International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Deep Convolutional Neural Network based Image Steganogrpahy Technique for Audio-Image Hiding Algorithm

D.Rathna Kishore, D.Suneetha, P.Narendra Babu, P.Chinababu

Abstract: ***Steganography is one expanding filed in the area of Data Security. Steganography has attractive number of application from a vast number of researchers. The most existing technique in steganogarphy is Least Significant Bit (LSB) encoding. Now a day there has been so many new approaches employing with different techniques like deep learning. Those techniques are used to address the problems of steganography. Now a day's many of the exisiting algorithms are based on the image to data, image to image steganography. In this paper we hide secret audio into the digital image with the help of deep learning techniques. We use a joint deep neural network concept it consist of two sub models. The first model is responsible for hiding digital audio into a digital image. The second model is responsible for returning a digital audio from the stego image. Various vast experiments are conducted with a set of 24K images and also for various sizes of images. From the experiments it can be seen proposed method is performing more effective than the existing methods. The proposed method also concentrates the integrity of the digital image and audio files.***

Index Terms: Steganography, Least Significant Bit, Deep Learning, Deep Convolutional Neural Network

I. INTRODUCTION

Now a day's computers and internet play an important role in this modern field especially in the field of information technology? Among those the important of data security plays a vital role. So much research is going in the field of data security. There are two main solution are existing for data security Cryptography and steganography. Cryptography is to protect the content of any message. Steganography is nothing but hiding of content in any of the media like image, audio and video etc. Under steganogarphy have various types of steganography techniques. Image steganography, audio steganography and video steganaography. Image steganaography means hiding of secret data into an image. In audio steganogrpahy hiding the secret data into the image and in video steganography hiding the secret data in to the video. In this paper we implement the concept of audio-into-image steganography[1][2] which hides the secret audio in to the digital image.

Revised Manuscript Received on April 27, 2020.
* Correspondence Author
Dr.D.Rathna Kishore*, Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.
Dr.D.Suneetha, Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.
Mr.P.Narendra Babu, Associate Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.
P.Chinababu, Assistant Professor, Department of CSE, LIMAT, Vijayawada, A.P, India.

When compared to hiding images to images hiding audio into image is more difficult because audio and image both are belonging to the different domains. In general audio data is in the form of one dimensional array and image is in the form of three dimensional arrays. Audio values are ranges from -2^{15} to $2^{15}-1$ and images values are ranges from 0 to 255. To eradicates these problems the proposed approach using deep convolutional neural network (DCNN) model. The DCNN model is capable of hiding audio and images.

The main contribution of this paper

1. The proposed work use DCNN to address the main problem of hiding the secret audio into the digital image
2. Comparing the proposed method on different images of various sizes.
3. Showing the proposed method is more effective than the traditional existing method.

The rest of the paper is organized is as follows. Section 2 presents literature review: it present brief review about various existing methods. In section 3 have proposed model architecture which is used for preprocessing of given data and hiding of given image into audio fie. Section 4 has experiments results. And section 5 provides the conclusion and future scope for this proposed approach.

II. LITERATURE REVIEW

Steganography technique has a very long history. It is one of the oldest techniques. This technique can be found from many of the surveys and applications. All the methods in the existing steganography techniques are very basic in traditional steganography techniques[3][4]. These methods are very simple and can be easily detected by the third party with this as a result modern secured algorithm was introduced in digital signal processing. In the field of digital signal processing so many algorithms are developed to embed data in a secure manner. Mchaughn[5] proposed one of the earliest method which is used to embed secrete data into 4 LSB bits of an cover image. Heranedz[6] proposed another technique for hiding data. In this technique data was hidden in different formats other than the image. In this for hiding use HTML, XML and EXE files. Hosmer[7] propose LSB technique for hiding the secret data. In this technique GIF and JPEFG format of an image and also this technique supports hiding of data in a music file also. The LSB based steganogaphy techniques have major drawbacks. One of the main disadvantages of this mechanism is to lack of robustness, when we apply the process of steganalysis. To avoid these type of existing problems in LSB approaches, we can employ deep neural networks. Imran[10] proposed one of the technique related to deep neural networks.

In this the feature representations can be automatically learned by the network. The proposed method of these methods using 10 convolutional layers. In another technique for this neural networks are used to hide the secret image into another image of the same size. Juilo[9] proposed another end to end neural network for both encoding and decoding. In this the hidden data is in the form of bits. Audio to image steganogrpahy is one of the fields in steganogrpahy. This hides secret data into the audio file. One of the major drawback for this one is both are in different formats. Audio have different range of frequency and message bits have different range of frequency level and both are belongs to different domains. In majority of the existing algorithms ere used Short wave Fourier transform to hide the secret data into the selected audio file. Based on this another algorithm was proposed known as generative algorithm which consists of different parts encode, decoder and steganalysis[11]. These parts are used for hiding and retrieving of secret data into the audio file with respect to audio to image steganography. Only some of the few algorithms were proposed. Most of the existing algorithms are using wavelets transform to compress the given data and use LSB algorithm for embedding the secret data into it[12].

III. PROPOSED METHOD

In proposed method first step is to obtain the preprocessing process for both image and audio files. In images first step is to convert into pixels with range of 0 to 255 and the domain range of values are in between 0 to 1. However the same processing technique is not applied to the audio files because the domain range is differ from audio files and images. Based on this reason we can use different technique. The amplitude of audio data is in the ranges of -2^{15} to $+2^{15}$-1. For this one two different methods are used for data preprocessing of audio files. In general the data preprocessing technique is used for normalization purpose.

Method 1: In this method raw audio data is converted into new 3 dimensional matrix of the same size as the three color images. Method 2: In this method apply the transformation technique for mapping two different domains of frequencies of audio and image. Model Architecture: The proposed model is divided into two different sub models namely prepare network and reveal network. In prepare network two sub models are present one is encoding sub model and decoding sub model. The encoding model extracts the different characteristics of audio while embedding image into the audio file. The hiding network of prepare model hides original image into corresponding audio file and it generate stego audio file. The decoding sub model is also called as reveal network decode the original audio from the container image. The general architecture for this proposed method is shown in Figure 1. Each components of our proposed algorithm consists of different convolutional neural networks and those are suitable for audio data and to help to reduce the training time of the entire architecture.

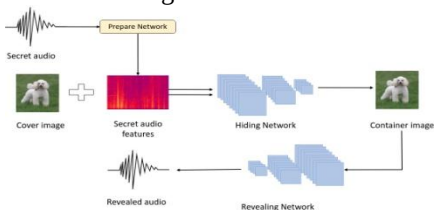

Figure 1: Architecture of proposed model

The proposed model consists of two basic models one is base model and prepare network; Base model: A block is architecture and it will available with the same size of kernel. There are three different parallel block are present in proposed network with different sizes. The outputs of the all the blocks are generated as a single convolutional layer. The base model is demonstrated in Figure 2 2) In prepare network two sub models are present one is encoding sub model and decoding sub model. Encoding sub model appropriately extracts the various characteristics o the audio before embedding with the image. And hiding network hides the secret audio features into the selected cover image and finally generated the container image. The decoding sub model is also called as reveal network decode the original audio from the container image. The general architecture for this proposed method is shown in figure. Each components of our proposed algorithm consists of different convolutional neural networks and those are suitable for audio data and to help to reduce the training time of the entire architecture.

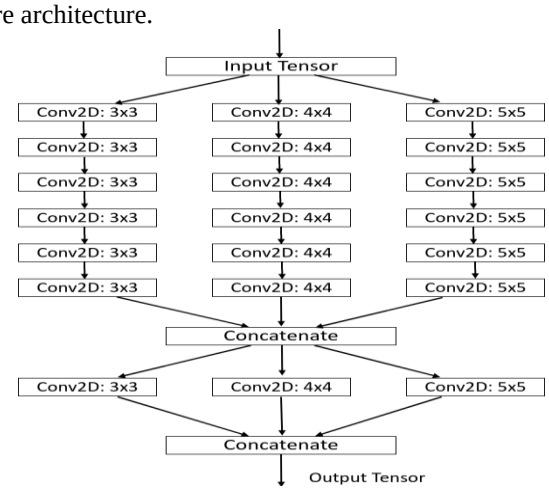

Figure 2: Architecture for Base model

IV. EXPERIMENTAL RESULTS:

For estimation of picture quality for projected algorithm two factors are estimated those are PSNR and MSE. The greater the PSNR, the recovering the environment of the trodden or re modelled picture. We can compute with this following specified expression[13].

$$PSNR=10 \log10 (MAXi^2)/MSE \quad (1)$$

Where MAXi is the extreme desirable pels value of a picture when the pels are denoted with 8 bits /sample this is 255.

The MSE expresses to the entire formed large variance between the trampled and the first picture. The lesser the calculated of MSE, the lesser the mistake.

$$MSE=\sum X, Y [J_1 (x, y)-J_2 (x, y)]^2/X*Y \quad (2)$$

In this region we present a comparison of various steganographic data hiding algorithms with projected security algorithm using image steganographic and image segmentation. It is clearly calculated and show there was a important change for projected algorithm is better than many extant algorithms based on the image segmentation and image steganography. For assessing various parameters and identifying difference between original cover picture and stego picture the MATLAB tools are used.

The resultant image after preprocessing technique is shown in Figure 3 and Table 1 shows the average correlation values with respect to preprocessing techniques.

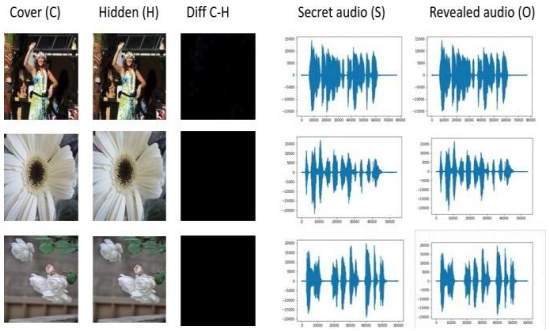

Figure 3: Results of preprocessing of raw data

Table 1: SSE (smaller is better) and correlation coefficient (greater is better) with raw and STFT pre-processing techniques

Pre-process	α/β	SSE	Average of correlation
Method-1: Raw	12 / 1	0.4566	99.83%
	11 / 1	2.0567	99.30%
	11 / 1	2.678	99.84%
	1 / 2	11.196	99.74%
	1 / 10	15.867	99.90%
Method-2: STFT	10 / 1	0.0192	99.43%
	12 / 1	0.0135	99.91%
	11 / 1	0.0334	99.85%
	1 / 2	0.0539	99.86%
	1 / 10	0.1393	99.93%

V. CONCLUSION

In this proposed technique, in audio-image steganography the use of deep learning techniques is explored. Two different models are designed with the help convolutional neural networks to work in pair with hiding the secret audio data into selected public image and retrieve the original audio from the container image. Various experiments were conducted and are carried out for different sizes of audio files with different formats of image files. Through this it has been verified the integrity of both audio and video files have to protect from unauthorized person and also it is to be preserved. The proposed method yields better length of audio data when compared to traditional existing steganography techniques. So the proposed method is capable of addressing various problem of audio into image steganography techniques.

REFERENCES

1. Faitha Djebbar, Beghada Ayad, Comparative study of digital audio steganography techniques, Journal on audio and sppech processinh
2. Aiswarya T, Steganographic Technique for Hiding Secret Audio in an Image, International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-03, Issue 04, May 2017
3. Pooja P. Balgurgi, Audio Steganography Used for Secure Data Transmission, Proceedings of International Conference on Advances in Computing
4. Chandramouli, Rajarathnam, Shumeet and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2001. Proceedings. 2016 Interna-tional Conference on. Vol. 3. IEEE, 2016.
5. Proceeding for the Second Information Hiding Workhop, Portland 0 regon, USA, April 1998, pp. 273-289.
6. Christina L, Kevin Curran Joe Irudayaraj V S “Optimized Blowfish Encryption Technique.” IJIRCCE Vol. 2(2017): 2320-9798.
7. Patil, Kaliappan Gopalan,Hosmer Priyadarshini, et al. "A comprehensive evaluation of cryptographic algo-rithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.
8. Awwad, DanieYousef Bani, and Mohammad Shkoukani. "The Affect of Genetic Al-gorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.
9. Van Cleeff, André, WolterPieters, and Roel J. Wieringa. "Security implications of virtualization: A literature study." Computational Science and Engineering, 2018. CSE'18. International Conference on. Vol. 3. IEEE, 2018.
10. Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to ste ganography." IEEE security & privacy 99.3 (2017): 32-44.
11. Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various ste-ganographic techniques used for information hiding." arXiv preprint arXiv:1401.5561 (2017).
12. Islam, Saiful, Mangat R. Modi, and Phalguni Gupta. "Edge-based image ste-ganography." EURASIP Journal on Information Security 2016.
13. Awwad, Yousef Bani, and Mohammad Shkoukani. "The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017).