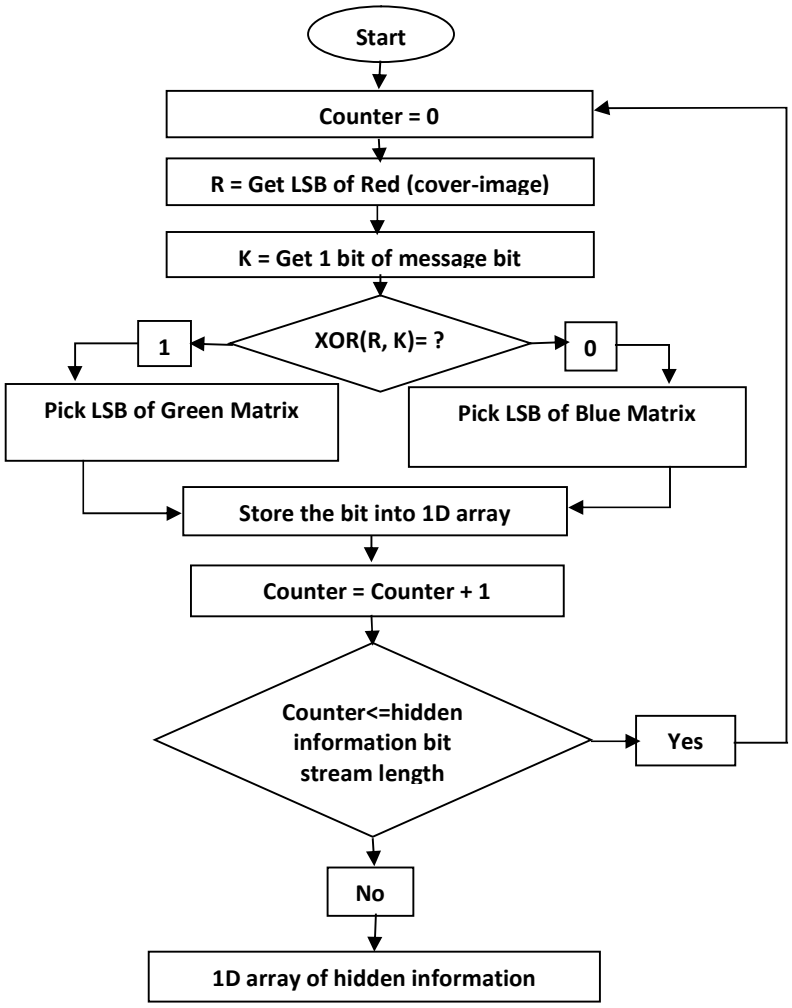


FIGURE 1.5: Flow Chart to stego-image into hidden information

CHAPTER 2

METHODOLOGY

This part mainly describes the detailed structure of hidden network and extraction network, and how to hide secret information and reconstruct secret information. In addition, the loss function we designed is introduced in detail.

2.1 NETWORK ARCHITECTURE

As depicting Figure 2.1, our proposed architecture mainly contains concatenation and an encoder (Hiding Network) and a decoder (Reveal Network). Concatenation can be described be two tensors of the same width and height and depth, D and D^{r}, where c and s are the carrier image and the secret image, respectively.

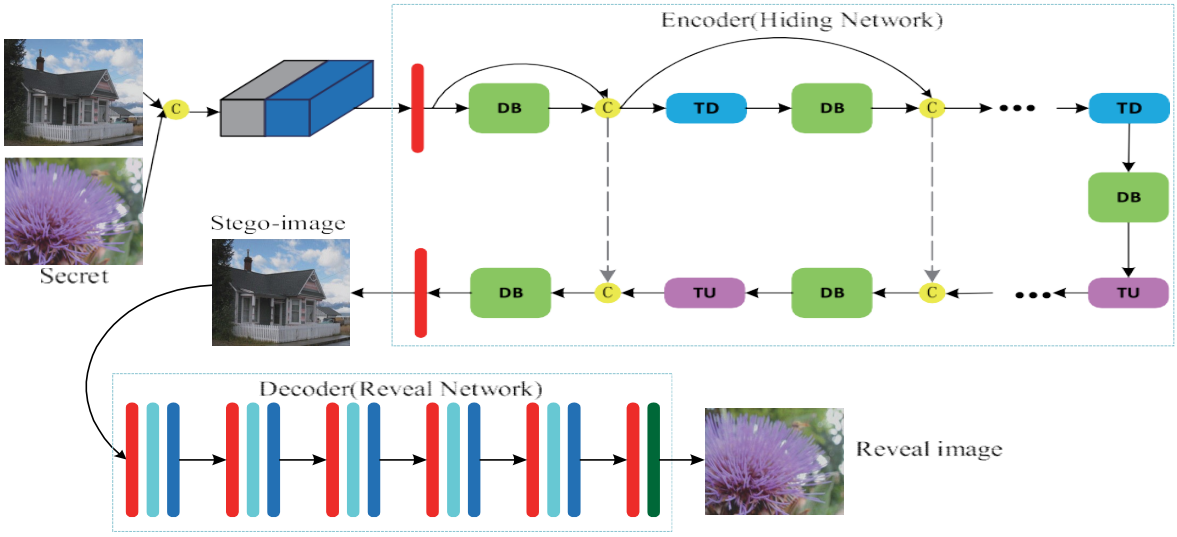


FIGURE 2.1: Framework for steganography model diagram.

then, let concatenation: $(c, s) \rightarrow \phi \in R^{W \times H \times (D+D^{r})}$ be the concatenation of the two tensors along the depth axis. The image size requirements input into the framework: W >= 256, H>=256, D>=256, uniformly adjusted to 256 x 256 through the image size function in python. The encoder is mainly used to hide secret information and the decoder

is mainly used to extract secret information. Our goal is to train encoders and decoders at the same time to achieve perfect information hiding and extraction

2.2 HIDE ENCODER OF THE SECRET IMAGE

The encoder was previously a concatenation operation. This function spliced the carrier image and the secret image and output a 6-channel tensor to prepare for the next full-size image hiding. The structure of the encoder is given. The first column indicates the architecture of the hidden network, the second column indicates the size of the output feature map, D is the number of channels. The input to the encoder is a 6-channel tensor and the output is a 3- channel tensor.

The foremost goal of the encoder is to encode a tensor with a channel number of 6 and the output stego- image should be as close as possible to the carrier image. Encoder components include two 3 x 3 convolution, 11 Dense Block (DB), 10 Concatenation, 5 Transition Down (TD) and 5 Transition Up (TU). The input of the first convolution block is a 6-channel tensor and the output is a 48-channel tensor. The input of the last convolution block is a 192 channels tensor, and its output is a 3-channel tensor. TD is composed of BN, ReLU, 1 1Conv, 2 x 2 maximum pooling. TU is a 3 x 3 Trans- posed Convolution strides 2, padding 1. TD is mainly used to extract and integrate the features of secret image and carrier images. The role of TU is to gradually restore the characteristics of the input. The combination of error τ and TU can restore the carrier image with high accuracy. In Figure 2.2, each DB consists of 4 layers, each layer including batch normalization, activation, 3 x 3 Conv, Droupt 0. Our goal is to minimize the loss between stego-image and carrier image:

$$\tau = \|c - c^r\|.$$

where c and c^r represent the carrier image and stego-image.

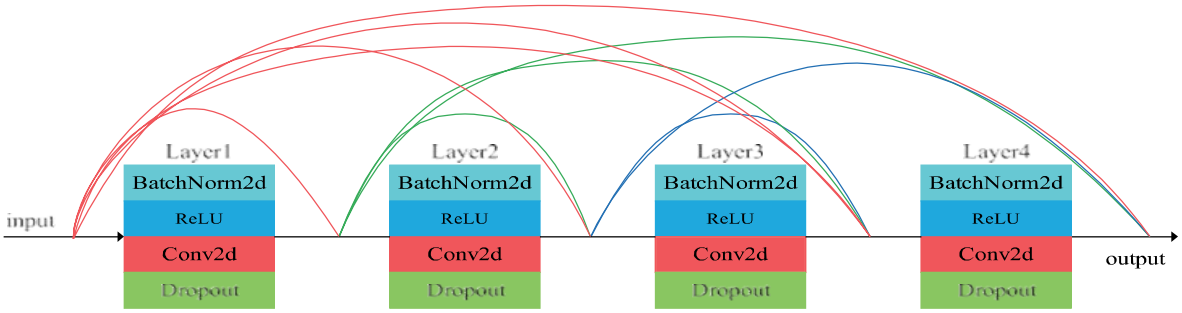


FIGURE 2.2: A Dense connection Block has four layers. Layers and layers are connected to each other.

2.3 REVEAL DECODER OF THE STEGO-IMAGE

The input to the decoder is a 3-channel tensor and the output is also a 3-channel tensor. The Decoder components include 6 Conv with a convolution core of 3 3, 5 BN, 5 ReLU, and 1 Sigmoid. The main goal of the Decoder is to decode the secret image s from the stego-image and the decoded s^r should be as similar to the original secret image as possible. Our goal of the decoder is to minimize the loss of the decoded secret image and the original secret image:

$$\gamma = s - s^r$$

where s and s^r represent the original secret image and the reveal secret image, respectively.

2.4 LOSS FUNCTION

In our work, the target of the encoder is to hide the secret image into the carrier image to get the stego-image, the decoder extracts secret images from stego-image. The training of the entire network is done by reducing the follow- ing errors: (β is their weight):

$$\zeta = \tau + \beta\gamma$$

Note that as the error τ changes, it has no impact on the weight of the decoder, only the weight of the encoder. Because the decoder does not need to reconstruct the cover

image; it only needs to recover secret information from stego-image. Both the encoder and the decoder are trained from the error signal $\beta\gamma$ since the hidden network and the extracted network are responsible for saving and forwarding information about secret images. Better hiding and extracting information by propagating error signals.

2.5 EXPERIMENTS

In this article, the dataset is taken from the public ImageNet image database, and we randomly selected 23,500 images, of which 20,000 were used only for training, and 3,500 were used for testing. The hyperparameter β 0.75 of the model, the number of input channels of the first convolution block of the hidden network is 6, and the number of output channels of the last convolution block is 3. The initial learning rate of the network is 0.001. The batch into which the image enters the model is set to 16, and the number of iterations of the training is set to 200. Experimental hardware configuration: 2 GPUs, GPU model is GeForce GTX1080, 1 GPU memory is 8G. Software environment required for the experiment: deep learning framework Pytorch1.1.0, programming experiment with python3.6. For performance evaluation, we used two assessment methods: visual evaluation and quantitative evaluation. In addition, steganalysis tools are introduced to detect the anti-steganography security of our proposed scheme. Image distortion is evaluated by the SSIM and the PSNR. In addition, the space occupied by our model parameters is 8.24M.

2.5.1 VISUAL EVALUATION

In check to see the performance of the model, we performed a human visual assessment of the carrier image, the secret image, and the stego-image. In Figure 2.3, after comparison, our eyes do not see the difference between the carrier image and the stego-image. The stego-image image is subtracted from the carrier image to obtain an error image. In the 1, 2, 3, 5, and 7 lines of Figure 2.3, after the error image is magnified 10 times and 20 times, we can only see artifacts of the carrier image without seeing the secret image artifacts.

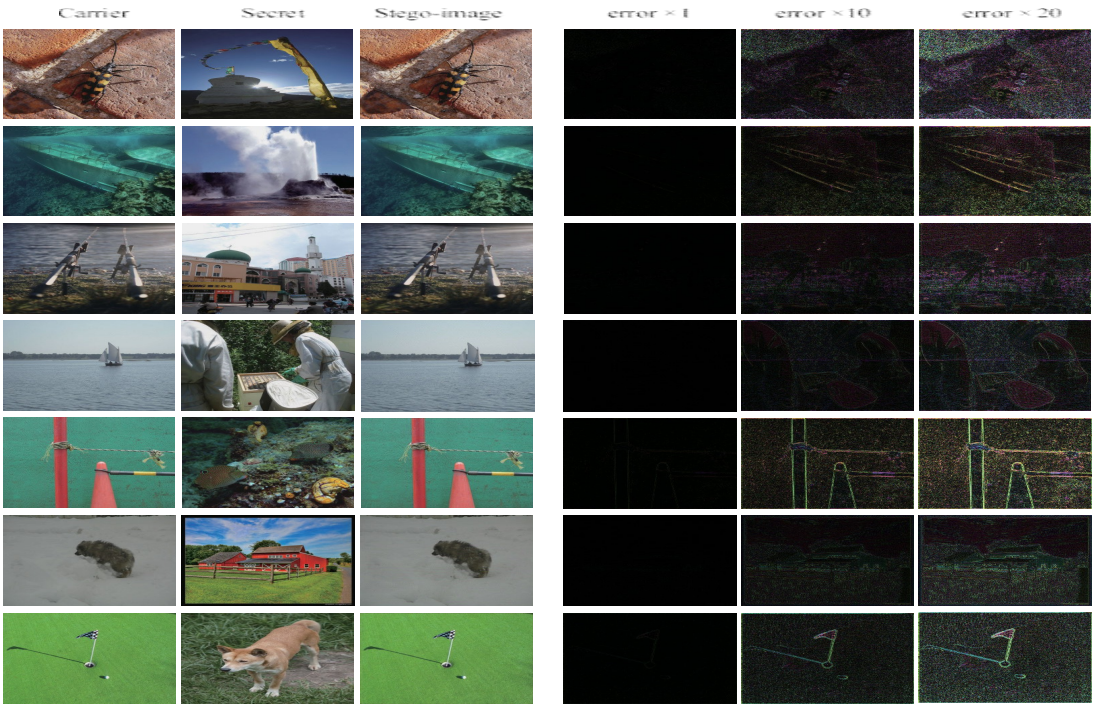


FIGURE 2.3: Starting from the left: carrier image, secret image, the stego-image. The last three columns are the errors for the setgo-image vs. carrier (enhanced ×1, ×10, ×20).

To further verify the generalization ability of the model, we selected several images from the Celeb. A dataset and the COCO dataset for testing. The results of the test are shown in Figure 6. The high-frequency region of the carrier image has a strong anti-interference ability, so the artifact of the carrier image appears in the error image. In the 4th line and the 6th line of Figure 2.3, in the 7th line of Figure 2.4, after the error image is magnified 10 times and 20 times, we only see the artifacts of the secret image blurred because the area of the carrier image is relatively flat.

FIGURE 2.4: Starting stego-image (stego-image not only contains secret images, but also looks like a carrier image), and the recovered secret image this is to say extracted from only the stego-image. 1 row and 2 rows, 3 rows and 3rows, 5 rows and 6 rows respectively of ImageNet dataset, CelebA dataset, COCO dataset.

2.5.2 QUANTITATIVE EVALUATION

In addition to visual assessment, we also measure the statis- tical mathematical distribution quality of stego-image. One widely-used metric for measuring image quality is

the PSNR. PSNR is mainly used to measure the distortion rate of an image and display it as a score. Given two images X and Y of size (W, H), the PSNR is defined as a function of the Mean Squared Error (MSE):

$$MSE = \frac{1}{WH} \sum_{i=0}^{W} \sum_{j=0}^{H} (X_{ji} - Y_{ji})^2$$

$$PSNR = 10 \log_{10} \frac{(2^n - 1)^2}{MSE}$$

where 2^{n-1} is the maximum value of the image point color and n is the number of bits of the sample point.

For a more complete evaluation of stego imGE , we declare the SSIM between the carrier image and the stegi-image.

$$SSIM = \frac{(2\mu_X\mu_Y + k_1R)(2\sigma_{XY} + k_2R)}{(\mu^2 + \mu^2 + k_1R)(\sigma^2 + \sigma^2 + k_2R)}$$

hereby default $k_1 = 0.01$, $k_2 = 0.03$, and the return value is between [-1, 1], where 1.0 means the two images are identical. To further illustrate the effectiveness of steganography, we introduce the carrier image and the stego- image, the extracted secret image, and the PSNR and SSIM of the original secret image. We can see that the average of PSNR and SSIM for the carrier image and the stego-images reached (39.556, 0.985), and the average of PSNR and SSIM of the reconstructed secret image and the original secret image reached (37.092, 0.975). A comparison of our approach to other solutions, and our PSNR and SSIM are the highest. Besides, in Figure 2.4, we plot the carrier image, stego-image, secret image, and the histogram of the reconstructed secret image, we can observe the carrier image and the stego-image, the secret original image and the reconstructed secret image, and the histogram difference between them is

not very large. It is worth noting that because these evaluation indicators are relatively good, the solution we designed will not destroy the visual integrity.

2.5.3 STEGANOGRAPHY CAPACITY ANALYSIS

The traditional LSB steganography has a relatively small steganographic capacity. Since our steganography scheme is relatively new, it is more intuitive to compare with other schemes, there is a hiding scheme including the steganography based on carrier selection and the steganography based on carrier synthesis. We can clearly see that the payload capacity of our proposed scheme is better than other schemes. Here, column 1, column 2, column 3, column 4 are steganography, steganography capacity per image, stego-image size, relative steganography capacity (steganography capacity per pixel):

Relative Capacity = Absolute Capacity/Image size

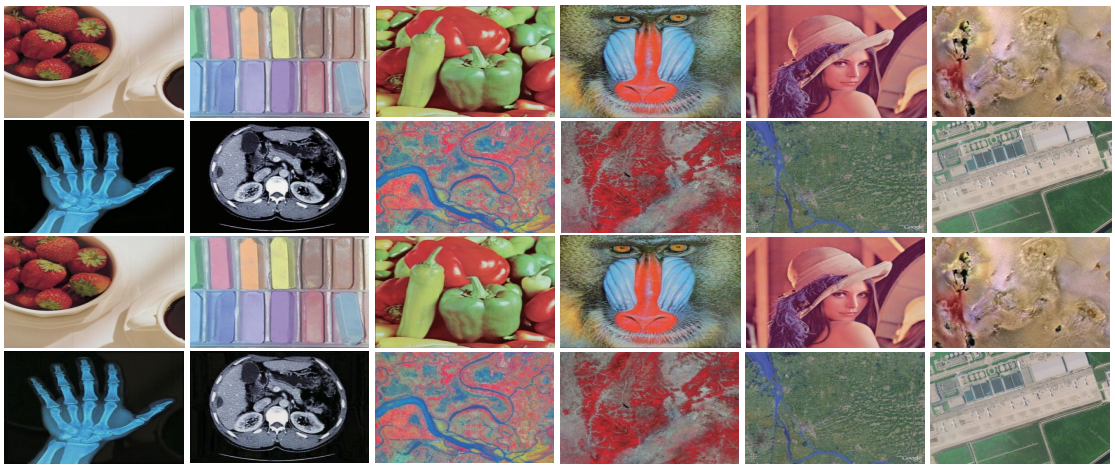


FIGURE 2.5 Experimental images of CT images, remote sensing images, and images captured by aerial cameras. Lines 1, 2, 3 and 4 are carrier image, secret image, stego-image, and extracted secret image respectively.

In addition, our proposed model is suitable for most images. As shown in Figure 2.5, we introduce CT images, remote sensing images, and images captured by aerial vehicles. The load capacity and the change rate of the carrier image in Figure 2.5.

The calculation method of payload capacity is:

$$payload\_capacity = r \times 8 \times 3$$

where 8 indicates that the space occupied by a single pixel is 8, and indicates that each image has 3 channels. We randomly selected 500 pairs of images as the test set, and the calculated average load rate was 23.96bpp.

FIGURE 2.6 The first line is the carrier image, the second line is the secret image, the third line is stego-image, and the fourth line is the secret image extracted. The carrier image and the secret image in the first column is the original images. The carrier image and the secret image in the second, third, fourth, and fifth columns are the images processed by the JPEG high-quality compression factor, and the quality factors are 70, 75, 80, and 85 respectively.

To verify the influence of image compression on our model, before the image enters our model, the carrier image and the secret image are compressed separately with JPEG high-quality factors. The final experimental results are shown in Figure 2.6. We can hardly see the difference between them. When the quality factor is 70, we cannot see the difference between them and the original image experimental results.

Finally, we use the steganalysis tool StegExpose to analyze our data, using a standard threshold of 0.2, and the analysis results are shown in Figure 2.6. The horizontal

axis indicates that a file that is not organized is judged as a steganographic file, and the vertical axis indicates that an organized file is judged as a steganographic file. The red dashed line represents random guessing, and the green solid line represents the ROC drawn. It can be seen that the performance of the steganalysis tool is only slightly better than random guessing.

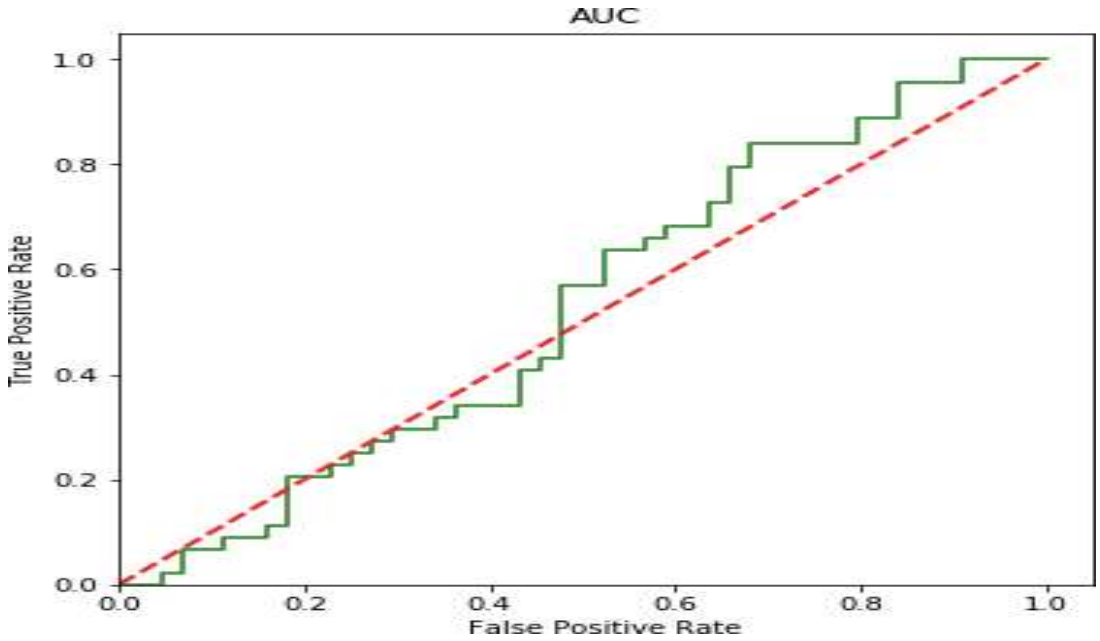


FIGURE 2.7: Get ROC curve with StegExpose analysis tool

CHAPTER 3

ADVANTAGES AND DISADVANTAGES

3.1 ADVANTAGES

- The advantage of DenseNet is to eliminate the vanishing-gradient problem, enhance feature.
- The advantages of steganography over cryptography alone are that message doesn't attract attention to themselves.
- In electronic communication may include steganographic coding inside the transparent layer, such as document file, image file, wave file.
- Hard to detect. Original image is very similar to altered image. Embedded data resembles Gaussian noise.
- It can be done faster with large amount of software.
- Provides better security for sharing data in LAN, MAN and WAN.
- Plainly visible encrypted messages – no matter how unbreakable – will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.
- Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

3.2 DISADVANTAGES

- The confidentiality of information is maintained by the algorithms, and if the algorithms are known then this technique is of no use.
- Password leakage may occur and it leads to the unauthorized access of data.
- If this technique is gone in the wrong hands like hackers can be very dangerous for all.
- Message is hard to recover if image is subject to attack such as translation and rotation.

- Image is distorted, message easily lost if picture subject to compression such as JPEG.
- Huge number of data, huge file size, so someone can suspect about it.
- During sending and receiving information can be spoofed.

3.3 APPLICATIONS

- Secure Private Files and Documents.
- Hide Passwords and Encryption keys.
- Transport Highly private Documents between International Government.
- Transmit message/data without revealing the existence of available message.

CHAPTER 4

CONCLUSION AND FUTURE ENHANCEMENT

This article is different from the traditional STC coding steganography scheme. The data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination.

4.1 Conclusion

Many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it use lessor obtain information un-intended to him. So, use of artificial intelligence to design the cost function instead of the cost function manually designed by STC coding. Through the end-to-end training model, the full-size image is hidden and the image distortion is small. This method has advanced visual effects and high steganography capacity, and the model has strong generalization ability, which can achieve steganography and extraction of different data sets. In the next step of this article, we will.

4.2 Future Enhancement

- To improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg, .tif etc., in the future.
- The compress of secret image and prepare to try to hide two secret images in the encoder, at the same time, the decoder extracts two secret images from stego-image. Further realize fast transfer and high-capacity steganography.

REFERENCES

[1] "Steganography Project", Jitu Choudhary, Research Scholar at National Institute of Technology Sikkim, https://www2.slideshare.net/jsdcuraj/project-ppt-21359799

[2] FC-DenseNet — One Hundred Layers Tiramisu, Fully Convolutional DenseNet (Semantic Segmentation), Sik-Ho Tsang, https://towardsdatascience.com/review-fc-densenet-one-hundred-layer-tiramisu-semantic-segmentation-22ee3be434d5

[3] A. Kokaj, ''Cyber war and terrorism in Kosovo'', *Academic J. Bus., Admin., Law Social Sci.*, vol. 5, no. 1, pp. 124–128, Mar. 2019.

[4] C. Kim, D. Shin, L. Leng, and C.-N. Yang, ''Lossless data hiding for absolute moment block truncation coding using histogram modification,''
J. Real-Time Image Process., vol. 14, no. 1, pp. 101–114, Jan. 2018.

[5] C. Kim, D.-K. Shin, C.-N. Yang, and L. Leng, ''Hybrid data hiding based on AMBTC using enhanced Hamming code,'' *Appl. Sci.*, vol. 10, no. 15, p. 5336, Aug. 2020.

[6] R. Vinodhini and P. Malathi, ''DNA based image steganography,'' in *Com- putational Vision and Bio Inspired Computing*, vol. 28. Cham, Switzerland: Springer, 2018, pp. 819–829.

[7] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, ''An effi- cient watermarking method based on significant difference of wavelet coef- ficient quantization,'' *IEEE Trans. Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008.

[8] T. Filler, J. Judas, and J. Fridrich, ''Minimizing embedding impact in steganography using trellis-coded quantization,'' *Proc. SPIE*, vol. 7541, Jan. 2010, Art. no. 754105.

[9] Y. LeCun, Y. Bengio, and G. Hinton, ''Deep learning,'' *Nature*, vol. 521, pp. 436–444, May 2015.

[10] J. Zhu, R. Kaplan, J. Johnson, and F. Li, ''HiDDeN: Hiding data with deep networks,'' in *Proc. Eur. Conf. Comput. Vis.*, Sep. 2018, pp. 682–697.

[11] K. Alex Zhang, A. Cuesta-Infante, L. Xu, and K. Veeramachaneni, ''SteganoGAN: High capacity image steganography with GANs,'' 2019, *arXiv:1901.03892*. [Online]. Available: http://arxiv.org/abs/1901.03892

[12] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, ''A novel image steganogra- phy method via deep convolutional generative adversarial networks,'' *IEEE Access*, vol. 6, pp. 38303–38314, 2018.

[13] C. Yu, ‘‘Attention based data hiding with generative adversarial networks,’’ in *Proc. AAAI Conf. Artif. Intell.*, vol. 34, no. 1, 2020, pp. 1120–1128.

[14] A. ur Rehman, R. Rahim, M. S. Nadeem, and S. ul Hussain, ‘‘End-to-end trained CNN encode-decoder networks for image steganography,’’ 2017, *arXiv:1711.07201*. [Online]. Available: http://arxiv.org/abs/1711.07201

[15] R. Zhang, S. Dong, and J. Liu, ‘‘Invisible steganography via generative adversarial networks,’’ *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8559–8575, Apr. 2019.

[16] F. Chen, Q. Xing, and F. Liu, ‘‘Technology of hiding and protecting the secret image based on two-channel deep hiding network,’’ *IEEE Access*, vol. 8, pp. 21966–21979, 2020.

[17] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, ‘‘Digital image steganography: Survey and analysis of current methods,’’ *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[18] F. Yaghmaee and M. Jamzad, ‘‘Estimating watermarking capacity in gray scale images based on image complexity,’’ *EURASIP J. Adv. Signal Pro- cess.*, vol. 2010, no. 1, Dec. 2010, Art. no. 851920.

[19] V. Kavitha and K. S. Easwarakumar, ‘‘Neural based steganography,’’ in *Proc. Pacific Rim Int. Conf. Artif. Intell.*, vol. 3157, 2004, pp. 429–435.

[20] Y. Sun, H. Zhang, T. Zhang, and R. Wang, ‘‘Deep neural networks for efficient steganographic payload location,’’ *J. Real-Time Image Process.*, vol. 16, no. 3, pp. 635–647, Jun. 2019.

[21] R. Khare, R. Mishra, and I. Arya, ‘‘Video steganography using LSB technique by neural network,’’ in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, Nov. 2014, pp. 898–902.

[22] S. Baluja, ‘‘Hiding images within images,’’ *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 42, no. 7, pp. 1685–1697, Jul. 2020.

[23] S. Jegou, M. Drozdzal, D. Vazquez, A. Romero, and Y. Bengio, ‘‘The one hundred layers tiramisu: Fully convolutional DenseNets for semantic seg- mentation,’’ in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 11–19.

[24] A. Hore and D. Ziou, ‘‘Image quality metrics: PSNR vs. SSIM,’’ in *Proc. Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 2366–2369.

[25] Y. Ye, J. Shan, L. Bruzzone, and L. Shen, ‘‘Robust registration of multi- modal remote sensing images based on structural similarity,’’ *IEEE Trans. Geosci. Remote Sens.*, vol. 55, no. 5, pp. 2941–2958, May 2017.

[26] W. Tang, S. Tan, B. Li, and J. Huang, ‘‘Automatic steganographic distortion learning using a generative adversarial network,’’ *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547–1551, Oct. 2017.

[27] J. Hayes and G. Danezis, ‘‘Generating steganographic images via adver- sarial training,’’ in *Proc. Neural Inf. Process. Syst.*, 2017, pp. 1951–1960.

[28] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, ‘‘SSGAN: Secure steganography based on generative adversarial networks,’’ in *Proc. Pacific Rim Conf. Multimedia.*, 2017, pp. 534–544.

[29] H. Zhao, J. Shi, X. Qi, X. Wang, and J. Jia, ‘‘Pyramid scene parsing network,’’ in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 2881–2890.

[30] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, ‘‘Densely connected convolutional networks,’’ in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 4700–4708.

[31] T. Tong, G. Li, X. Liu, and Q. Gao, ‘‘Image super-resolution using dense skip connections,’’ in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Oct. 2017, pp. 4799–4807.

[32] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, ‘‘Coverless image steganography without embedding,’’ in *Proc. Int. Conf. Cloud Comput.*, vol. 9483, 2015, pp. 123–132.

[33] Z. L. Zhou, Y. Cao, and X. M. Sun, ‘‘Coverless information hiding based on bag-of-words model of image,’’ *J. Appl. Sci.*, vol. 34, no. 5, pp. 527–536, 2016.

[34] K.-C. Wu and W. Chung-Ming, ‘‘Steganography using reversible texture synthesis,’’ *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 130–139, Jan. 2015.

[35] M.-m. Liu, M.-q. Zhang, J. Liu, Y.-n. Zhang, and Y. Ke, ‘‘Coverless information hiding based on generative adversarial networks,’’ 2017, *arXiv:1712.06951*. [Online]. Available: http://arxiv.org/abs/1712.06951

[36] J. Xu, X. Mao, X. Jin, A. Jaffer, S. Lu, L. Li, and M. Toyoura, ‘‘Hidden message in a deformation-based texture,’’ *Vis. Comput.*, vol. 31, no. 12, pp. 1653–1669, Dec. 2015.

[37] B. Boehm, ‘‘StegExpose—A tool for detecting LSB steganography,’’ 2014,

[38] *arXiv:1410.6656*. [Online]. Available: http://arxiv.org/abs/1410.6656