Application of Machine Learning for Data Security

Priyanka M Ninganure[1]

[1]Student, ECE Dept of Gogte Institute of Technology, Belagavi.Karnatak, India. MTech in (Digital Communication and Networking)

---***---

Abstract - *The security of information or message has become one of the principle challenges of the resource sharing with data communication over computer network. by using internet, secured messages or information can be transferred in a fast and easy way in various sectors such as government offices, private sector, military, medical areas and defence areas. most of the times, confidentiality of the transferred information needs to be maintained. To make sure that the information is transferred securely and safely over the computer network, a suitable method is needed. To improve the security of information or data, steganography must have the ability to resist detection by machine learning algorithms. In this paper, i am going to present an efficient algorithm for information hiding in an image based on machine learning. My proposed method uses all blocks of the host image and then embedding message bits are hides in to the host image pixels. The machine learning based model is designed to have 5 convolution layers with feed forward neural network. The SVM is a most common algorithm of machine learning, which is been used to smoothen the distorted image and we can retrieve the missed data by making use of it.*

Key Words: *Encryption, Decryption, Machine Learning, SVM, hiding information, Smoothening and retrieving.*

1. INTRODUCTION

Basically, there are two methods for protecting data from intruders while transferring over an open channel network, those are Cryptography and Steganography. Cryptography is a method to encrypt data and steganography is an art and science of hiding secret information in a cover image[7]. Maximum number of characters that can be hidden in an image is equal to the product of width and height of the image. Data in computers is transmitted and stored as a series of zeros and ones (also its known as Binary). To store an image on a computer, the image is broken down in to tiny blocks called pixels. This proposed simple method is to hide information in the encrypted image then send the encrypted image to the receiver over the network. Here we are taking the not a single word or single sentence instead we are taking a text file which contains the secrete information, its size can be in kb's or MB's. When we take text file which is to be hidden in to an image, that image is called as cover image which is of 256*256 pixel size. Already there are many encryption and decryption methods and also security of the data can be handleled by the stenography but the problem occurs when, we are transferring a large amount of data or large text file it may be of any size. Once we finish the encryption part and append the information in to an image the encrypted image will be distorted because of the misplacing of pixels or we can say bits. So due to that we may lose the important message which is present in the file so machine learning algorithm can be used to retrieve that lost message and here SVM is been used for smoothening of distorted image. The most popular medium used is image files because of their high capacity and easy availability over the internet [2]. At the sender's side, the image used for embedding the secret message is called cover image, and the secret information that needs to be protected is called a message.

This paper proposes a new filtering method based on SVM. We establish a relationship between the secret information size and a noise vector.

2. Literature Cited

"Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, Bin Li" They proposed a methodology that utilizes GANs for steganography, it is very different from past methodologies. Past steganography strategies which are utilizing GANs are inserting based ones, where customary installing abilities, for example, LSB-coordinate are utilized in the to conceal the mystery data. While in this technique, they have utilized DCGANs to a produce spread picture just as per mystery data, and the spread picture (additionally is simply the stego picture) officially "contained" mystery data, there is no inserting procedure in their strategy.

Kamaldeep Joshi, Swati Gill, and Rajkumar Yadav

They have proposed the LSB strategy, This technique gives an exceptionally fundamental thought of steganography in a simple way. The LSB technique expresses that the mystery data bits we can put by supplanting the least noteworthy bits of the pixels of a picture. It permits full 100% inclusion of a data double bits in the pixels of a picture with an exact moment change of +1 or −1 in the estimation of the pixels. This technique was helpless against assault as the message was available at LSB, and by just picking LSBs, there is a probability of getting to information by introdure. And after that quantization commotion comes in to the image and it can likewise crush the information present on least critical bits. Along these lines, this strategy can be effectively decoded by the programmer and is likewise not invulnerable to the clamor and pressure procedures. Additionally, LSB strategy enables us to embed just single piece of message information inside the specific pixel. Give us a chance to

attempt to comprehend with the assistance of the accompanying model.
Assume the message string must be sent over the PC system or web is 10010101, what's more, the estimation of consistent pixels are as per the following:

01101000 10101001 01101000 11110000 00011101 10000001 11110000 10101010.

At that point subsequent to embeddings the message, pixels would be as pursues:

01101001 10101000 01101000 11110001 00011100 10000001 11110000 10101011.

Saleh Delbarpour Ahmadi and Hedieh Sajedi

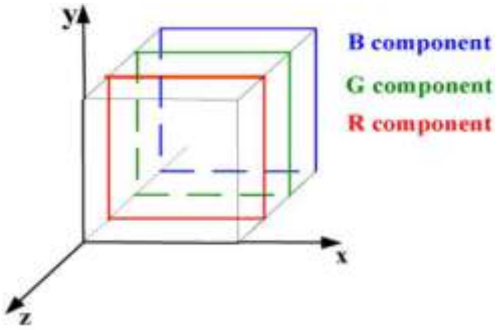
In this paper, they proposed a strategy dependent on AIS calculation and the least critical bits substitution. The proposed technique right off the bat finds a locale of a host picture that is like the host picture and afterward implant a little piece of a message in it to hold the proportion of the quantity of message bits to the quantity of host picture bits and tunes the parameters of AIS calculation. Inserting is moderate when the measure of a mystery message is substantial. When we use meta-heuristic calculations for finding the best answer for installing, this procedure is moderate. To conquer this issue utilized a piece of host picture p and after that resized mystery message r with the end goal that the proportion of host picture pixel bits to mystery message bits and the proportion of p pixel bits to r bits be equivalent.

Dong-hyun kim and Hae yeoun Lee

In this they presented a deep learning based stegnoanalyse model against spatial domain stenography and show the preliminary results. Unknown images are tested to decide the existence of the secret message. Experiments are performed using BOSS and SIPI database and 98% and 90% accuracy are achieved for LSB stegno-images with the same key and the different keys.

Ms. A. S. Bhandare, Padmabhooshan Vasantrodada Patil institute.

“In this mentioned system only one bit from a pixel is used to store the information available. A character contains 8 bits of information. So it takes 8 pixels of the image to store one character information. So the number of characters that can be stored in an image is very less i.e. Number of pixels/8. In the currently proposed system, color images are used to hide the information. In color images, each pixel has three components i.e. Red, Blue and Green as a vector space as shown in Fig.1. Each component is represented by 8 bits. Three LSB bits from each color component are used to store the information. So nine bits are available from each pixel to store the information. One character can be stored in one pixel. So total number of characters that can be stored in the image are equal to the total number of pixels in the images. The quality of image is not affected by this approach. So the redundancy bits are used more efficiently and the capacity of storing the information is improved 8 times the previous system.”



Ako Muhammad Abdullah and Roza Hikmat Hama Aziz

This paper proposes a new system to embed a secret message in a cover image using Hash based (3, 3, 2) LSB insertion method with Affine cipher algorithm. Our system is designed to encrypt data and hide all the data in patted within the message to keep the privacy of the data. Then, the system has been developed based on the cryptography and steganography algorithm. The main focus of the paper is to develop a system with extra security features. Cryptography strategy i.e Affine figure calculation has been executed to scramble the mystery message and changed over into ASCII code before installing it in the picture so it is difficult to interloper to break the encryption without the keys and secret word. Furthermore, Hash based Least Significant Bit (H-LSB) strategy has been executed for implanting scramble message into spread pictures.

3. CONCLUSION

At last our intension is to accomplish an application for information security by utilizing AI(ML) calculations. Also, we can have handle on loosing information amid change from source to goal.

REFERENCES

[1] Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, Bin Li" A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks"

[2] Kamaldeep Joshi, Swati Gill, and Rajkumar Yadav" A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image"
Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India. kamalmintwal@gmail.com

Received 25 December 2017; Accepted 11 April 2018; Published 1 August 2018

[3] Saleh Delbarpour Ahmadi. "Image Steganography with Artificial Immune System" Faculty of Computer and Information Technology
Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran Saleh.delbarpour@yahoo.com

[4] Dong-Hyun kim "Deep learning based steganalysis against spatial domain steganography" dept.of software engineering kumaho national institute of technology,Gumy, gyeonbuk republic of korea.

[5] Kumar Nannapaneni Manoj, Kumar M. Praveen, Rao M. Srinivasa,"
Data Hiding Using Image Steganography " International Journal of Advance Research and
Development.

[6] https://www.researchgate.net/publication/304066315
Ako Muhammad Abdullah and Roza Hikmat Hama Aziz " New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm "
MSc. Computer Science Faculty of Physical & Basic Education Computer Science Department University of Sulaimani Kurdistan Region-Iraq