IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Video and Image Steganography

Samyuktha V[1], Shree Shradha S[2], Tejaswini P[3], Vaishnavi[4],Sowmya K S[5]

BE, Departmentof ECE, DBIT, Bangalore, India[1,2,3,4]

Associate Professor, ECE, DBIT, Bangalore, India[5]

Abstract: Steganography is a method which hides conceal data within an ordinary file to avoid detection. Steganography includes encryption and decryption process, where the secret image or data to be transmitted is hidden inside the cover file and encrypted output is called stego object. Steganography can be done using any digital format like image, video or audio etc. The aim of this paper is to improve the data hiding capacity through various methods. In this paper, first video is divided into frames where the color conversion takes place from RGB to YUV. Advanced Encryption Standard (AES) is used which chooses the pixel positions randomly for embedding process. Second we focus on Least Significant Bit (LSB) technique where the information is hidden in the Least Significant Bit of each pixel of the chosen video. Main advantage of LSB is that huge amount of data in any digital formats can be encoded and it can be retrieved back in a lossless way. Third, In order to improve the security of the hidden data, a linear block code principle is implemented; i.e. Hamming code is used to check for the errors. To detect the errors of the obtained AES encrypted message, we use ECC (Error Correction and Coding) using (7,4) Hamming Code where reorganization of data is done. Finally, to increase the strength of the Stego video Deep Steganography method is implemented, where Deep Neural Networks is used, where we try to place a Full-size color image within another image with minimum distortion. This paper presents a novel method i.e. robust Steganography which is effective when compared to existing Steganography methods. It also provides comparison of various methods to improve the security of the message.

Keywords: Video steganography, Security, Advanced Encryption Standard (AES), Least Significant Bit (LSB) algorithm, data hiding, hamming code, Deep steganography, secret message, cover video, video frames, Steganalysis, stego video, PSNR ratio, ECC (Error Correction and Coding), and MSE (Mean Square Error).

I. INTRODUCTION

Video Steganography refers to using video as a cover object (carrier file) to hide some secret message inside the video file by using some embedding procedure. This secret information will be hidden in the text, image, audio, and video files [1] [2]. Hiding secret information in the video files is called video steganography. Steganography is defined as the art of concealing secret information in specific carrier data, establishing covert communication channels between official parties. The primary objective of the steganography is to eliminate any suspicion of the transmission of hidden messages and provide security and anonymity for legitimate parties. As the usage of the internet in the world is increased very high, hence all are needed more security. Internet developers are always trying to make the internet free from jamming. For that there are many techniques and algorithms are proposed. They are also worked on how the hackers are acting smartly to hack information and also invent new techniques to stop hacker's intentions. Any techniques which try to improve the embedding payload or robustness should preserve imperceptibility. Different embedding payload may have different effects on audio quality. In this paper, the deep steganography method is used for video steganography to get efficient results and with less distortion. The steganography is one of among old sciences as the cryptography [2]. Steganography becomes of greater significance in the digital era as more people are joining the cyberspace revolution. Its main objective is to pass unnoticed information in another message. Computer network requires special means of security as the number of data being exchanged on the internet is increasing. Therefore, confidentiality and data integrity play a major role to protect against unauthorized access. In modern literature, the aim of steganography is to hide secret data in a medium file so that an intruder who controls the communication does not remark existing a hidden message behind the medium file. The medium file can be an image, a sound, a video, etc. Video steganography is the most common form of steganography that is used in various applications for hiding text in the image, video in the image, and audio in the image. In our paper, we study four techniques of data hiding in an image or video, they are AES algorithm, Least significant bit substitution, (7,4) Hamming code, and hiding images in plain text using Deep Steganography. In our work we study the LSB technique (LSB) i.e. embedding the secret data into the cover video and in order to protect and provide security for the stego-image AES (Advanced Encryption Standard) algorithm is used. We take different images of various formats and try to hide the secret data of varied length into the cover image. Then PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) between the original and the encrypted image is estimated. PSNR, MSE, and histogram are also plotted.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

II. MOTIVATION

Steganography hides the very existence of information / given message so that if successful it generally attracts no suspicion at all. Using steganography technique, information can be hidden in carriers such as audio files, images, text files and videos. Major advantages of Image Steganography have motivated us to take up this assignment. Firstly, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional to the size of the stego texture image. Secondly, a steganalytic algorithm is not likely to defeat this steganographic approach since the stego texture image is composed of a source texture rather than by modifying the existing image contents. Third, the reversible capability inherited from our scheme provides functionality to recover the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed.

III. LITERATURE SURVEY

Video and image based steganographic methods are mainly classified into frequency and spatial domain based techniques. The former embedding techniques are LSB embedding, AES embedding, using (7, 4) Hamming code and hiding images in plain text using Deep Steganography. Over the past few years, numerous form of steganographic algorithms based on the replacement of least significant bits have been proposed. Two important parameters for checking the performance of this system are capacity and undetectability. To expand the capacity of the concealed secret information and to give an detectable stego-image for human vision, an Advanced encryption standard(AES) algorithm is used for inserting and (7,4) hamming code algorithm is also used in order to provide high embedding efficiency.

The next technique we are using is hiding images in plain text using Deep Steganography. In this section, we briefly discuss a few observations found in this study and present ideas for future work. This study opens a new method for study with steganography and, more generally, in placing supplementary information in images. We have illustrated a technique to create a fully skilled system that provides visually excellent results in unobtrusively placing a full-size, color image into another image. Few related works on the evolutionary steganography:

1. In [1], the imperceptibility, hiding capacity, and robustness against attacks are three main requirements that any video steganography method should take into consideration. In this paper, a robust and secure video steganographic algorithm in discrete wavelet transform (DWT) and discrete cosine transform (DCT) domains based on the multiple object tracking (MOT) algorithm and error correcting codes is proposed. The secret message is preprocessed by applying both Hamming and Bose, Chaudhuri, and Hocquenghem codes for encoding the secret data. First, motion-based MOT algorithm is implemented. Then, the data hiding process is performed .This improves the embedding capacity and imperceptibility but also enhances its security and robustness by encoding the secret message and withstanding against various attacks.
2. In [2],they proposed an improved method based on the combination of the Pseudo-random LSB (Bit Substitution Technique) and the cryptographic algorithm and used AES algorithm with size key 256 which is the strongest symmetric algorithm until now and it is very fast compared to asymmetric-key algorithms. In this approach, reduced the length of hidden message by Deflate algorithm which is a lossless data compression algorithm that combines the LZ77 algorithm and the Huffman algorithm. In this work, hide a secret message of type text in a medium file of type image.
3. In [3], it proposes a method to replace a full size color image within another image of the identical size. Deep neural networks at the same time are trained to generate the hiding and disclosing processes and are planned to notably work as a set. The structure is trained on images drawn arbitrary from the Image Net database, and slogs well on natural images from a vast diversity of sources. Beyond signifying the successful request of deep learning to concealing images, we thoughtfully examine how the outcome is attained and survey extensions.
4. In [4], hide the secret message or image inside the image using Least Significant Bit technique. To protect and provide security for the hidden message or image, Advanced Encryption Standard (AES) Algorithm is used. Various image formats with different text length or image size are compared. Efficiency of algorithm is estimated by Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) where higher PSNR value gives the high-quality image.

IV. SOFTWARE REQUIREMENTS SPECIFICATION

A. Functional Requirements

A functional requirement defines a function of a system or its components, where a function is described as a specification of behaviour between outputs and inputs. It involves technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish.

- Image file in the form of JPEG and video in the form of AVI.
- The text to be transmitted securely in digital format.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

- The bit stream to be embedded onto a cover image (or a video) or a stego object along with a stego key (known by both sender and receiver).
- Decryption of the information at the receiver end to obtain original data.

B. Non-Functional Requirements

Non-functional requirements define certain parameters such as usability, reliability, performance, scalability, portability, reusability and flexibility of the system even at its critical stages of functioning.

- Usability-Simple is the key here. The system must be simple that people like to use it, but not to complex that people avoid using it. The user must be familiar with the user interfaces and should not have problems in migrating to a new system with a new environment. The menus, buttons and dialog boxes should be named in a manner that they provide clear understanding of the functionality. Several users are going to use the system simultaneously, so the usability of the system should not get affected with respect to individual users.
- Reliability- The system should be trustworthy and reliable in providing the functionalities. Once a user has made changes, the changes must be made visible by the systems. The changes made by the programmer should be visible both to the project leader as well as the test engineer.
- Performance- The system is going to be used by many employees simultaneously. Since the system will be hosted on a single web server with a single database server in the background, performance becomes a major concern. The system should not succumb when many users would be using it simultaneously. It should allow fast accessibility to all of its users. For example, if two engineers are simultaneously trying to report the presence of a bug, then there should not be any inconsistency while doing so.
- Scalability- The system should be scalable enough to add new functionalities at a later stage. There should be a common channel, which can accommodate the new functionalities.
- Reusability- The system should be divided into such modules that it could be used as part of another system without requiring much of work.

V. PROPOSED METHODOLOGY

Steganography techniques can be chosen based on their ability to secure communication and their resistance to being cracked. Our paper proposes secure methods to resist the steganalysis and they are: AES method, LSB Substitution method, Hamming Code method and Deep Steganography.

1. Advanced Encryption Standard (AES)

When AES is compared with DES Algorithm, AES is more mathematically efficient than DES [3]. The main benefit of AES lies in its key length options. Depending upon the key length the time to crack the encryption algorithm is estimated. This secures the communication and provides high throughput. Figure 1 shows the AES encryption process. The cipher takes a plaintext block size of 128 bits or 16 bytes. The Algorithm is referred to as AES-128, AES-192, or AES- 256, depending on the key length. The input to the encryption and decryption algorithm is a single 128-bit block. The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32- byte key. The first N-1 rounds consist of four distinct transformation functions: Sub Bytes, Shift rows, Mix columns and Add round key. The Output of the final round is cipher text.

- *Substitution Bytes*: Uses an S-box to perform a byte-by-byte substitution of the block.
- *Shift rows*: It is a simple permutation.
- *Mix columns*: It is a substitution process.
- *Add round key*: It is a simple bitwise XOR of the current block with a portion of the expanded key.

For both encryption and decryption process the cipher begins with an Add Round key stage, which is followed by nine rounds where each round includes all four stages. Only Add Round Key stage makes use of a key, Hence the cipher begins and ends with an Add Round Key stage. Each stage is reversible. The decryption algorithm makes use of an expanded key in reverse order. AES Encryption process is more secure because each round is provided with different keys. This makes the cipher strong and it cannot be broken easily. Figure 2 shows both the encryption and decryption process.

2. Least Significant Bit(LSB) Substitution

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 susceptible to steganalysis so we encrypt the raw data before embedding it in the image to make it more secure. Though the embedding process increases the time complexity, but at the same time provides higher security also. In this method the least significant bits of few or all of the bytes inside an image is altered with a bits of the covert message. [2] The simplest of LSB steganography techniques is LSB replacement for all pixels of n image. Since only LSB is changed, the difference between the cover (i.e. original) image and the stego-image is difficult to notice. This LSB technique has become the basis of many techniques that hide the secret information within the carrier data. First part explains about the encoding process where the covert data is hided and next part explains about the decoding process where the data gets retrieved. Figure 3 shows the LSB method of hiding data. Figure 4 shows the effect of replacing *k* LSB bits of the carrier image (a) and by a secret data, (b) and the resulting stego image is

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

shown in (c). The extracted secret data is shown in Figure 4(d). The image degradations due to using different number of LSB bits are shown in Figures 4(c) and (d). We can conclude that, as more LSB bits are used, the worse the stego image becomes, and the more the stego recovered secret data is, and vice versa. [5] [6]

3. (7,4) Hamming Code

The Hamming Code is one of the most popular block code techniques that can do both error detection and correction on a block of data. (7, 4) Hamming code is used to detect and correct a single bit error of data or parity. First, the message (M1, M2, M3, and M4) of length k bits is encoded by adding three parity bits (P1, P2, P3) to become the code word of length n, which is ready for transmission. The Hamming codes are linear codes so they have two matrices: parity-check matrix H and generator matrix G, which they need for both encoding and decoding. On the encoding side, each message M, which consists of 4- bits, will be multiplied by the generator matrix and then have modulo of 2 applied; the result is the code word X of 7-bits ready to be sent through a noisy channel. [10]

4. Deep Steganography

Steganography is the practice of concealing a secret message within another, ordinary, message. Commonly, steganography is used to unobtrusively hide a small message within the noisy regions of a larger image. In this technique, we attempt to place a full size color image [4] within another image of the same size. By demonstrating the successful application of deep learning to hiding images, we carefully examine how the result is achieved and explore extensions. In this technique, the goal is to visually hide a full N × N × RGB pixel secret image in another N × N × RGB cover image, with minimal distortion to the cover image. By demonstrating this technique we can also provide brief discussions of the discoverability of the existence of the secret message. Though visually hard to detect, given the large amount of hidden information, we do not expect the existence of a secret message to be hidden from statistical analysis. Nonetheless, we will show that commonly used methods do not find it, and we give promising directions on how to trade- off the difficulty of existence-discovery with reconstruction quality, as required. [7]

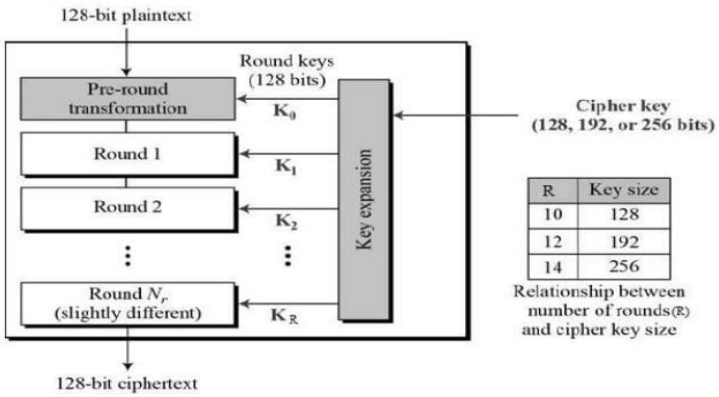

Figure 1 shows the AES encryption process.

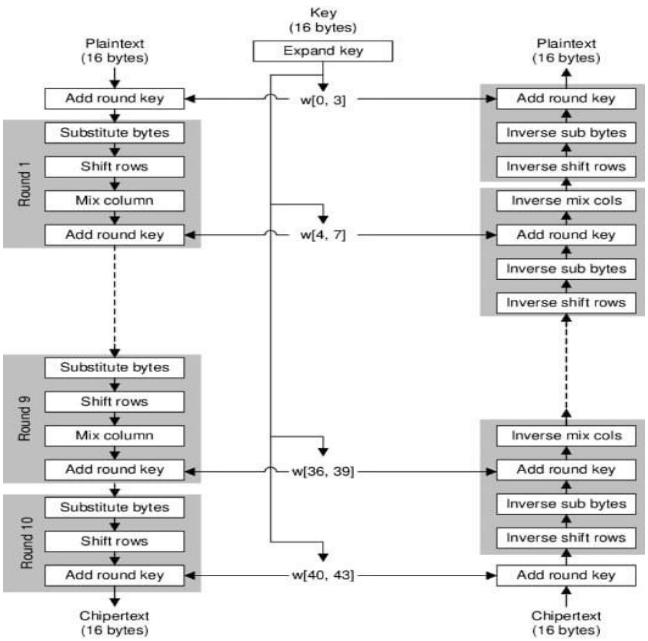

Figure 2 shows both the AES encryption and decryption process.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

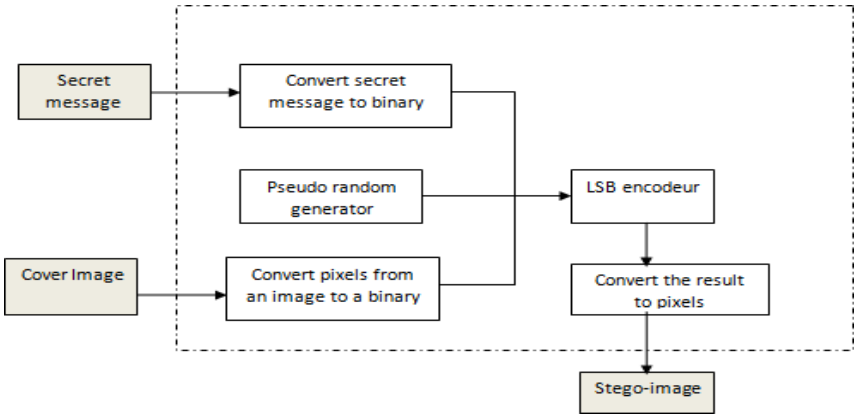

Figure 3 shows the LSB method of hiding data.

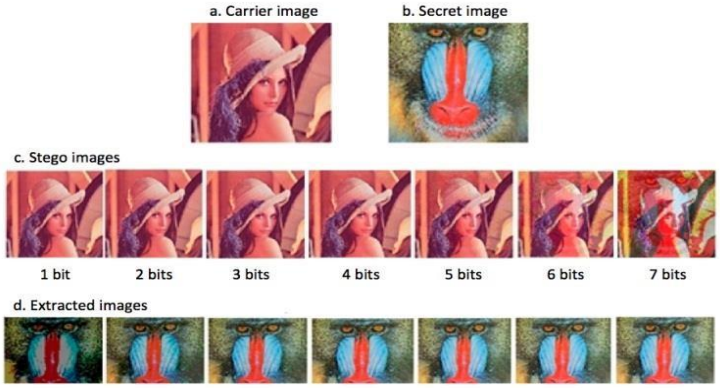

Figure 4 shows the carrier, secret, stego images and extracted images of the LSB method of steganography.

VI. IMPLEMENTATION

We train the hiding and reveal networks simultaneously in the form of an auto encoder, using keras. The model has two inputs corresponding to a pair of secret and cover image and two outputs corresponding to their inputs. Since we are using a auto encoder based architecture, the labels are same as their corresponding inputs [4]. The network consists of three parts viz. Prepare block, Hide block, Reveal block. In prepare block, we transform the color- based pixels to more useful features for succinctly encoding the images. We then hide this transformed image inside the input cover image using the hide block, to generate the container image. Finally, in the reveal block we decode the container image to produce the secret output. Therefore, the training graph has two inputs and two outputs. Net, Hide Net, and Reveal net have the same convolution block structure. Therefore, in the image, only the reveal network is shown, and prep/hide networks are collapsed (to make the image fit). We use a weighted L2 loss function along with Adam optimizer for training the model. The model is trained for 100 epochs suing a batch size of 8.

Loss: L(c, c 0, s, s 0) $= ||c - c\ 0\ || + \beta||s - s\ 0\ ||$

Here c and s are the cover and secret images respectively, and β is how to weigh their reconstruction errors

To ensure that the networks do not simply encode the secret image in the LSBs, a small amount of noise is added to the output of the second network (e.g. into the generated container image) during training. After the training, we split the trained model into two: hide network and reveal network (we remove noise layer).The hide network has two inputs corresponding to secret and cover image and one output corresponding to the container image**.** The reveal network takes the container image as input and reveals (decodes) the secret image as output. [8]

1. The hide network is used by the sender while the reveal network is supposed to be used by the receiver.
2. The receiver has access only to the container image. In addition to the normal steganographic hiding mechanism, we also encrypt (block shuffle) our secret images for added security.
3. Therefore, both the sender and the receiver share a symmetric key for encrypting/decrypting the shuffled secret message.
4. The encryption is performed by the sender on the input secret image; whereas the decryption is performed by the receiver on the final decode image.

Figure 5 shows the flowchart of reveal network and figure 6 shows the flowchart of hide network. Figure 7 shows the steps involved in deep steganography (train/ network diagram).

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

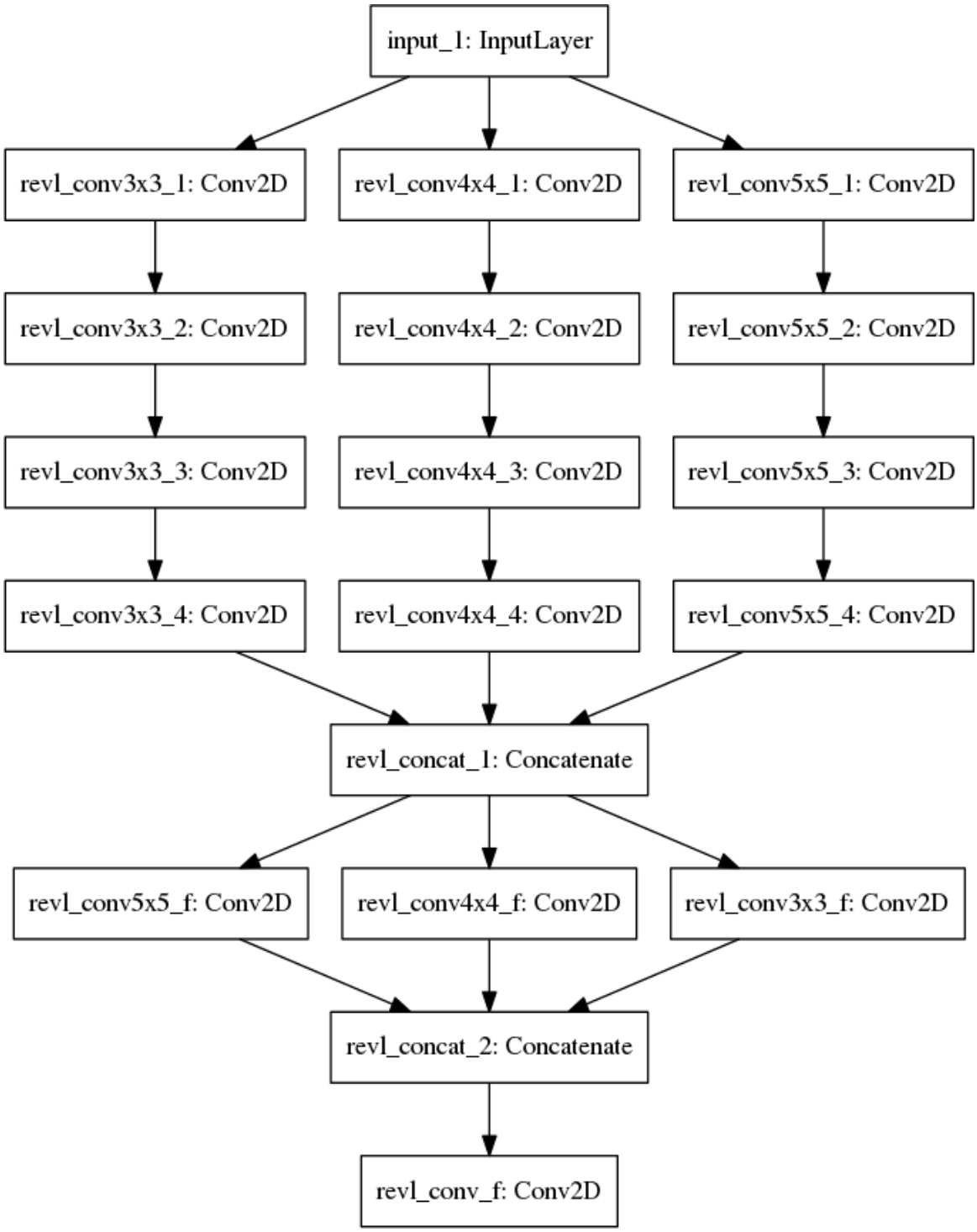

Figure 5 shows the flow chart of the reveal network

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

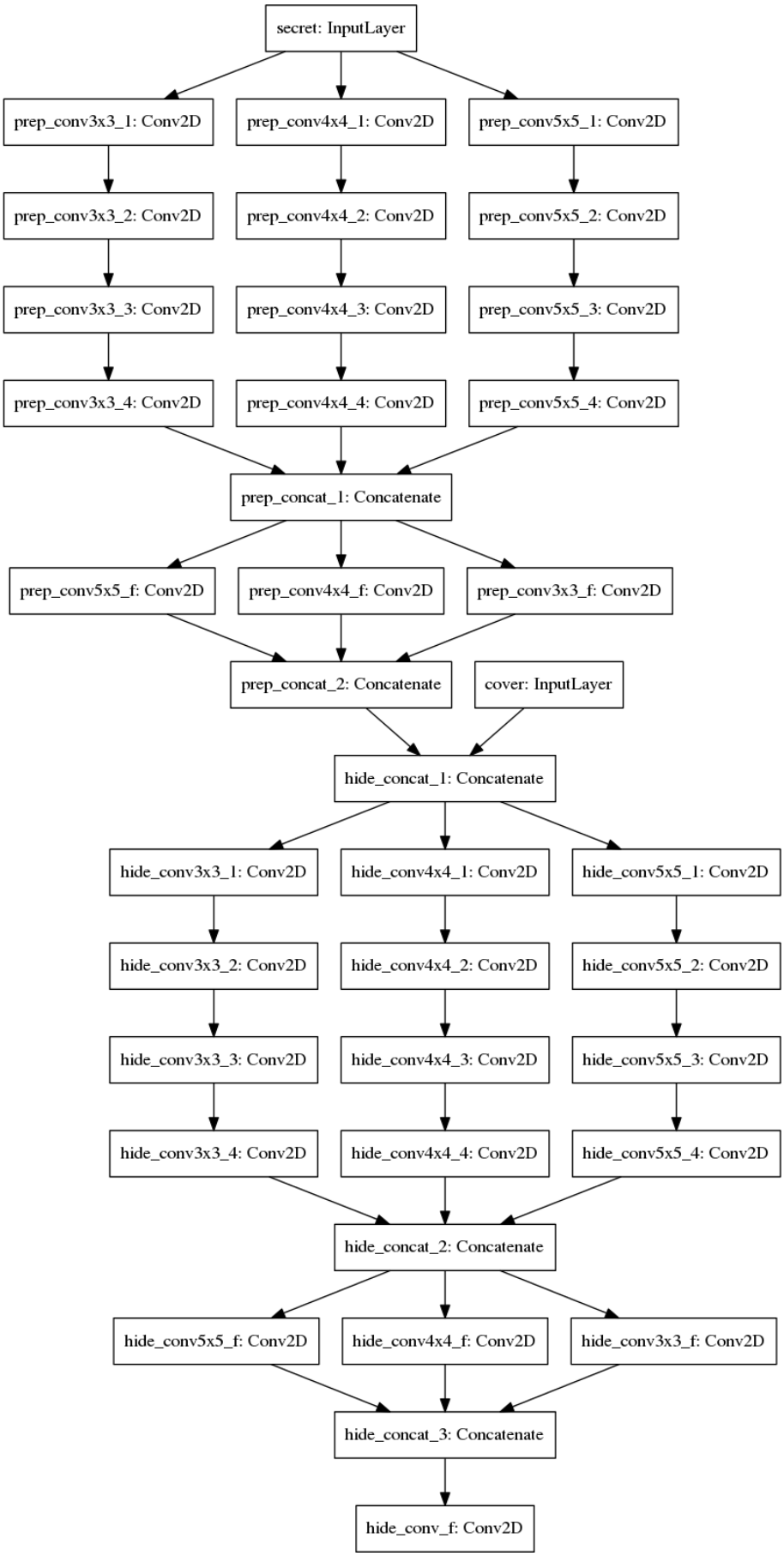

Figure 6 shows the flowchart of hide network.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

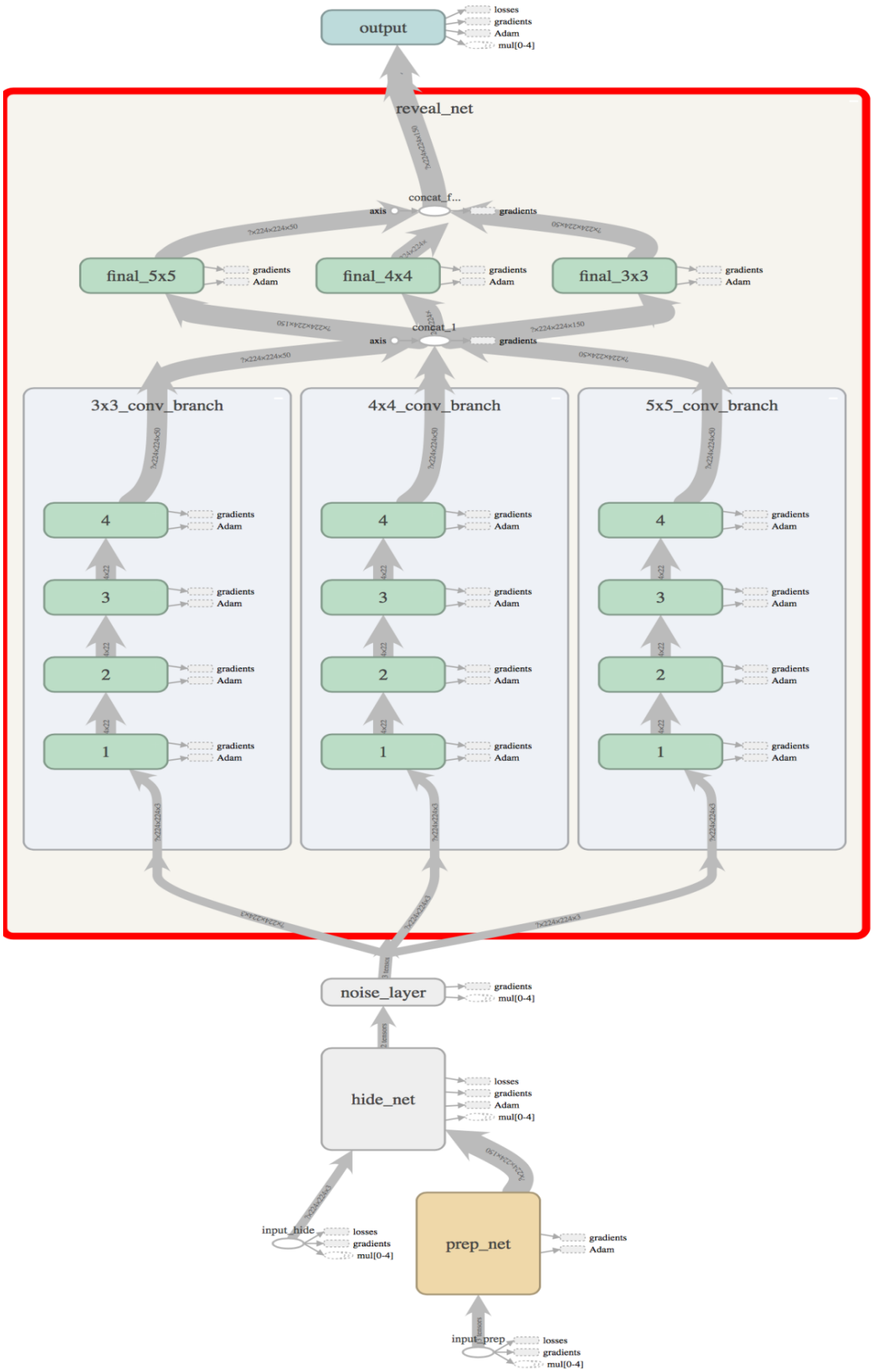

Figure 7 shows the steps involved in deep steganography (train diagram/ network diagram).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

VII. RESULTS

The following technique was practiced on google colaboratory using the Python software. [9] This technique undergoes two sub processes i.e. image in image hiding and video in video hiding process. During the first technique, we are considering two images, “cover.png” and “secret.png” which are the cover image and the secret image respectively. Figure 8 shows the cover image and figure 9 shows the secret image. Later, the secret image is hidden in the cover image,thus producing a stego image. Figure 10 shows the stego image. Finally, the stego image undergoes the reveal technique and hence the secret image which is hidden in the stego image is retrieved back. Figure 11 shows the secret image which is retrieved back. During the second technique i.e. video in video hiding, we make use of two images namely: “cover_input.gif” as cover video and “secret_input.gif” as secret video. There are totally 189 frames in the cover video and 174 frames in the secret video. As the technique is complicated, hence it consumes more time. In order to overcome this problem, we work on all the frames at a time. We are diving all the frames into batches and each batch consists of five frames. Next, we are performing the hide technique where the secret video is hidden inside the cover video by which we obtain the stego video. In order to retrieve back the secret video, the stego video undergoes the reveal technique thus producing back the secret video. Figure 12 and 13 shows ‘cover_input.gif’ and ‘secret_input.gif’ respectively. Figure 14 shows the stego video.

Figure 8 shows the cover image

Figure 9 shows the secret image.

Figure 10 shows the stego image.

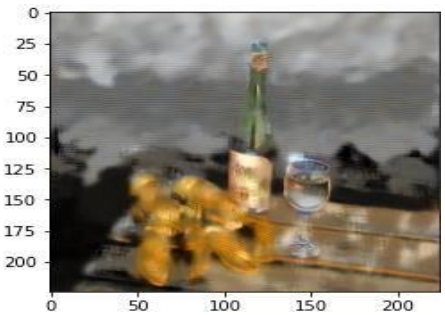

Figure 11 shows the secret image which is retrieved back.

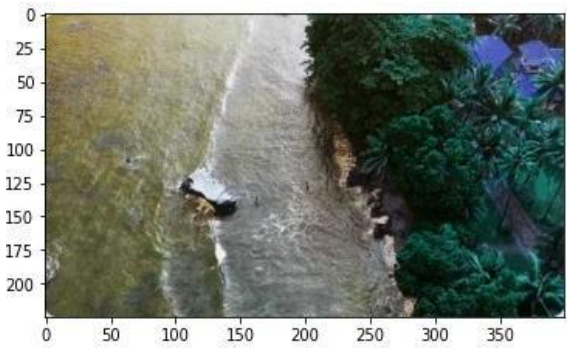

Figure 12 shows ‘cover_input.gif’.

Figure 13 shows ‘secret_input.gif’.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

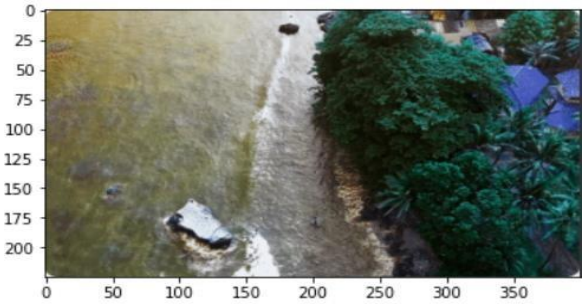

Figure 14 shows the stego video.

VIII. CONCLUSION

In this paper we have proposed various methods of steganography and implemented the video steganography process. Deep steganography which is one of the video stegnography methods was implemented on python software. This method explores Steganographic techniques for placing supplementary information in images. Here a method is demonstrated to create a fully trainable system that provides excellent visual results in placing a color image into another image. The chosen system should be retrained as a hiding network where the secret image's local structure should not be exploited for encoding information. In this paper, methods are proposed to make it difficult for the attacker to recover the contents of the hidden image by reducing the similarity of cover image's residual to the hidden image.

REFERENCES

[1] Ramadhan J. Mstafa, Khaled M. Elleithy,and Abdelfattah, "A Robust and Secure Video Steganography Method in DWT- DCT Domains Based on Multiple Object Tracking and ECC".
[2] Sofyane Ladgham Chikouche and Noureddine Chikouche, "An Improved Approach for LSB-Based Image Steganography using AES Algorithm" The 5th International Conference on Electrical Engineering – ICEE-B October 29- 31, 2017.
[3] Jorg J. Buchholz, "Advanced Encryption Standard" http://buchholz.hs-bremen.de , December 19, 2001.
[4] Shumeet Baluja "Hiding Images in Plain Sight : Deep Steganography" 31st Conference on Neural Information Processing Systems NIPS 2017.
[5] Priya Paresh Bandekar and Suguna G C, "LSB Based Text and Image Steganography using AES Algorithm" the International Conference on Communication and Electronics systems (ICCES 2018) IEEE Xplore Part Number: ISBN:978-1-5386-4765-3.
[6] C. Lalengmawia, A. Bhattacharya, "Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data" 2016 5th International Conference on recent trends in information technology, 2016 IEEE.
[7] Ranyiah Wazirali, Waeed Alasmary, Mohamed Mahmoud, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms" volume 4, 2016, DOI 10.1109/ACCESS.2019.2941440, IEEE Access.
[8] Dolnghui Hu, Shengnan Zhou, Qiang Shen, Shuli Zhenh,Zhongqiu Zhou, and Yuqi Fan, "Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning" volume 7,2019 10.1109/ACCESS.2019.2900076IEEE access.
[9] Souma Pal and Prof.Samir Kumar Bandyopadhyay, "VARIOUS METHODS OF VIDEO STEGANOGRAPHY" International Journal of Information Research and Review Vol. 03, Issue, 06, pp. 2569-2573, June, 2016.
[10] Ramadhan J. Mstafa and Khaled M. Elleithy, "A Highly Secure Video Steganography using Hamming code (7, 4) IEEE long usland systems, DOI: 10.1109/LISAT2014.6845191.

OUR GUIDE

Mrs Sowmya K S is an Associate Professor in the Department of ECE, DonBosco Institute of Technology. . She has a total teaching experience of 17 Years. She has done bachelor's degree in Electronics and Communication Engineering from Siddaganga Institute of Technology, Tumkur under Bangalore University. She is GATE qualified and obtained Masters in Electronics Engineering from BMS College of Engineering, Bangalore under VTU. She holds Honours Diploma in Network centered computing from NIIT. Her research interests are in computer vision and machine learning with a focus on visual recognition and understanding of human actions and activities, objects, scenes, and events. She is an active researcher, having presented her work in conferences of repute and published in domestic and international journals. She has worked as an organizing committee member for International conferences successfully organized by Department of ECE, DBIT. She has guided more than 20 projects at UG and PG level. She has won Best Project Award in the Final year Project Exhibition & Best Paper Award in International Conference on recent trends in signal processing; image Processing & VLSI Organized by Dept of ECE, Don Bosco Institute of technology.