iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49742

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Survey on Encoding Binary Data within a Digital Image Using Deep Steganography and Multilayered Neural Network

Anurag Singh[1], Ankur Kumar[2], Deepak Raj[3], Subhanshu Jha[4], Rakesh Kalshetty[5]
[1, 2, 3, 4]*Student,* [5]*Professor, Dept. of Computer Science Engg, SCE, Bangalore-560057, India*

Abstract: ***An image is the most popular media format amongst the current modern digital generation. Encoding binary data within an image is an easy way to hide the secret image. Broadly speaking, steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography helps us as the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages might be better protected but they arouse interest and may in themselves be incriminating in countries in which encryption is illegal. In other words, steganography is more discreet than cryptography when we want to send secret information while also being easier to extract. The usual implementations tend to significantly lose the image quality and are also easily detectable. However, this implementation makes efforts to overcome the existing problems of image steganography with the help of a deep neural network which results in the generation of a final image that is almost identical to the original image and isn't detectable easily.***
Keywords: Information hiding, Steganography, Multilayered Neural Network.

I. INTRODUCTION

In today's digital age, information security and privacy have become critical concerns. With the vast amount of data being transmitted and stored online, it is essential to have effective methods of protecting sensitive information from unauthorized access or interception. Steganography, which involves concealing data in another medium, such a digital image, is one such technique.

Deep steganography is a modern approach that utilizes multilayered neural networks to embed binary data within an image. This technique goes beyond traditional steganography by using advanced machine learning algorithms to ensure that the hidden data is virtually undetectable. With deep steganography, the binary data is encoded into the image's pixel values, making it indistinguishable to the human eye.

This technology has numerous practical applications, from secure communication to digital watermarking, and has become increasingly popular in recent years. In this paper, we will explore the concept of deep steganography, its working principle, and its potential applications.

A. Background

Maintaining data secrecy has become a vital problem as a result of the exponential increase of digital data, which has ushered in a new era of security concerns. Steganography has gained popularity as a promising method for hiding critical information in digital media including photographs, films, and audio files recently.

High degrees of data security have been demonstrated by deep steganography, a kind of steganography that employs deep neural networks to conceal data inside digital media. Particularly, it has been demonstrated that multilayered neural networks may successfully incorporate binary data into digital photographs while preserving the image's quality and perceptual resemblance.

The use of deep steganography with multilayered neural networks may have certain advantages, but there are still a number of issues that need to be resolved. For example, the trade-off between the data payload and the image quality, the encoding algorithm's resistance to assaults, and the algorithm's compatibility with various image formats.

In order to overcome these difficulties, we study in this paper how well deep steganography and multilayered neural networks encode binary data into digital pictures. We also look at how this method may be used in fields like digital forensics and secure data transmission. We want to give a deeper understanding of the possible influence of deep steganography and multilayered neural networks on data security in the digital era by addressing these research concerns.

B. Overview of Present Work

Before the dawn of deep steganography, steganography was done using traditional methods such as least significant bit (LSB) steganography, spread-spectrum steganography, transform domain techniques, adaptive steganography, and compressed-domain steganography. LSB steganography involves hiding data within the least significant bit of each pixel in an image, while spread-spectrum steganography involves spreading the hidden data over a wide frequency range to make it difficult to detect. Transform domain techniques hide data in the transform domain of an image, such as the discrete cosine transform (DCT) or the discrete wavelet transform (DWT). Adaptive steganography changes the steganographic method depending on the characteristics of the cover media, while compressed-domain steganography hides data in the compressed data of an image or audio file. These methods allowed for the effective hiding of data within digital media, but deep steganography using neural networks has since taken steganography to a new level of sophistication.

Deep steganography is a subfield of steganography that uses deep learning techniques to hide information within digital media. It involves training artificial neural networks on large datasets of cover media and their corresponding secret messages, to generate stego images that are visually indistinguishable from the original cover media, while still containing the hidden message.

C. Problem Statement

In this paper, we provide an answer to the question whether a method exists for encoding multiple images within a single image while minimizing the loss of secret image quality and keeping the container image hidden requires advanced steganography techniques. These techniques must ensure that the secret images are embedded within the cover image without significantly altering its appearance, making it difficult for anyone to detect their presence. This task involves finding a balance between the amount of data that can be hidden within the cover image and the level of distortion that can be tolerated. Additionally, the encoding process must be reversible, allowing the authorized parties to extract the hidden images without any loss of quality.

D. Objectives

The objective of this paper is to explore the use of advanced steganography techniques, specifically deep steganography and multilayered neural networks, for encoding binary data within digital images. In order to preserve the integrity of the cover picture and reduce the quality loss in the concealed data, the study intends to demonstrate the usefulness and efficiency of
CNN for embedding data within images. The goal is to offer a safe and dependable technique for concealing binary data in digital photographs, which may be applied to a variety of tasks like data transportation, digital forensics, and privacy protection.

II. LITERATURE SURVEY

Traditionally, image steganography is done using the Least Significant Bits (LSB) substitution method. Pictures typically have higher pixel quality, however not all of them are utilised. The foundation of LSB techniques is the idea that small changes in pixel values would not result in noticeable alterations. The encrypted data is transformed into binary form. The least significant bits in the noisy region are found by scanning the cover image. The LSBs of the cover picture are then filled with the binary bits from the secret image. It is important to use caution while using the substitution method because overloading the cover image could cause noticeable modifications that reveal the presence of the secret information [4] and [5].

The authors of [2] proposed an improved least significant bit (LSB) based steganography technique for images conveying better data security. The method used an embedding algorithm for hiding encrypted messages in nonadjacent and random pixels in the images where the area was smooth and had edges. Their main aim was to evaluate and design a new and improved information-concealing technology based on LSB. The improved LSB technique was both resilient and successful, as well as one that makes it extremely difficult for the naked eye to predict and identify the presence of any hidden data inside the host image.

Paper [3] discusses a new method of image steganography by encoding the encrypted data or message using Hash-LSB with Rivest–Shamir–Adleman (RSA), which provides more security to data. The main objective is to combine one steganographic technique and one cryptographic technique to enhance data security. The algorithm uses a hash function which is used to generate a pattern for concealing secret data bits into LSB of cover image pixel values, but if the hash function is figured out, the secret data can easily be decoded.

In the paper [4] a deep learning-based encoder-decoder model for encoding of images as the payload was proposed. The method directly used images to encode and recover from the cover image, unlike earlier methods which used the binary representation of secret data. This is a novel technique that showed excellent results on a wide range of image datasets. Though the technique is new, the visual loss in the data is high.

Proposed by the authors of [5] a steganography technique in which the secret data was encoded in jpeg pixels of the cover image. The image underwent Discrete Cosine Transformation (DCT) followed by a quantization process which transformed the cover image. Their main objective was to increase the embedding capacity which was done using the modified quantization process and to maintain the visual quality of the

reconstructed image which was achieved by embedding the secret data into middle-band quantized DCT coefficients. In this scheme, rather than embedding the secret data bits directly into the coefficients, an appropriate indirect approach is adopted to conceal two bits of the secret message into some selected DCT coefficients, but the method was tested only on grayscale images.

In the paper [6] authors discuss a method that combined cryptography and LSB-based Image Steganography. This paper is like some of the previously mentioned papers, as it combines cryptography and steganography. The security level is increased by using two private keys but the disadvantage here is that the LSB is an insecure technique for concealing messages since it can be easily detected.

The authors of [7] proposed Generative Adversarial Networks (GAN) model which can completely hide a Gray secret image into an RGB cover image of the same size. Their main aim was to improve data security through the use of adversarial training. The model experimented with different activation functions and different optimizers which speeded up the training and produced better results but were not suitable for applications that require the secret image to be accurately revealed since the secret image gets distorted.

The approach of utilizing CNN models for image steganography draws inspiration from the encoder-decoder architecture. The encoder takes two inputs - a cover image and a secret image, which generates a stego image. This stego image is then used as an input for the decoder, which outputs the embedded secret image. While different methods have tried different architectures, the fundamental principle remains unchanged. However, the concatenation of the cover image and the secret image varies among the different approaches, as do the convolutional layer, pooling layer, number of filters used, strides, filter size, activation function, and loss function. It's worth noting that the cover image and secret image must be of the same size to ensure that every pixel of the secret image is distributed in the cover image.

In the paper [1] , the author presented a Neural Network model based on autoencoders to hide a full-color image inside another color image of similar size with a minimal pixel loss in both images. Unlike the widely used steganography techniques which encode the secret image inside the least significant bits of the cover image, the method compresses and distributes the secret image's representation across all of the available bits. The system was trained with images from the ImageNet dataset and numerous transformations were applied to the image to analyze the quality of cover and secret images. paper [8] discussed a new high-capacity image steganography method based on deep learning which used SegNet Deep Neural Networks with a set of Hiding and Extraction networks. The SegNet Deep Neural Network with a collection of Hiding and Extraction networks enabled steganography and retrieval of complete pictures to boost steganographic ability. The DCT was used for converting the secret image, and then the modified image was encoded by Elliptic Curve Cryptography (ECC) but the amount of data that can be hidden inside the cover image was minimized when compared with other techniques.

The authors of the paper [9] primarily discussed the application of steganography on Portable Network Graphics (PNG) image media with the Spread Spectrum Image Steganography (SSIS) method which was more secure. The SSIS technique was more secure because the keywords from this method were known only to the sender and the receiver. From this research work, it was observed that if larger the image size (pixels), the larger the number of characters or messages that can be inserted. But the number of characters that can be inserted in the RGB digital image was more than the Grayscale digital image since RGB has 3 color channels and a greater number of characters can be inserted into it. So, for grayscale images, the system seems to be comparatively low in efficiency than the RGB digital images.

The paper [10] focused on the implementation of LSB Steganography on Bitmap along with Advanced Encryption Standard (AES) cryptography technique for better

security. The main focus was on the usage of Bitmap images since Bitmap images are uncompressed and more convenient than any other image format. Their research work involved a new Steganography technique to hide large data in Bitmap images using a filtering-based algorithm, which used the Most Significant Bit bits for filtering purposes.

This method used the concept of status checking for the insertion and retrieval of messages which was more efficient than the LSB method. But it is found to be more powerful for grayscale images only.

In the papers [11] and [12] the authors have proposed an encoder-decoder architecture. U-Net-based encoder-decoder architecture is used for hiding and a CNN with 6 layers for extraction is proposed by authors in [13]. The input shape of the U-Net is modified to accept 256 × 256 and 6 channels. The secret and cover images are concatenated to give the input and hence 6 channels. A U-net-based Hiding (H-net) and revealing (R-net) network are used by authors in [14].

Batch normalization and ReLU activation are used. The cover and the secret images are concatenated before being sent to the network. Two optimization losses using SSIM and MSE are used to reduce the loss and hence improve the performance. A Separable Convolution with Residual Block (SCR) is used to concatenate the cover image and the secret image [11]. The embedded image is given as the input to the encoder for constructing the stego image which is fed to the decoder to output the decoded secret image. ELU (Exponential Linear Unit) and Batch normalization are used. A new cost function to reduce the effect of noise in the generated container image called the variance loss is proposed [12]. An encoder-decoder
architecture was proposed by Rahim et al. in [14]. This method differs from the others in the way the inputs are given. The encoder part consists of two parallel architectures each for the cover and the secret image. Features from the cover image and the secret images are extracted through the convolutional layer and concatenated. The concatenated features are used to construct the stego image.

III. CONSOLIDATED TABLE

SL NO	REFERENCE	YEAR	DESCRIPTION	LIMITATIONS
1	[2]	2009	• Improved LSB for better security than previous approaches. • Hides encrypted message in non-adjacent and random pixels	• Less secure • Low payload capacity.
2	[3]	2016	• Encodes data using hash-LSB with RSA. • Combines steganography with cryptography	• Not as secure as deep learning methods. • If the hash function is figured then info is easily compromised.
3	[4]	2016	• Directly made use of images instead of binary data of it. • Deep learning based method.	• Visual loss of data was high.
4	[5]	2017	• Made use of DCT followed by quantization process. • Increase in embedding capacity	• Was tested only on black and white images.
5	[6]	2019	• Uses non symmetric cryptographic technique along with older LSB technique.	• Security level was increased but LSB was an insecure way to hide information.
6	[7]	2019	• GAN model which can hide B/W image in an RGB image.	• Distorted revealed image.
7	[1]	2020	• Use of auto-encoders to hide images. • Increased capacity of hiding.	• Loss of quality in revealed image.
8	[8]	2020	• High capacity image steganography method. • Uses DCT along with Ellipse Curve Cryptography for security.	• Amount of data that can be hidden wasn't large enough.
9	[9]	2017	• Makes use of Spread Spectrum Image Steganography technique. • Can encode data in PNG images.	• System showed low efficiency for B/W images in compared to RGB images.
10	[10]	2014	• Implementation of LSB technique on Bitmap format images. • Also makes use of AES encryption.	• Wasn't effective for non-grayscale images.
11	[11]	2018	• Image – to-Image deep learning technique. • Increased image capacity	• Noise in non-texture rich areas of recovered image.
12	[12]	2020	• New cost function introduced to reduce noise in generated images.	• Was less effective in case of non 1:1 ratio images.
13	[13]	2019	• U-net based hiding and revealing network used.	• 256*256 size images only accepted.
14	[14]	2019	• CNN based encoder-decoder architecture	• Payload capacity not high enough.

IV. ACKNOWLEDGEMENT

Any achievement does not depend solely on the individual efforts but on the guidance, encouragement and co-operation of intellectuals, elders and friends. We extend our sincere thanks to Dr. Kamalakshi Naganna, Professor and Head, Department of Computer Science and Engineering, Sapthagiri College of Engineering, and Rakesh Kalshetty, Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering, for constant support, advice and regular assistance throughout the work. Finally, we thank our parents and friends for their moral support.

V. CONCLUSION

In this paper, a method for transforming any binary data into an image and concealing the resultant picture within another image utilising sophisticated steganographic techniques is presented. The article specifically suggests using multilayered neural networks and deep steganography to insert the binary picture into the cover image while minimising any image quality loss. The objective is to offer a reliable method for concealing information inside digital photographs, with potential uses in data transfer, digital forensics, and privacy protection. The goal of the study is to illustrate the viability and efficiency of the suggested approach for securely encrypting data within digital photographs. This is done by utilising sophisticated steganographic techniques.

REFERENCES

[1] S. Baluja, "Hiding Images within Images," in IEEE Transactions on Pattern Analysis and Machine Intelligence,L. Zhu, J. Zhang, Z. Xiao, X. Cao, D. O. Wu, and X. Xia, “Joint Power Control and Beamforming for Uplink Non-Orthogonal Multiple Access in 5G Millimeter-Wave Communications,” IEEE Transactions on Wireless Communications, vol. 17, no. 9, pp. 6177–6189, Sep. 2018.

[2] M. Juneja and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," 2009 International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305, doi: 10.1109/ARTCom.2009.228..

[3] R. Halder, S. Sengupta, S. Ghosh and D. Kundu, “A secure image steganography based on RSA algorithm and hash-LSB technique,” IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 1, pp. 39–43, 2016

[4] A. Rehman, R. Rahim, M. Nadeem and S. Hussain, “End-to-end trained CNN encode-decoder networks for image steganography,” in ECCV Workshops, Munich, Germany, pp. 723–729, 2017

[5] A. K. Pal, K. Naik and R. Agrawal, “A steganography scheme on JPEG compressed cover image with high embedding capacity,” The International Arab Journal of Information Technology, vol. 16, no. 1, pp. 116–124, 2019.

[6] R. J. Rasras, Z. A. AlQadi and M. R. A. Sara, “A methodology based on steganography and cryptography to protect highly secure messages,” Engineering, Technology & Applied Science Research, vol. 9, no. 1, pp. 3681–3684, 2019..

[7] R. Zhang, S. Dong and J. Liu, “Invisible steganography via generative adversarial networks,” Multimedia Tools and Applications, vol. 78, no. 7, pp. 8559–8575, 2019.

[8] X. Duan, D. Guo, N. Liu, B. Li, M. Gou et al., “A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network,” in IEEE Access, vol. 8, pp. 25777–25788, 2020.

[9] B. Oktavianto, T. W. Purboyo and R. E. Saputra, “A proposed method for secure steganography on PNG image using spread spectrum method and modified encryption,” International Journal of Applied Engineering Research, vol. 12, no. 21, pp. 10570–10576, 2017.

[10] M. R. Islam, A. Siddiqa, Md. P. Uddin, A. K. Mandal and M. D. Hossain, “An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography,” International Conference on Informatics, Electronics & Vision (ICIEV), vol. 3, pp. 1–6, 2014.

[11] P. Wu, Y. Yang, and X. Li, ‘‘Image-into-image steganography using deep convolutional network,’’ in Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland: Springer, 2018, pp. 792–802.

[12] Pin Wu, Yang Yang, & Xiaoqiang Li (2018). StegNet: Mega Image Steganography Capacity with Deep Convolutional Network. Future Internet, 10(6),54.

[13] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ‘‘Reversible image steganography scheme based on a U-Net structure,’’ IEEE Access, vol. 7, pp. 9314–9323, 2019.

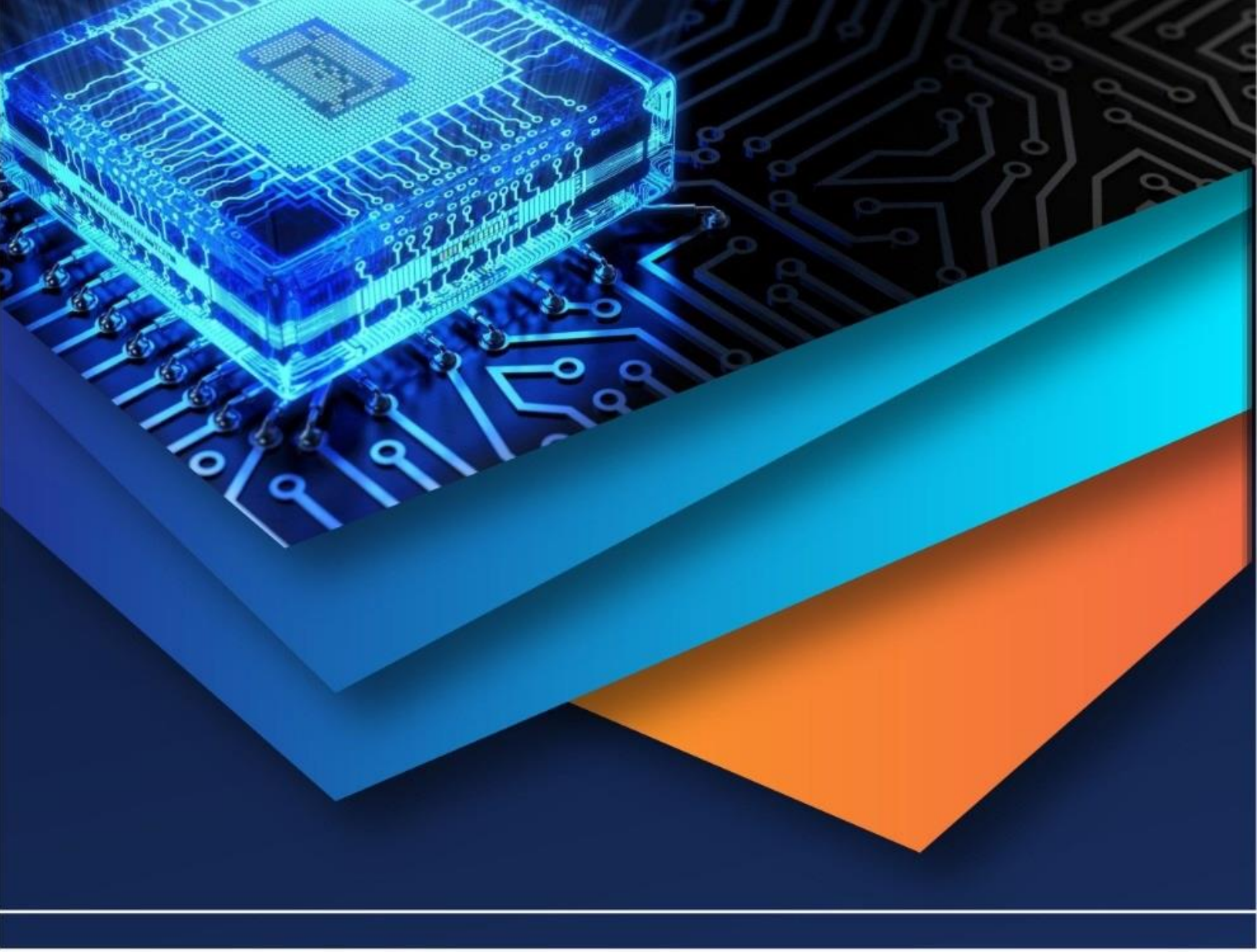
[14] T. P. Van, T. H. Dinh, and T. M. Thanh, ‘‘Simultaneous convolutional neural network for highly efficient image steganography,’’ in Proc. 19th Int. Symp. Commun. Inf. Technol. (ISCIT), Sep. 2019, pp. 410–415.

[15] R. Rahim and S. Nadeem, ‘‘End-to-end trained CNN encoder-decoder networks for image steganography,’’ in Proc. Eur. Conf. Comput. Vis. (ECCV), 2018, pp. 1–6.

[16] Hayes, Jamie, and George Danezis. "Generating steganographic images via adversarial training." Advances in neural information processing systems 30 (2017).

[17] Zhang, Ru, Shiqi Dong, and Jianyi Liu. "Invisible steganography via generative adversarial networks." Multimedia tools and applications 78.7 (2019): 8559-8575

[18] Agarwal, S., & Venkatraman, S.. (2020). Deep Residual Neural Networks for Image in Speech Steganography. /arXiv:2003.13217.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY