IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STEGANALYSIS OF DIGITAL IMAGES USING DEEP FRACTAL NETWORK

Mr. Dharma Prakash[1], D. Chanikya Reddy [2], P. Sevith Reddy[3,] M B. Akhil Kumar[4]

Department of Computer Science and Engineering

PERI INSTITUTE OF TECHNOLOGY

Abstract

In Cryptography, plain text is converted to encrypted text before it is sent, and it is converted to plain text after communication on the other side. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data. In this project it proposes to encrypt the IoT networks data by Cryptography method and hide the encrypted message inside an image file using Steganography method as well increases the number of bits that can be saved within a pixel of an image. We are going to incorporate the usage of Convolutional neural networks in traditional steganography method to drastically increase the payload that can be transmitted through an image. Thus, in this project the Convolutional networks algorithm will be developed and trained in such a way to increase the payload of the data to be encrypted as well as safely decrypted to view the original message.

Keyword: Steganography, Cloud storage, Fractal Net.

INTRODUCTION

In Cryptography, plain text is converted to encrypted text before it is sent, and it is converted to plain text after communication on the other side. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data. In this project it proposes to encrypt the IoT networks data by Cryptography method and hide the encrypted message inside an image file using Steganography method as well increases the number of bits that can be saved within a pixel of an image. We are going to incorporate the usage of convolutional neural networks in traditional steganography method to drastically increase the payload that can be transmitted through an image. Thus, in this project the convolutional networks algorithm will be developed and trained in such a way to increase the payload of the data to be encrypted as well as safely decrypted to view the original message.

LITERATURE SURVEY

Steganalysis of Digital Images Using Deep Fractal Network

In the recent literature on steganalysis, it has been observed that a deeper network is, in general, preferred for detecting low tone embedding noise, e.g., SRNet. However, very recently, a deep model, called FractalNet, became popular, which is based on self-similarity and grows deeper and wider by maintaining a balance between depth and width using a recurrent adaptation of a fundamental building block [1]. In this work, the concept of the FractalNet model has been exploited for steganalytic detection, where the embedded image has been used as input. In a practical scenario, it has been observed that steganalytic detection for test images is increasing if the width of the network can be increased with a certain proportion to the depth.

A Novel Image Steganography Method for Industrial Internet of Things Security

The rapid development of the Industrial Internet of Things (IIoT) and artificial intelligence (AI) brings new security threats by exposing secret and private data [2]. Thus, information security has become a major concern in the communication environment of IIoT and AI, where security and privacy must be ensured for the messages between a sender and the intended recipient. To this end, we propose a method called HHOIWT for covert communication and secure data in the IIoT environment based on digital image steganography.. Thus, utilizing this approach can keep unauthorized individuals away from the transmitted information and solve some security challenges in the IIoT.

Securing Data in Internet of Things (IoT) Using Cryptography and Steganography

Internet of Things (IoT) is a domain wherein which the transfer of data is taking place every single second **[3]**. The security of these data is a challenging task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are crucial when dealing with user authentication and data privacy.

Secure Halftone Image Steganography Based on Feature Space and Layer

Syndrome-trellis codes (STCs) are commonly used in image steganographic schemes, which aim at minimizing the embedding distortion, but most distortion models cannot capture the mutual interaction of embedding modifications (MIEMs) **[4]**. In this article, a secure halftone image steganographic scheme based on a feature space and layer embedding is proposed. First, a feature space is constructed by a characterization method that is designed based on the statistics of 4 × 4 pixel blocks in halftone images.

Secure Data Delivery with Identity-based Linearly Homomorphic Network Coding Signature Scheme in IoT

With the appearance and flourishing development of the Internet of Things (IoT), wireless sensor networks technology has been attracting increasing attention. Network coding is an indispensable technology in the wireless sensor networks, which can improve network transmission throughput **[5]**. However, a pollution attack is a serious security problem that must be faced in the process of data coding. Although the homomorphic network coding signature schemes can solve this troublesome, the high signature generation and verification cost of these schemes will reduce the transmission efficiency. In this paper, we propose an efficient identity-based linearly homomorphic network coding signature scheme for wireless sensor networks to guarantee data integrity and authenticity. In our scheme, the computation cost of signature generation and verification are both independent of the size of the data packet.

SYSTEM DESIGN

ARCHITECTURE DIAGRAM

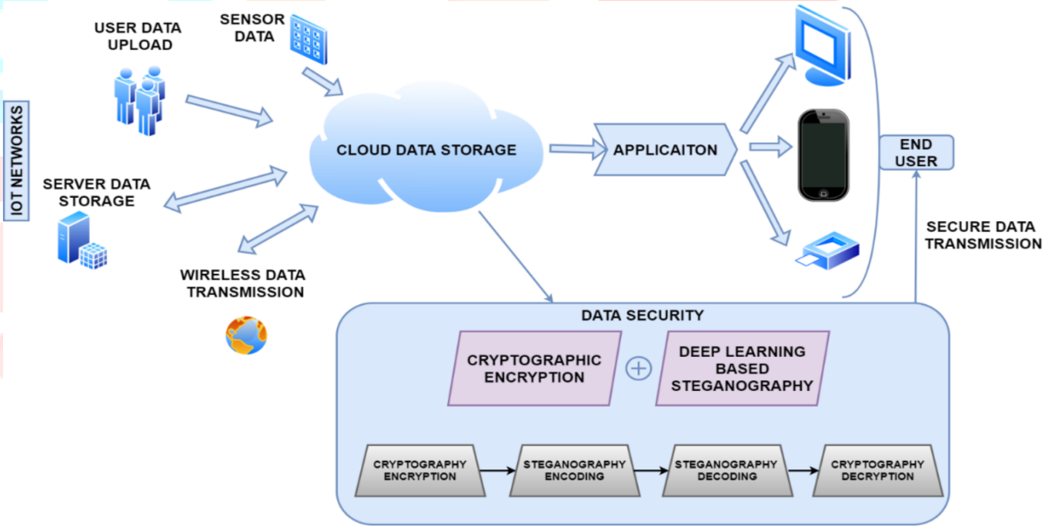

Fig 1: system architecture

WORKING

In this project, it proposes system to secure army data stored in network inside an image file using Steganography method as well increases the number of bits that can be saved within a pixel of an image.The usage of convolutional neural networks in traditional steganography method to drastically increase the payload that can be transmitted through an image. So, the first step in the project will be collecting the DIV2K dataset and then will be separating these datasets into training as well as testing dataset where the testing dataset will be kept separate and the training dataset will be used to train the model. For training the dataset, encoding, decoding and critic modules are used. For training the algorithm 20 to 100 epochs are used.

The Encoder module takes a cover image and a data tensor and combines them into a steganographic image. The Critic module takes an image and predicts whether it is a cover image or a steganographic image (N, 1).

The Decoder module takes a steganographic image and attempts to decode the embedded data tensor. Then calculating the metric values such as payload, bits per pixel and accuracy, will be used to predict the accuracy of the model. After that, algorithm is enhanced to increase the payload or storage capacity of the message inside the image. The normal storage capacity is 0.5 bits per pixel. By modifying the existing algorithm in a such way to increase the bpp to more than 2 to 3 bpp, it will be trained and compared to the existing system using the metrics. After performing cryptography, using AES algorithm the data has been encrypted and the hash key has been generated. This hash key has been encoded inside an image using steganography and encoding the message in the image, the original image and the encoded image will look the same. Whenever the data needs to be decrypted the hash is been decoded from the image using steganography decryption and cryptography decryption is applied to get the actual data. Also, it will be safely decrypted using AES to view the original message.

SYSTEM IMPLEMENTATION

The system has been implemented in different modules. The features of this system are split up into various modules. The modules are explained below:

MODULES DESCRIPTION

1. Image Reading and Writing
2. Text to Bits Conversion
3. Deep Learning Algorithm
4. Metrics Calculation
5. AES Cryptography Encryption
6. AES Cryptography Decryption
7. Encoding and Decoding of Image using Steganography.

PERFORMANCE ANALYSIS

METRICS CALCULATIONS

For comparing stego image with cover image results requires a measure of image quality, commonly used,

- Payload
- Loss
- Accuracy
- Peak Signal to Noise Ratio (PSNR)

- Structural Similarity Index (SSIM)

Payload

Payload capacity is the maximum size of a message that can be embedded in a cover image, usually; the payload capacity is measured using bits per pixel (bpp). But the amount of capacity that message pinned on the cover image will have an impact on changes level in the value of the cover image pixel.

Loss

Neural networks or neurons work with corresponding weight, bias and their respective activation functions. The weights get multiplied with the inputs and then activation function is applied to the element before going to the next layer.

Accuracy

Accuracy is defined as the percentage of correct predictions for the test data. It can be calculated easily by dividing the number of correct predictions by the number of total predictions.

Peak Signal to Noise Ratio (PSNR)

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

Structural Similarity Index (SSIM)

The Structural Similarity Index (SSIM) is a perceptual metric that quantifies image quality degradation caused by processing such as data compression or by losses in data transmission. It is a full reference metric that requires two images from the same image capture a reference image and a processed image.

CONCLUSION

Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. This project proposed that encrypt the IoT networks data by Cryptography method and hide the encrypted message inside an image file using 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 which we have developed an algorithm effectively protect and secure the data.

- In the existing system, with heavy data augmentation, FractalNet still cannot have the best result when comparing with those with other algorithms.
- Fractal networks are resistant to being too deep; extra depth may slow training, but does not impair accuracy.
- One of the biggest challenges in training any steganalytic model is the time that it takes to converge for the images with a low payload, such as 0.1 or 0.05 bpp. Sometimes, the model failed to converge at all.
- Embedding secret messages directly in the cover image causes MIEM and decreases undetectability performance.

REFERENCE

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

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

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

[4] CNN-based Adversarial Embedding for Image Steganography [2019, Vol.14, Issue:8] Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni, Jiwu Huang

[5] Deep Residual Network for Steganalysis of Digital Images [2019, Vol.14, Issue: 5] Mehdi Boroumand, Student Member, IEEE, Mo Chen, Member, IEEE, and Jessica Fridrich, Fellow, IEEE

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

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

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

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

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