International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

Hybrid Cryptography and Steganography-Based Security System for IoT Networks

T.Suguna[1], C.Padma[2], ,M.Janaki Rani[3] , G.Padma Priya[4]
[1]Assistant Professor,
Department of ECE,
Panimalar Engineering College,
Chennai, India
suguna.pec22@gmail.com
[2]Associate Professor,
Department of ECE,
Sri Venkateshwara College of Engineering,
Tirupati, India
padmasekhar85@gmail.com
[3]Professor,
Department of EC,
Dr MGR Educational and Research Institute,
Chennai, India
janakiranimathi@gmail.com
[4]Associate Professor,
Department of ECE,
Sri Venkateshwara College of Engineering,
Tirupati, India
padmapriya.gudiyatham@svcolleges.edu

Abstract— Despite the fact that many IoT devices are publicly accessible to everyone on the network, understanding the security risks and threats posed by cyber attacks is critical; as a result, it should be safeguarded. Plain text is constructed into encrypted text, before being delivered by using cryptography, and is then reconstructed back to plain text after receiving a response from the recipient. The steganography technique can be used to hide sensitive information incorporated in a text, audio, or video file. One approach is to hide data in bits that correspond to successive rows of pixels with the same color in an image file. As a consequence, the image file retains the original's appearance while also containing "noise" patterns made out of common, unencrypted data. To do this, the encrypted data is subtly applied to the redundant data. In this work, it is suggested that IoT network data be encrypted using cryptography, and that an encrypted message be concealed inside an image file using steganography. Additionally, it is suggested to enhance the number of bits that may be stored within a single picture pixel. The payload that may be sent through an image is significantly increased by incorporating Convolutional Neural Networks into the classic steganography technique. In this work, we propose, design, and train Convolutional Neural Networks (CNN) to enhance the amount of data that can be securely encrypted and decrypted to show the original message.

Keywords- Encryption, Decryption, Security, IoT, Convolutioal Neural Networks (CNN)

I. INTRODUCTION

Sensors and minicomputers that use machine learning to act on sensor data are examples of IoT devices [1]. Sensor data is shared between IoT devices via a link to an IoT gateway or other edge device and is either forwarded to the cloud for analyzing or evaluated locally. Even while people may control, direct, and obtain data from the devices, the majority of the work is done by the devices on their own. [2].

Internet of things users have complete control over their lives and the ability to work and live more wisely. IoT is crucial to business in addition to giving smart home automation features. Businesses can use the Internet of Things (IoT) to track the performance of their systems in real-time and obtain insights into everything from equipment operation to supply chain and logistics operations. Businesses may use the Internet of Things (IoT) to automate processes and save expenditure on labor. Furthermore, it lowers production and transportation costs, enhances service delivery, minimizes waste and encourages greater consumer openness. [3]. As more businesses start to understand the importance of connected devices in maintaining their

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

competitiveness, IoT will gain in acceptance and rank among the most significant technology in daily life. IoT devices are susceptible to viruses and hacking since they are essentially tiny computers that are linked to the internet.

A. IoT Security Concerns:

This must be the first problem that manufacturers tackle if the Internet of Things is to become a major force. The risk of having their personal information taken from their smart home worried 27% of all Americans, which alarmed 44% of all Americans, according to the 2015 State of the Smart Home poll. Customers would be reluctant to buy similar things if they felt this unease. Because IoT devices are linked, it only takes one flaw to corrupt all data and render it useless. Manufacturers who fail to regularly or at all expose their products to cyberattacks.

Furthermore, linked devices frequently require users to input personal information such as names, ages, cellphone numbers, addresses and even their social media accounts that intruders may access. The amount of data created by IoT devices is incredible. Less than 10,000 households may generate 150 million discrete data points each day. According to the research "Internet of Things: A Consumer Guide" published by the Federal Trade Commission. Security and Privacy in a Connected World increases the number of entry points for invaders while also exposing personal information. [4].

Manufacturers or intruders could virtually break through an individual's house by using a linked device. The German researchers achieved this by obtaining unencrypted data from a smart meter device and identified which television show was being watched during the vulnerable period.

The objective of this paper is to develop a secure data transmission system for Internet of Things devices. Data was transferred in this case using a combination of cryptography and steganography, effectively increasing data payload while transferring through image files. Plain text is encrypted before being sent using cryptography, and following the other party's conversation, it is transformed back to plain text. Steganography is the process of hiding confidential information by encoding it into an audio, video, picture, or text file.

This paper is organized as, in section 2 discusses work related to the security systems related to IoT and their inferences. Section 3, discusses in detail about the existing system and proposed system for the IoT security. Section 4 discusses implementation ang its results and section 5 give the conclusion of the proposed models of IoT security systems with its future scope.

II. LITERATURE SURVEY

Since many IoT devices are publicly available to everyone on the network, even though it should be secured, it is critical to be aware of the security risks and hazards caused by cyberattacks. The survey for secure hybrid steganography communication technology is provided below. The following is a discussion of the most well-liked approaches currently in use.

The paired learning framework addresses the challenge of picture steganalysis, and S. Wu et al. [1] developed an important solution for CNN models, the Batch Normalization (BN). Theoretical results show that while successfully training with paired learning, a CNN model with several batch normalization layers struggles to generalize to fresh data in the test set. A brand-new normalization method called Shared Normalization (SN) is suggested as a solution to this issue. SN employs uniform statistics for training samples as opposed to the BN layer, which normalizes each input batch using the mini-batch mean and standard deviation. The authors then proposed a novel neural network model for image steganalysis based on the proposed SN layer. Extensive testing demonstrates that the suggested SN-layer network is robust and detects complex steganography more successfully than classic rich model methods and sophisticated CNN models. However, when cover-stegos are not paired, the network becomes unstable and fails to detect stego images.

Boroumand et al. [5] developed a universal deep residual architecture that eliminates the need for heuristics and externally imposed components while attaining cutting-edge detection accuracy for both spatial-domain and JPEG steganography. The front detector section that "computes noise residuals" with pooling turned off to avoid stego signal suppression is the distinguishing feature of the suggested architecture. According to comprehensive testing, this network performs better than others, with a notable improvement in the JPEG domain in particular. For payloads of 0.4 and 0.5 bpp, the improvement over the original SRNet is around 1%, gradually rising to 4% for the smallest tested payload 0.1. The procedure takes a long time, is difficult, and has poor accuracy for complex data.

PEKS (Public-key Encryption with Keyword Search) is a promising and practical encryption solution that secures and searches data stored in clouds. introduced near the IIoT as a cloud substitute to improve search efficiency even further. The slow PEKS encryption of IIoT devices delays edge response, therefore the straightforward connection of the two techniques works poorly in latency-sensitive applications. To solve this problem, W. Wang et al. [6] introduced Edge-aided

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

Searchable Public-key Encryption, a small-footprint method based on the edge-cloud architecture (ESPE). In addition to guaranteeing semantic security of all outsourced ciphertexts, this technology enables IIoT devices to offload time-consuming cryptographic operations to the neighboring edge for faster computing. Due to the fact that the throughput of encryption and decryption is inversely related to key length, ESPE speeds up the ciphertext corresponding procedures on edges and lowers the encryption cost of an IIoT device by over 70%. However, it is not suitable for encrypting large messages.

In order to offer a steganographic method that conceals a stego message while deceiving a convolutional neural network (CNN)-based steganalyzer, W. Tang et al. [7] used a novel technique called adversarial embedding (ADV-EMB). Due to the fact that the throughput of encryption and decryption is inversely related to key length, ESPE speeds up the ciphertext corresponding procedures on edges and lowers the encryption cost of an IIoT device by over 70%. However, it is not suitable for encrypting large messages. Therefore, the gradient's inverse sign is more likely to match the modification direction. This results in adversarial stego images. The test findings demonstrate that by raising the rate of missed detection, the suggested steganographic technique improves security against the target adversary-unaware steganalyzer. The proposed technique, however, solely employs gradient indications, which might lead to a faster rate of alteration with less image quality.

Adaptive payload distribution in multiple picture steganography was developed by X. Liao et al. [8] based on image texture properties, and a theoretical security research was carried out. Depending on the complexity and distribution of the picture texture, two payload distribution options are provided below. These strategies can be used with single-image steganographic algorithms. When contrasted to the modern universal pooled steganalysis per picture detectability versus the modern single image steganalyzer, these multiple image steganographic methods' security is evaluated. According to comprehensive investigations, payload distribution strategies suggested might enhance security performance. ESPE improves the ciphertext corresponding operations on edges and lowers the encryption cost of an IIoT device by more than 70% since the throughput of encryption and decryption is inversely related to key length. It is not, however, appropriate for encrypting long communications.

According to the literature review, FractalNet still [9] isn't capable of producing the best results when compared to those produced by other algorithms, even with significant data augmentation. Fractal networks can withstand being excessively deep; although improved depth reduces training, it has no negative effects on accuracy. The time it takes to train a steganalytic model for images with a little payload, say 0.1 or 0.05.bpp, is one of the main challenges. On some occasions, the model did not converge at all. When concealed messages are directly included into the cover picture, MIEM is produced, which lowers the performance of undetectability.

EXISTING SYSTEM

A deeper network, like SRNet, has been mentioned in recent steganalysis literature as being superior for recognizing low tone embedding noise. As shown in Fig. 1, FractalNet [9], a deep model based on self-similarity, has lately grown in popularity. Through several variations of a core construction component, it achieves a balance of depth and width. A steganalytic detection method built on the FractalNet model-concept was applied using the embedded picture as input.

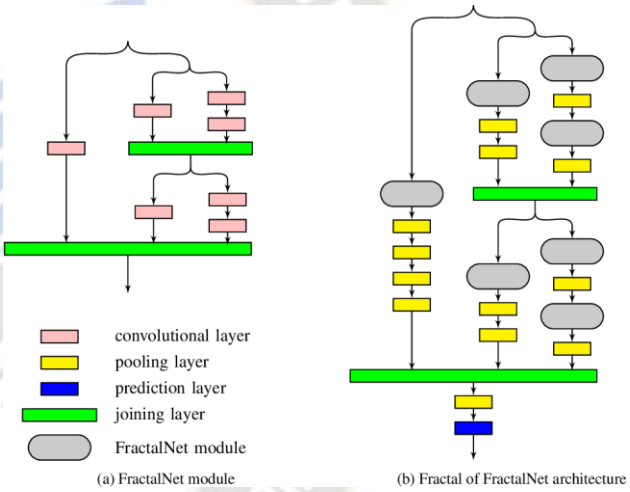

Figure.1. Existing System Architecture

In a real-world setting, it has been observed that expanding the network's breadth in a certain ratio to its depth improves steganalytic identification for test photos. A simple fractal block is repeated to create the proposed deep network, which allows for the maintenance of a balance between the network's depth and width. The proposed model outperformed the findings of the most recent studies, according to a thorough set of tests. A study on ablation is also given to support the performance of the suggested architecture. The advantages of this system are its ability to attain great levels of complexity and performance with low error rates.

With a modest payload, like 0.1 or 0.05 bpp, it takes longer for the images in this training model to converge. The model would occasionally fail to converge. Fractal networks can withstand being overly deep; while more depth may

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

reduce training, it has no negative effects on accuracy. Even with significant data augmentation, FractalNet still can't compete with other algorithms in terms of performance.

III. PROPOSED SYSTEM

Given that many IoT devices are publicly available to everyone on the network, it is essential to be aware of the security risks and hazards posed by cyberattacks and to take precautions to secure your IoT devices. Fig. 2 illustrates how data from multiple IOT networks, including user uploads, sensor data, server storage, and wireless data transfer, is stored in the cloud and secured using deep learning steganography and cryptographic encryption. Plain text is changed to encrypted text in cryptography before being delivered, and it is then converted back to plain text after receiving a response from the recipient. By incorporating sensitive information into a text, audio, or video file, steganography is a method for hiding it. Data can be concealed in bits that correspond to succeeding rows of pixels with the same color in a picture file.

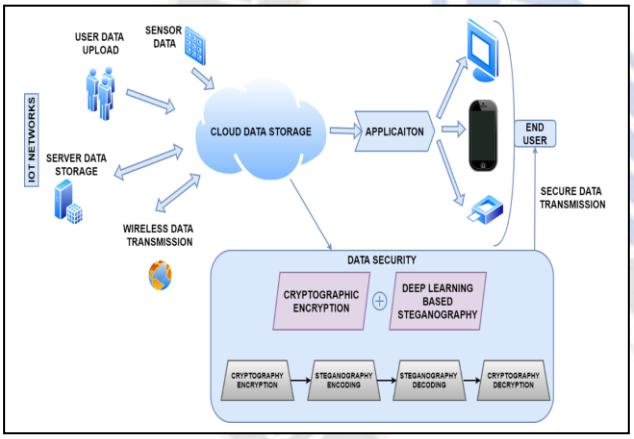

Figure.2. Proposed System Architecture

The outcome will be a picture file with the same visual appearance as the original but with "noise" patterns made up of common, unencrypted data. This is done by covertly combining the redundant data with the encrypted data. In this study, data from Internet of Things (IoT) networks is encrypted using cryptography, and the encrypted message is then hidden within an image file using steganography to enhance the number of bits that can be contained inside each image pixel. The payload that may be communicated through an image is considerably improved by combining convolutional neural networks with the traditional steganography technique. Convolutional networks are therefore created and trained in this study's suggested method in a way that enhances the amount of data that can be securely decrypted while also increasing the amount of data that can be securely encrypted.

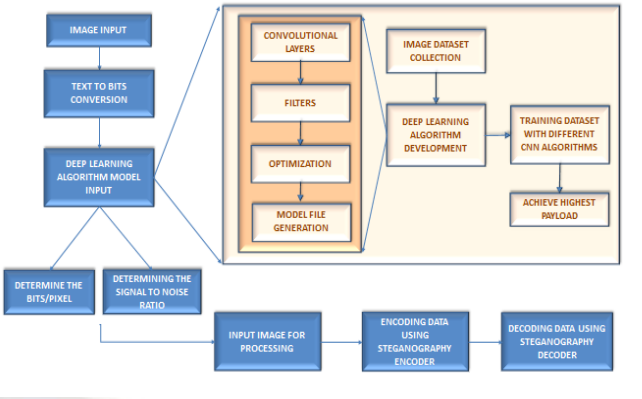

Figure.3 Flowchart for Implementing Proposed Security System In IOT

All these processes will take place one after the other and at last a model file will be generated. Image dataset collection is given as input to deep learning model where the dataset is trained with different CNN algorithms.Fig.3 Flowchart for Implementing Proposed Security System In IOT.Image is given as input after which text to bits conversion takes place so that the bits can be stored inside pixel of an image. This converted image is given as input to deep learning model, inside which there are convolution layers, filters, optimization and model file generation. achieve high payload. Finally, the secure data is sent to the end user. Fig. 4, shows the detailed process of steganography. The original text which is sent by the sender is called plaintext. This plaintext is encrypted into ciphertext at the sender side so that no other person accesses it. At the receiver side, the ciphertext is decrypted back to plaintext. So that the receiver receives the original message which is sent by the sender.

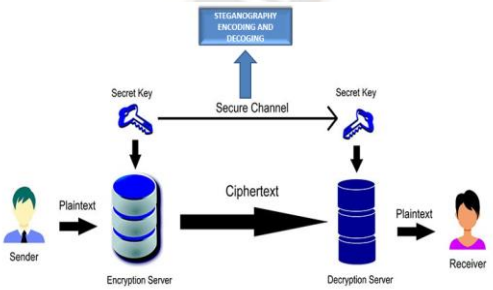

Figure.4 Steganography encoding and decoding

IV. RESULTS AND DISCUSSION

This section goes over the implementation and results of the proposed security system. To begin with, the work is divided into modules of implementation that are completed. The image is first read and converted into bits, which will be used to hide the data within the image. Then, when the data is fetched from the image, the bits are converted into text. After that, the almost 1000 image Div2k dataset was downloaded in order to train the deep learning algorithm. The training is done utilizing the fundamental deep learning algorithm

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

development after the dataset has been downloaded. Encoding, decoding, and image checking are the three stages of the algorithm, and the epochs are carried out during training, as shown in Fig. 5. As shown in Fig. 5, various metrics including accuracy, loss, SSIM, and PSNR are computed. As a result, the proposed convolutional networks technique in this study is created and trained in a way that improves the amount of data that can be encrypted while also allowing for a secure decryption of the original message.

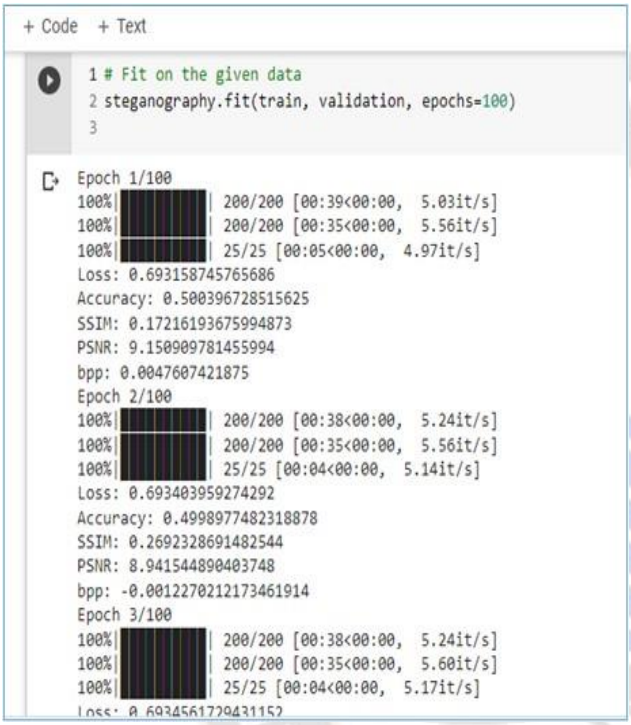

Figure.5 Deep Learning Algorithm Training

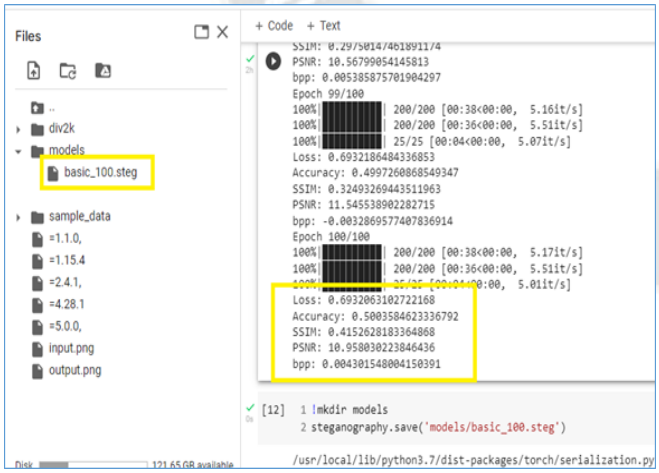

Figure.6 Model File Generation

As shown in Fig. 6, the model file is created after the training method, and metrics for the model are also calculated. The primary factor that is improved is the number of bits per pixel. The greatest bits per pixel that appear to have been reached with this basic algorithm development are only 0.004, which is far too low to be used in real time.

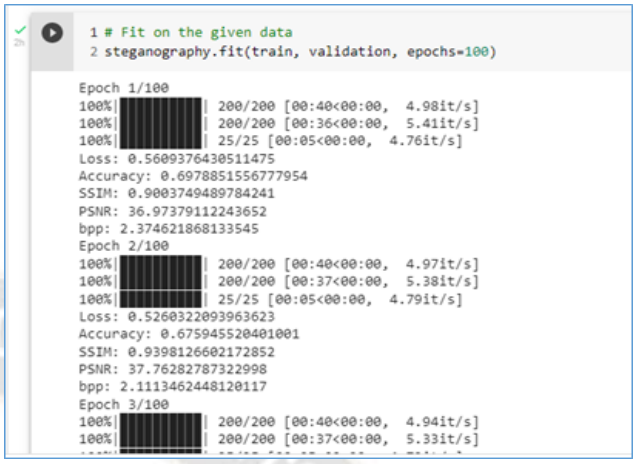

Figure.7 Enhanced Deep Learning Algorithm Training

The training process is then started for an enhanced algorithm model; the training commencement for this model is shown in Fig. 7. The model file, which enables the output for encoding and decoding to be validated, is prepared after training with the fundamental deep learning method is complete.

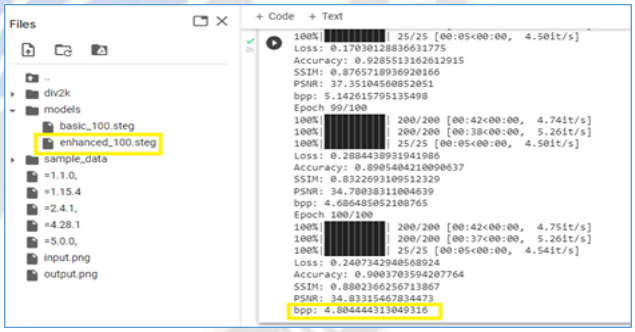

Figure.8. Model File Generation After Enhanced Algorithm Training

Following the training method, the model file shown in Fig. 8 is constructed, and the metrics are computed. According to the data, the objective of the study, which was to achieve more than three bits per pixel, was attained in real time at 4.8 bits per pixel. When the training is complete and the model files are ready, the model files are checked for data encoding and decoding to and from the image.

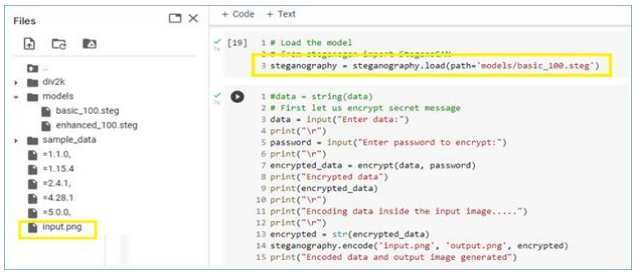

Figure.9 Loading Basic Model File for Encoding

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

The key is then concealed inside the image using steganography since the data must first be transformed into a cypher text using AES encryption, as seen below. The initial stage, which asks for importing the model file in which the data will be buried, also includes an input image. below Fig. 8. The output image is successfully generated when the data is transformed into a cypher text and concealed inside the input image, as seen in Figs. 9 and 10.

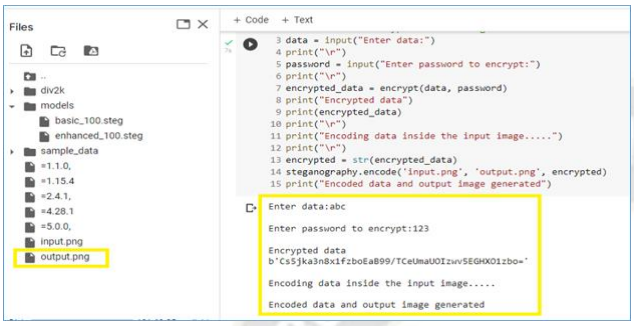

Figure.10 Encrypting and Encoding Data Using Basic Model

The created output image file, which is shown in Fig. 11 below, is now being decoded.

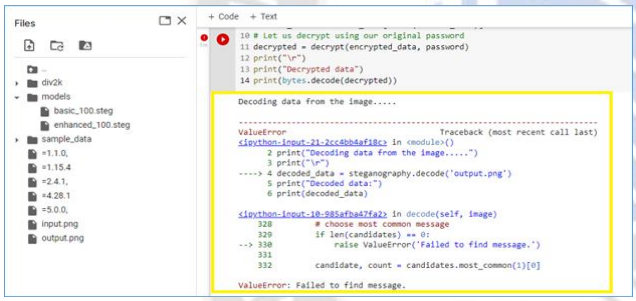

Figure.11 Decoding and Decrypting Data Using Basic Model

Because the bits per pixel were so little, data could not be correctly encoded, the image file raises an error when it is analyzed to find the data concealed therein, claiming that no data was found.

In order to perform data encoding, the upgraded model file has now been loaded, as seen in Fig. 12.

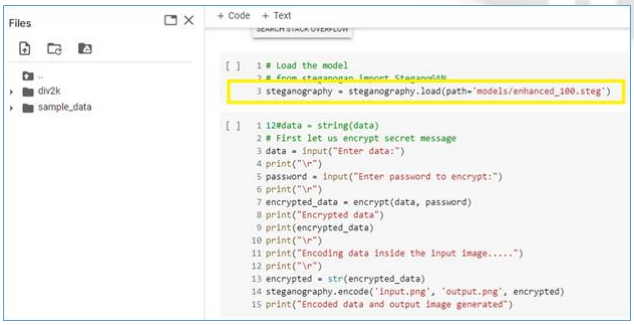

Figure.12 Loading Enhanced Model File for Encoding

The data is changed to cypher text when the encoding procedure gets under way, successfully creating an output image file as illustrated in Fig. 13.

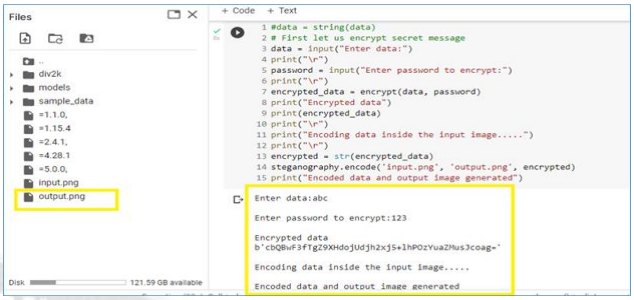

Figure.13 Encrypting and Encoding Data Using Enhanced Model

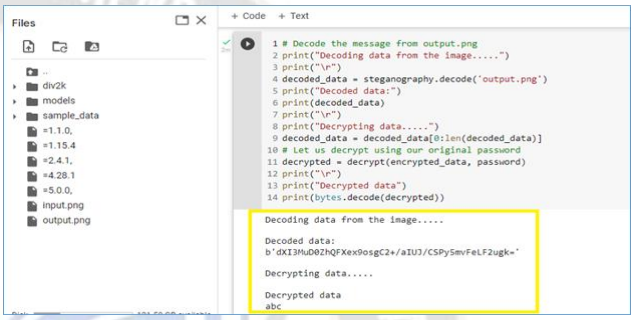

Figure.14 Decrypting and Decoding Data Using Enhanced Model

Decoding of data is then performed to get back the data hidden inside the output image file which can be seen in Fig.14.

TABLE1. COMPARISION OF EXISTING SYSTEM AND PROPOSED SYSTEM

Metrics	Existing System	Proposed System
Payload	0.004760	4.804443
Loss	0.693158	0.240734
Accuracy	0.500396	0.900370
PSNR	9.150900	34.83315
SSIM	0.172161	0.880236

The above Table 1 shows the comparison of metrics of existing and proposed system. Various metrics such as Payload, Loss, Accuracy, PSNR and SSIM are calculated for existing and proposed system. Each and every metrics is improved for the proposed system while comparing with existing system. Also, the loss is widely reduced in the proposed system.

Existing system has achieved the payload to the maximum extent of 0.5 bpp whereas in proposed system payload is achieved up to 4 bpp. From the above results we can see that the cipher text is been successfully decoded from the image and AES decryption is been performed to get back the data successfully. Even with significant data enhancement, FractalNet cannot outperform other algorithms in the current system. Fractal networks can withstand being

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7221
***Article Received**: 28 April 2023 **Revised:** 14 June 2023 **Accepted:** 26 June 2023*

too deep; while more depth may make training more difficult, accuracy is unaffected. To address this issue, this study constructs and trains the convolutional network technique in order to enhance the payload of the data to be encrypted while still reliably decrypting the initial message.

The suggested approach increases the payload that can be conveyed by an image by using deep learning, and the data is safely transmitted while being encoded and decoded in real time.

VI.CONCLUSION

Steganography is meant to complement cryptography, not to replace it. When a message is encrypted and hidden using a steganographic approach, the likelihood of the hidden message being discovered decreases and an extra level of protection is provided. This article proposes employing deep learning to enhance the number of bits that can be saved within an image pixel, cryptography to encrypt IoT network data and steganography to hide the encrypted message within an image file.

This is used to provide a technique that successfully secures and protects data.

Future research will use a variety of efficient methodologies and algorithms to increase prediction accuracy, and bit storage capacity can be increased to increase data payload.

REFERENCES

[1] S. Wu, S. -h. Zhong and Y. Liu, "A Novel Convolutional Neural Network for Image Steganalysis with Shared Normalization," in IEEE Transactions on Multimedia, vol. 22, no. 1, pp. 256-270, Jan. 2020, doi: 10.1109/TMM.2019.2920605.

[2] M. Hassaballah, M. A. Hameed, A. I. Awad and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7743-7751, Nov. 2021, doi: 10.1109/TII.2021.3053595.

[3] W. Su, J. Ni, X. Hu and J. Fridrich, "Image Steganography with Symmetric Embedding Using Gaussian Markov Random Field Model," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 3, pp. 1001-1015, March 2021, doi: 10.1109/TCSVT.2020.3001122.

[4] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi:10.1109/TSMC.2019.2903785.

[5] M. Boroumand, M. Chen and J. Fridrich, "Deep Residual Network for Steganalysis of Digital Images," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1181-1193, May 2019, doi: 10.1109/TIFS.2018.2871749. [6] W. Wang, P. Xu, D. Liu, L.

[6] T. Yang and Z. Yan, "Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4221-4230, June 2020, doi: 10.1109/TII.2019.2950295.

[7] W. Tang, B. Li, S. Tan, M. Barni and J. Huang, "CNN-Based Adversarial Embedding for Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2074-2087, Aug. 2019, doi: 10.1109/TIFS.2019.2891237.

[8] X. Liao, J. Yin, M. Chen and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 897-911, 1 March-April 2022, doi: 10.1109/TDSC.2020.3004708.

[9] B. Singh, A. Sur and P. Mitra, "Steganalysis of Digital Images Using Deep Fractal Network," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 599-606, June 2021, doi: 10.1109/TCSS.2021.3052520.