e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 2, April 2023



9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

# End to End Encryption to Enhance Security in IoT Networks Using Steganography and Deep Learning Algorithm

**Dr. P. Pritto Paul[1], SJason[2], K Sundar[2], R Tamilarasu[2]**

Associate Professor, Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, India[1]

UG Students, Department of CSE,Velammal Engineering College, Chennai, Tamil Nadu , India[2]

**ABSTRACT:**Internet of Things (IoT) defines a network of objects or objects embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems via the internet. Although several IoT devices are accessible to all on the network, it is very important to be aware of security threats and threats online attacks; Accordingly, it must be protected. In cryptography, blank text is converted into encrypted text before being sent, and it is converted into the blank text after communication on the other side. Steganography is a method of encrypting private data, by embedding it in an audio, video, image, or text file. Another method is to hide data in bits representing the same color pixels that are repeated sequentially in an image file. By using encrypted data on this obsolete data in a vague way, the result will be an image file that looks similar to the original image but has "sound" patterns of normal, unencrypted data. This paper proposes to encrypt IoT network data in the form of cryptography and encrypt the encrypted message within the image file using the steganography method and increase the number of bits that can be saved within the pixel image. It will incorporate the use of convolutional neural networks in the context of conventional steganography to significantly increase image transfer payloads. Hence, in this paper, a convolutional network algorithm will be developed and trained in a way to increase the amount of data encryption and securely deleted it to view the actual message.

**KEYWORDS:** Internet of things, Cryptography, Encryption, Decryption, Steganography, CNN.

## I. INTRODUCTION

Internet of Things (IoT) is the concept of connecting any device (as long as it has a turn on / off) to the internet and other connected devices. IoT is a huge network of connected people - all of whom collect and share data about how they are used and the environment around them. IoT devices contain sensors and small computer processors that run data collected by sensors for machine learning. IoT devices share the sensory data they collect by connecting to an IoT gateway or other peripheral device where data is sent to the cloud for analysis or localization. In some cases, these devices interact with other related devices and generate the information they derive from others. [1] Devices do a lot of work without human intervention, although people may not be able to interact with devices - for example, set them up, give them instructions, or access data.

The Internet of Things helps people to live and work smarter, and gain more control over their lives. In addition to providing smart devices to make automated homes, IoT is important for business. IoT provides businesses with real-time monitoring of how their systems work, bringing details to everything from machine operations to chain and equipment operations. IoT empowers companies to create their processes and reduce labor costs. It also reduces waste and improves service delivery, makes it less expensive to produce and deliver goods, as well transparency in customer sales. Thus, IoT is one of the most important technologies of everyday life and will continue to take momentum as many businesses see the power of connected devices to keep them competitive. IoT devices are small computers, connected to the Internet, and are at risk of malware and hacking.

This paper proposes a system to protect the army data stored on the network within the image file using the Steganography method and to increase the number of bits that can be stored within the image pixel. The use of convolutional neural networks in the form of conventional steganography greatly enhances image transfer payloads. Thus, the first step in the paper will be to collect the DIV2K database and will be separating these databases into training and the test database where the test data will be kept separate and the training database will be used for model training. [2] For training, a set of data, coding, recording, and criticism modules are used. For training, an algorithm of

20 to 100 epochs is used. The Encoder module takes a cover image and data tensor and merges them into a steganographic image. The critic module takes a picture and predicts whether a cover image or a steganographic image (N, 1).

The Decoder Module takes a steganographic image and attempts to record the embedded data tensor. Then calculated metric values such as payload, bits per pixel, and accuracy will be used to predict model accuracy. After that, the algorithm is upgraded to increase the payload or retention of the message inside the image. The typical storage capacity is 0.5 bits per pixel. By adjusting the existing algorithm in such a way that it raises the bpp to more than 2 to 3 bpp, it will be trained and compared to the existing system using metrics. After performing cryptography, using the AES data algorithm is encrypted and the hash key is created. This hash key is encoded within the image using steganography and encrypts the message in the image, the original image and the encoded image will look the same. Whenever data needs to be removed encryption hash is extracted from images using steganography and cryptography extraction is used to retrieve the actual data. Also, secure encryption will be cleared using AES to view the actual message.

### 1.1 DEEP LEARNING

Deep Learning is a study of computer software that mimics a network of neurons in the brain. It is a subset of machine learning and is called deep learning because it uses deep neural networks.In-depth learning algorithms are built on connected layers.

• The first layer is called the Installation Layer

• The final layer is called the Output Layer

• All layers in the middle are called Hidden Layers.

The term deep means that a network comprises neurons of more than two layers.Each Hidden layer is made up of neurons. Connected neurons. The neuron will process and transmit the input signal it receives to the surface above it.[3] The signal strength given to the neuron in the next layer depends on weight, bias, and activation function.The network consumes a large amount of input data and operates in multiple layers; the network can read the most complex data features in each layer.

In-depth learning is a powerful tool for making predictions and possible outcomes. Intensive reading thrives on pattern acquisition (unsupervised reading) and cognitive-based guesses. Big data is fuel for deep learning. When both are combined, an organization can achieve unprecedented results in terms of manufacturing, marketing, management, and innovation.

Deep learning can go the extra mile. For example, in-depth reading algorithms are 41% more accurate than machine-readable algorithms for image classification, 27% more accurate in facial recognition, and 25% more in voice recognition.

## II. RELATED WORKS

### A. *Secure Halftone Image Steganography Based on Feature Space and Layer*[4]

Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni, and Jiwu Huang suggested that Syndrome-trellis (STCs) codes are commonly used in steganographic programs, which aim to reduce embedded distortions, but many distortion models cannot capture image interaction. embedding modification (MIEMs). In this article, a secure halftone image steganographic system based on feature space and layer embedding is suggested. First, the feature area was created by a character description system designed based on 4 × 4-pixel block figures in halftone images. In addition to the feature space, it is proposed to analyze a standard step with good differentiation capability, which is used to measure embedded distortion. As a result, a distortion-based hybrid feature-based model is developed, surpassing other high-end models. Then, as the deviation model is established in local regional statistics, a layer embedding strategy is proposed to reduce MIEM. It divides the host image into multiple layers according to the corresponding positions in the 4 × 4 blocks, and the embedding process is done layer by layer. In each layer, any two pixels are found in different 4 × 4 blocks in the first image, and the distortion model ensures that the calculation of the pixel distortion is independent. Between layers, the pixel distortion of the current layer is updated according to previous versions of embedding, thus reducing the distortion of the full embedding. Comparisons with previous systems show that the proposed steganographic system gains higher statistical protection when resisting modern steganalysis analysis. The key answer is that embedding secret messages directly on the cover image triggers MIEM and reduces invisible performance.

### B. *Image Steganography with Symmetric Embedding using Gaussian Markov Random Field Model*[7]

WenkangSu, Jiangqun Ni, Xianglei Hu, and Jessica Fridrich have worked on the latest developments in dynamic steganography to demonstrate how steganographic image communication performance can be enhanced by combining non-additional photographic models that rely on close pixels. In this paper, a Gaussian Markov Random Field (GMRF) model with four-dimensional cross-sections is proposed to show an interaction between local photographic cover elements, and the problem of secure steganography imagery is being used as one of reducing KL-fragmentation by a series of low-profile structures associated with GMRF by taking advantage of GMRF's conditional independence. The proposed GMRF adoption uses tessellates cover images into two small non-integrated images, and a flexible development scheme is developed to effectively embed a given payload burden while minimizing the total KL separation between cover and stego, i.e., statistical recognition. Test results show that the proposed GMRF transcends previous models of model-based schemes, e.g., MiPOD, and high-level HiLL competitors for active steganography, where the selected channel information is not available for analysis. The main result is that the adaptive image steganography method is based on a small distortion embedding framework, which includes additional embedding costs for each cover element and coding method, usually syndrome-trellis codes (STCs).

### C. *Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features*[11]

Zinan Lin, Yongfeng Huang, and Jilong Wang say that, with the advent of cloud technology, cloud computing is an emerging technology for storing large digital images, giving steganography a new fashion to embed private information on large images. Specifically, a smart steganographer may embed a set of confidential information on multiple images in a variable, and share these images in a cloud storage with the recipient, instead of steganography for a single standard image. However, it is still an open issue on how to assign embedded load between consecutive images to improve security performance. This paper creates a flexible paid load distribution on multiple steganography images based on image texture features and provides a true security analysis from the steganalyst point of view. Two payload distribution strategies based on image complexity and distortion distribution are designed and discussed sequentially. Proposed techniques can be used in conjunction with these state-of-the-art single-image steganographic algorithms. A comparison of safety performance compared to modern integrated global steganalysis is provided. In addition, this paper compares the availability of each image of these many steganographic systems against a single image analyzer. Extensive test results show that proposed payload distribution strategies can achieve better safety performance. The main result is that compared to Embedding Strategy Based on Distortion Distribution (ES-DD) and IMS, ES-ITC security performance is slightly lower, especially at higher pay rates.

### D. *RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network*[13]

Wei Lu, Junjia Chen, Junhong Zhang, Jiwu Huang, Jian Weng, and Yicong Zhou claim that quantization index modulation (QIM) steganography makes it possible to hide confidential information in VoIP streams, which can be used by unauthorized organizations to set up private channels. with evil intent. Obtaining short samples of QIM steganography, as required by real circumstances, remains an unresolved challenge. This paper proposes an effective online steganalysis method to obtain QIM steganography. We find four strong coding patterns in VoIP streaming, which will be distorted after embedding with hidden data. To eliminate those linking factors, we propose the Codeword Correlation Model (CCM), based on a continuous neural network (RNN). In addition, we propose the Feature Classification Model (FCM) to divide those associated elements into coverage sections and stego speech sections. The entire RNN Based Steganalysis Model (RNN-SM) is trained in a supervised learning framework. Studies show that in full embedded samples, RNN-SM has a high detection accuracy, which remains more than 90% even though the sample is as short as 0.1s and much higher than other modern methods. With the challenging task of performing steganalysis on low embedded rate samples, RNN-SM also gains high accuracy. The average test time for each sample is less than 0.15% of the sample length. These indicators indicate that RNN-SM meets the requirement of short sample acquisition and is a modern Internet VoIP steganalysis algorithm. The main drawback is that it is very difficult to train RNNs in a very long sequence, especially when using ReLU or tanh activations.

From the above reference papers, we can conclude that the following are major problems:
• In an existing system, with heavy data additions, FractalNet still cannot have a much better result compared to other algorithms.
• Fractal networks with greater depth; additional depth may delay training, but does not interfere with accuracy.
• One of the biggest challenges in training any steganalysis model is the time it takes to convert low-resolution images, such as 0.1 or 0.05 bpp. Sometimes, the model completely failed to meet.
• Embedding secret messages directly on the cover image triggers MIEM and reduces invisible performance.

## III. PROPOSED MODEL

Internet of Things (IoT) defines a network of objects or objects embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems via the Internet. Although several IoT devices are accessible to all on the network, it is very important to be aware of security threats and threats online attacks; therefore, it must be protected. In cryptography, blank text is converted into encrypted text before being sent, and it is converted into the blank text after communication on the other side. Steganography is a method of encrypting private data, by embedding it in an audio, video, image, or text file. Another method is to hide data in bits representing the same color pixels that are repeated sequentially in an image file. By using encrypted data on this obsolete data in an obscure way, [5] the result will be an image file that looks similar to the original image but has "sound" patterns of normal, unencrypted data. In this paper, we will encrypt the data of IoT networks in the form of cryptography and hide the encrypted message inside the image file in the form of Steganography and increase the number of bits that can be saved within the pixel image. We will incorporate the use of convolutional neural networks in the context of conventional steganography to significantly increase image transfer payloads. Therefore, in this paper, an algorithm for convolutional networks will be developed and trained in a way to increase the amount of data encrypted and securely removed to view the actual message.

### *A. IMAGE READING AND WRITING*

Literacy is fundamental to image processing and computer-assisted visualization. Even if you crop, resize, rotate, or use different filters to process images, the images need to be read first.[6] OpenCV-Python is an integrated Python library designed to solve computer vision problems. cv2.imread () method uploads an image from the specified file. If the image cannot be read (due to a missing file, invalid permissions, unsupported or invalid format) then this method returns an empty matrix. OpenCV library boundaries,
• Method: A character unit representing the image path to be read
• Flag: Specifies how the image should be read. Its default value is cv2.IMREAD_COLOR
OpenCV, the world's largest computer library, has three built-in functions,
1. imread() helps us to read the picture
2. The display() shows the image in the window
3. imwrite() writes an image in the file directory

Images are usually in PNG or JPEG format and can be uploaded directly using the imread() function in the image class. This returns an image object that contains pixel image data and details about the image. The machines store the images in the form of a matrix of numbers. The size of this matrix depends on the number of pixels a given image contains. These numbers, or pixel values, denote the intensity or brightness of a pixel. Small numbers (near zero) represent black, and large numbers (near 255) mean white. The color image is usually composed of multiple colors and almost all colors can be generated in three main colors - red, green, and blue.[8] Thus, in the case of a color image, there are three Matrices (or channels) - Red, Green, and Blue. Each matrix has values between 0-255 that represent the color intensity of that pixel.

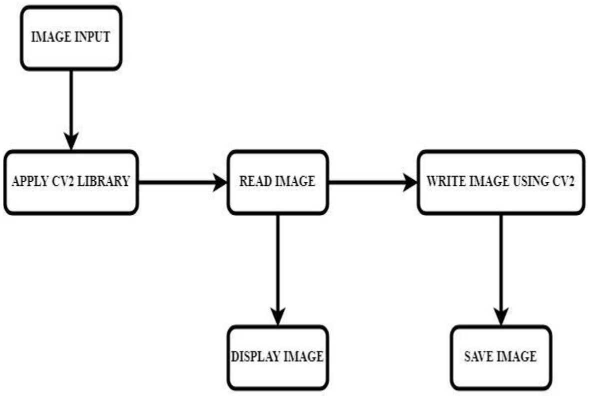


*Figure 1. Image Reading and Writing*

### B. *TEXT TO BITS CONVERSION*

The text cannot fit directly into the deep reading models. Text data should be encoded as numbers to be used as inputs or outputs for in-depth reading models. On computers, all data of different types is transmitted as 1s and 0s. However, some communication channels and applications may not understand all the pieces they receive. This is because the definition of sequence 1 and 0 depends on the type of data it represents. For example, 10110001 should be processed differently if it represents a character or image. Keras's in-depth reading library provides basic tools to help organize text data. It is popular to represent a document as a whole value sequence, where each word in the document is represented as a unique whole number.[9]

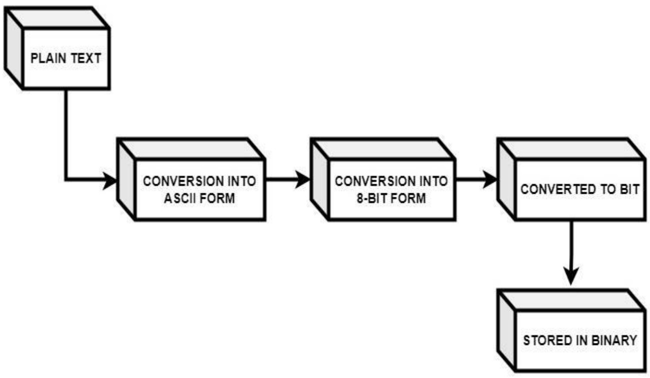


*Figure 2. Text to Bit Conversion*

Keras provides a one_hot() function that we can use to create token and text document integration steps in one step. The name suggests that it will create hot code and document code, which it does not. Instead, the function is a function of the hashing_trick() function described in the next section. The function returns the version with the complete document code. The use of the hash function means that there may be a conflict and not all words will be assigned whole numbers.

### C. *DEEP LEARNING ALGORITHM*

Advanced Learning is a sub-field of machine learning related to algorithms that stimulate brain formation and function called artificial neural networks. In addition to scalability, another commonly cited advantage of in-depth learning models is their ability to create an automatic extraction feature in raw data, also called the learning feature. Writing an in-depth learning algorithm from the beginning is a very rewarding learning experience.[12] Some algorithms are more complex than others, so start with something simple algorithm development. The next 6-step process is to write algorithms from scratch,

1. Get a basic understanding of the algorithm

2. Find different sources of information

3. Divide the algorithm into pieces

4. Start with a simple example

5. Ensure reliable use

6. Write the process

FractalNet is a type of convolutional neural network that roams the residual connection instead of the "fractal" design. It involves the repeated use of a simple extension system to produce deep networks with its precision-cut fractals. These networks contain sub-interactive modes of varying lengths, but do not include any intermediate or residual connections; every internal signal is converted by filter and incompatibility before the following layers are detected. Fractal networks are similar to the excellent performance of residual networks typically in both the CIFAR and ImageNet split operations, thus indicating that residual presentations may not be the basis for the success of deep-convincing emotional networks.[14] Instead, the key may be the ability to change, during training, from depth to effectiveness. FractalNet networks provide strong evidence that trajectory is important in training deep emotional networks.

Then the FractalNet algorithm is configured in such a way that the layers (convolutional, batch normalization, etc.,) are adjusted to achieve a higher payout than 3bpp. We have therefore achieved very high payouts using steganography and an in-depth learning algorithm.

### *D. METRICS CALCULATIONS*

Comparing stego photo with cover photo effects requires a high-quality image quality, which is widely used,

- Payload
- Loss
- Accuracy
- Peak Signal to Noise Ratio (PSNR)
- Structure similarity index (SSIM)

*1.Payload*

Payload capacity is a large message size that can be embedded in the cover image, usually; the payload capacity is measured using bits per pixel (bpp). But the amount of that message pinned to the cover image will affect the level of change over the pixel image value. The change in the pixel value of the cover image affects the quality of the produced image of stego, where changes in the number of fine pixels should not be detected by the human senses, this is what the invisible means. Visibility quality can be measured using a high-to-high signal (PSNR) signal where the PSNR value is generated from the value of the square measurement error (MSE) generated in the figure between the real cover image and the stego image. You need to emphasize that the size of the pinned message will greatly affect the invisibility, logically if the larger the size of the pinned message, then the quality of the invisibility will decrease.

*2. Accuracy*

Accuracy is defined as the percentage of accurate prediction of test data. It can be easily calculated by dividing the number of correct predictions by the number of complete predictions. The accuracy of the in-depth learning model is a measure used to determine which model is best for identifying relationships and patterns between data variables based on inputs, or training, data. A better model can get used to ‘unseen’ data, better predictions, and data I can generate, which brings in more business value. The cost of errors can be huge, but improving the model reduces those costs. There is, of course, a point of declining return on which the value of developing a more accurate model will not result in concurrent growth, but it is generally beneficial across the board. False cancer diagnoses, for example, call a hospital and a patient. The benefits of improving model accuracy help to avoid the unnecessary time, money, and stress.

*3. Peak Signal to Noise Ratio (PSNR)*

The term peak signal-to-noise ratio (PSNR) is a reflection of the ratio between the maximum possible signal (power) of a signal and the distortion of sound that affects the quality of its representation. Because most signals have a very wide variable range, (the ratio between the largest and smallest possible values of a variable value) the PSNR is usually expressed in terms of a logarithmic decibel. Image enhancement or enhancement of digital image viewing quality can be a straightforward matter. Whether one method provides a better-quality image may vary from person to person. For this reason, it is necessary to establish quantitative/dynamic measurements to compare the results of image enhancement algorithms in image quality.

Using the same set of test images, different image enhancement algorithms can be systematically compared to determine if a particular algorithm produces better results. The probe metric is the peak-signal-to-noise ratio. It will show that the algorithm or set of algorithms can improve the downloaded image to be more similar to the real one, and then can more accurately conclude that it is the best algorithm. The suggestion is that the higher the PSNR, the better the reduced image is rebuilt to match the real image and improve the reconstruction algorithm. This will happen because they prefer to reduce the MSE between images by respecting the higher signal value of the image.

*4. Structural Similarity Index (SSIM)*

The Structural Similarity Index (SSIM) is a visual metaphor that measures image quality degradation resulting from processing such as data congestion or loss of data transfer. It is a full reference metric that requires two images from the same image to capture the reference image and the processed image. The processed image is often compressed.[15] For example, it can be obtained by saving a reference image such as JPEG (at any quality level) and re-reading it. SSIM is well-known in the video industry, but it has robust still photography applications. Unlike the PSNR (Peak Signal-to-Noise Ratio), SSIM is based on the physical properties of the image. Although PSNR can no longer be considered a reliable indicator of image quality degradation it is available as an alternative to the Imatest SSIM module.

## *E. ANALYSIS*

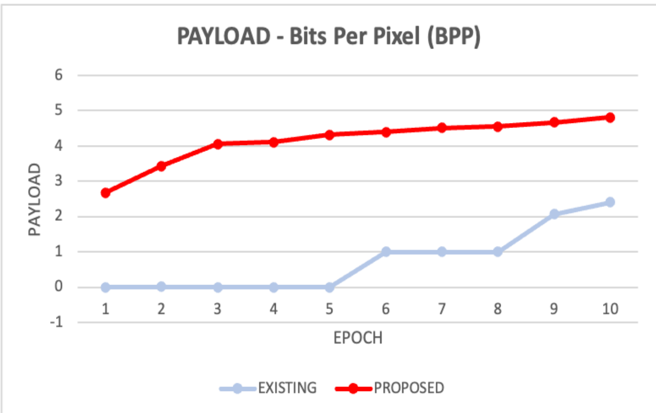


*Figure 5. Payload Capacity Graph.*

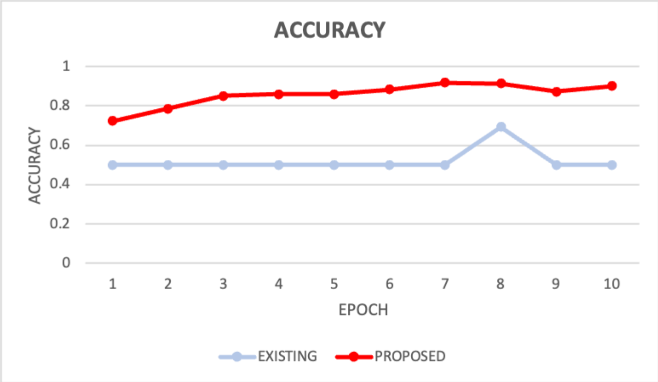


*Figure 6. Accuracy Graph.*


*Figure 7.Loss Graph.*

## IV.CONCLUSION

The steganographic method provides an additional layer of protection and reduces the chance of the hidden message being detected. This paper proposed that encrypting the IoT network data by Cryptography method and hiding the encrypted message inside an image file using the Steganography method as well increases the number of bits that can be saved within a pixel of an image using the currently prevailing deep learning approach. Using an algorithm was developed effectively to protect and secure the data.

## REFERENCES

[1] Songtao Wu, Sheng-Hua Zhong, Yan Liu, *A Novel Convolutional Neural Network for Image Steganalysis with Shared Normalization*,[2020, Vol.22, Issue: 1].

[2] M. Hassaballah, Mohamed Abdel Hameed, Ali Ismail Awad, Khan Muhammad, *A Novel Image Steganography Method for Industrial Internet of Things Security,* [2021, Vol. 17, Issue: 11].

[3] Xin Liao, Jiaojiao Yin, Mingliang Chen, Zheng Qin, *Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features* [2020]

[4] Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni, Jiwu Huang, *Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis* [2019, Vol.14, Issue:8].

[5] Mehdi Boroumand, Student Member, IEEE, Mo Chen, Member, IEEE, and Jessica Fridrich, Fellow, IEEE,*RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network*[2019, Vol.14, Issue: 5].

[6] Ru Zhang, Feng Zhu, Jianyi Liu, Gongshen Liu, *Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis* [2020, Vol.15].

[7] WenkangSu, Jiangqun Ni, Xianglei Hu, Jessica Fridrich, *Image Steganography with Symmetric Embedding using Gaussian Markov Random Field Model* [2021, Vol.31, Issue: 3].

[8] Wei Wang, Member, IEEE, Peng Xu, Member, IEEE, Dongli Liu, Laurence Tianruo Yang, Senior Member, IEEE and Zheng Yan, Senior Member, IEEE, *Light-weighted Secure Searching over Public-key Ciphertexts for Edge-Cloud Assisted Industrial IoT Devices* [2019, Vol. 16, Issue: 6] .

[9] Pietro Tedeschi, Savio Sciancalepore, AreejEliyan, Roberto Di Pietro, *LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications* [2020, Vol. 7, Issue: 1].

[10] Arijit Karati, SK Hafizul Islam, Marimuthu Karuppiah, *Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments* [2018, Vol. 14, Issue:8].

[11] Zinan Lin, Yongfeng Huang, Jilong Wang, *RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network*[2018, Vol. 13, Issue: 7].

[12] Yumei Li, Futai Zhang, Xin Liu, *Secure Data Delivery with Identity-based Linearly Homomorphic Network Coding Signature Scheme in IoT* [2020].

[13] Wei Lu, Junjia Chen, Junhong Zhang, Jiwu Huang, Jian Weng, Yicong Zhou, *Secure Data Delivery with Identity-based Linearly Homomorphic Network Coding Signature Scheme in IoT* [2020].

[14] Manju Khari, Aditya Kumar Garg, Amir H. Gandomi, Rashmi Gupta, Rizwan Patan, Balamurugan Balusamy, *Securing Data in Internet of Things (IoT) Using Cryptography and Steganography* [2020, Vol. 50, Issue: 1].

[15] Brijesh Singh, Arijit Sur, Pinaki Mit, *A Novel Image Steganography Method for Industrial Internet of Things Security* [2021, Vol. 8, Issue: 3].