International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 08 | Aug 2019 www.irjet.net p-ISSN: 2395-0072

Machine Learning Application for Data Security

Ms. Priyanka M Ninganure[1], Asst.Prof. V K Shende[2]

[1]MTech(DCN) Student, Dept. of ECE, Gogte Institute of Technology, Belagavi, Karnataka, India
[2] Asst.Professor, Dept. of ECE, Gogte Institute of Technology, Belagavi, Karnataka, India

---

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, secrete 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 defense 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, stegnography must have the ability to resist detection by machine learning algorithms. This presents an efficient algorithm for information hiding in an image based on machine learning. Proposed method uses blocks of the cover image and then embedding message bits are hides in to the cover 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 to provide double fold to security VGG19 model of DNN is been building. Since by using these model it is possible to retrieve the data which is missed during transmission.*

Key Words: **Cryptography, Steganography, Secret message, Cover image, encryption, decryption, SVM and DNN Model.**

1. INTRODUCTION

Initially, there are two techniques for shielding information from interlopers while exchanging over an open channel. Those are Cryptography and Steganography. Cryptography is a technique to encode information and steganography is a craftsmanship and investigation of concealing mystery data in a spread picture. 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 values). To store an image on a computer, the image is broken down in to tiny blocks. 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 not taking 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. There are many encryption and decryption methods are present, security of the data can be handled 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 appending 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. The image used for embedding the secret message at the sender side is called cover image, and message is that the secret information which needs to be protected by intruder or hacker. This model proposes a new filtering method based on SVM. In this is been demonstrated that a relationship between the noise vector and secrete information size.

2. Designing of Proposed Model Stages of proposed system.

1) Secret Text on to an image using only steganography.

2) Image to image steganography using machine learning.

Picture Selection to Disguise Cryptography Select a picture that can without much of a stretch mix with its encompassing when it is adjusted. For example a picture that has a high level of relationship with its environment, this procedure proposing to embed content. We don't expect to choose an exceedingly particular picture supposing that we alter such a picture the progressions would be unmistakable. Since we are wanting to adjust picture in the spatial space choosing an appropriate picture is significant procedure. To embed the mystery message on the chose picture, we have two essential presumptions in this progression: initially, the sender and the recipient realize which picture is being transmitted and also, the territory in the picture that is utilized for concealing mystery information. We recommend utilizing a zone that has a high level of clamor or high level of connection with its environment. Choosing a legitimate picture is a basic advance since we will change the pixels in the spatial space. In the wake of choosing an appropriate part in a picture the content can be embedded. Content can be written from numerous points of view. The picture chose for this object is known as the spread picture and the picture acquired after steganography is known as the stego-picture. A picture is spoken to as a N*M (in the event of greyscale pictures) or N*M*3 (if there should be an occurrence of shading pictures) lattice in memory, with every passage speaking to the power estimation of a pixel. In picture steganography, a message is inserted into a picture by

modifying the estimations of certain pixels, which are picked by an encryption calculation. The beneficiary of the picture must know about a similar calculation so as to known which pixels the person in question must choose to extricate the message.

2.1 Pixel idea and shading models

As of now referenced, pixels are the littlest individual component of a picture. Thus, every pixel is an example of a unique picture or an image. That is to say, the original can have progressively exact portrays by using more samples. The strength of every pixel in an image is variable. Frameworks in colour imaging, a colour is ordinarily indicates by three or four segment powers, for example, red, green, and blue, or cyan, red, yellow, and dark. Here, will work with the RGB shading model. As you can envision, the RGB shading model has 3 channels, red, green and blue. In this way, every pixel from the picture is made out of 3 esteems (red, green, blue) which are 8-bit esteems (the range is 0– 255).for every pixel we have three qualities, which can be spoken to in paired code (the PC language).When working with twofold codes, we have increasingly critical bits and less noteworthy bits. For instance, on the off chance that we change the furthest left piece from 1 to 0 it will change the decimal incentive from 255 to 127. On the other hand, the furthest right piece is the less huge piece. In the event that we change the furthest right piece it will have less effect on the last esteem. For instance, in the event that we change the furthest left piece from 1 to 0 it will change the decimal incentive from 255 to 254. Note that the furthest right piece will change just 1 of every scope of 256 (it speaks to under 1%).

3. Architecture of Proposed Model

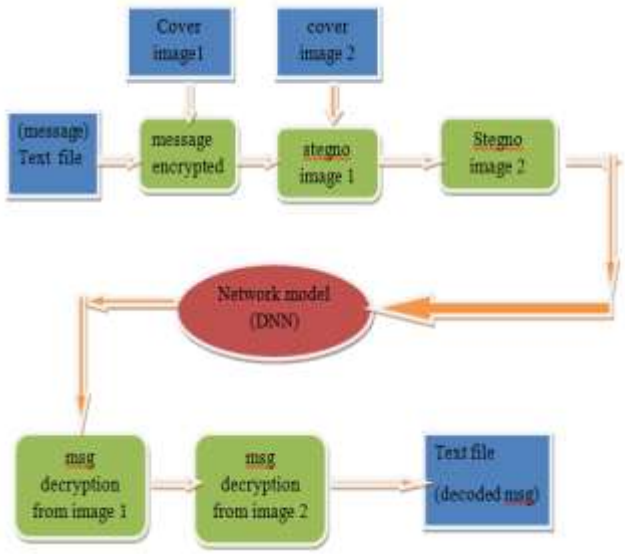


Fig1: Flow of proposed model using DNN

The above block diagram shows the flow of proposed model. Which consists of two stages. Secrete Text appended on to an image using only Stegnography and in second stage image to image stegnography using DNN.

- Secrete message and cover image: Where secrete message is a file which consists of text, it can be of any size. Within cover media steganography hides the secrete message, where we can use the cover media as audio, video, text or an image The each pixel of the cover image merged with the each bits of characters. This resultant image is called as stegno image1 which consists of encrypted message.
- Cover image2 and stegno image2: Here cover image2 is similar to cover image1 but it is different image. Which gets appended with the stegno image and gives the resultant image which we can call stegno image2.To provide still more stronger security this step is been performed. Here it is possible to perform stegno image to cover image appending and smoothening process in parallel by using DNN.
- Decryption of stegno images 1 &2: Decryption is the process of transforming encrypted information so that it is intelligible again. Will get non-readable messages to readable messages.

Network Model: The network model is built by using SVM(Support vector machine) and DNN(Deep Neural Network) Since SVM is classification algorithm we can use this in removing noise from message. The support vectors are created during the training time. These support vectors are required for the formation of the optimal hyperplane.

3.1 EXPERIMENTAL RESULTS

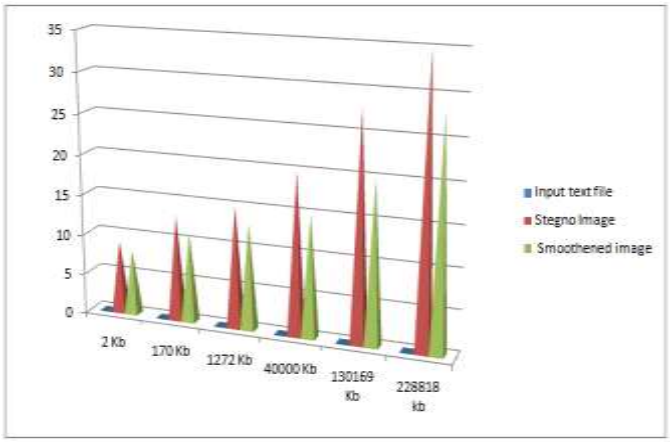
Table1: Results Comparing Before Smoothening and after Smoothening of stegno images.

Text file (Size in kb)	Cover image 1 (Size in kb)	Cover image 2 (Size in kb)	Stegno Image which contained secret information (size in kb)	Output Image After smoothening by using proposed model (Size in kb)
2	7	12	9	8
170	7	12	13	11
1272	7	12	15	13
40000	7	12	20	15
130169	7	12	28	20
228818	7	12	35	28

Description: By looking at above table we can justify that, if the text file size increases then the amount of noise will be

increased accordingly. And that noise is been removed by smoothing process.

GRAPH1: Variation in the size of the images in each of the stage.



This graph shows the variation in the size of the images when the text file is varied from small size to large size. Where Input text file is indicated by blue, Stegno image is indicated by red and Smoothened stegno image is been indicated by green which contains the encrypted information. Where six different sizes of text files are taken and performed the proposed technique for data security. We can observe the reduction in noise at the final stage.

Fig (a) Original cover image1 (Size 7Kb)

Fig (b) Stegno image1(Contained secrete information and Size is 14Kb)

(a) and (b) : For ex 170kb input text file is been considered, this information is encoded and appended with original image1. which gives us Stegno image1 which contained secrete information along with that natural noise is added.

Fig (c) Stegno image1(Blurred image)

Fig (d) Cover image2 (11Kb)

(c) and (d): Stegno image1 is again appended with one more cover image2 just to provide strong security.

Fig (e) Output image after Smoothening (11Kb)

(e): We will get one more stegno image2 and which is fed to network as an input to smoothen it. In this process we smoothen the image2 first then image1 secondly to remove noise from this image also we can retrieve the lost information during transmission. Then we go for decoding data to get desired text file.

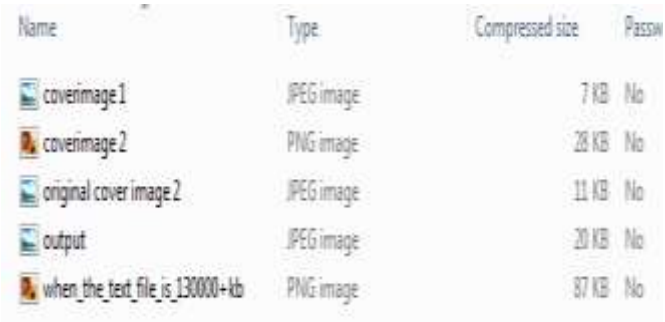


Fig2: performed demo when text file is130000Kb

Note: Here you can observe that, file size is 130000Kb and stegno image which contained secrete information is 28Kb then after smoothening image size will become 20kb. So we can say that around 8kb of noise is been removed from an image.

Fig 3: Output when File size is 40000kb

4. CONCLUSION and FUTURE SCOPE

This project presents the Information hiding and which prevents the information loss which occurs during the transmission on a particular path. It is the right technique to exchange secret information over the internet. Proposed model uses VGG19 model of DNN to remove the noise from stegno images.

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 "

[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 "

[7] Fuzhou Gong and Zigeng Xia Academy of Mathematics and Systems Science, Chinese Academy of Sciences2University of Chinese Academy of Sciences. "

[8] Álvaro Ramiro Hernández Millán, Larry Mauricio Portocarrero López, Miguel Mendoza-Moreno, Alexander Castro-Romero. Facultad de Ingeniería, Escuela de Ing. Sistemas y Computación Universidad Pedagógica y Tecnológica de Colombia, U.P.T.C. Tunja, Colombia alvaro.

[9] Subhajit Chaudhury, Sakyasingha Dasgupta, Asim Munawar, Md. A. Salam Khan, Ryuki Tachibana. 2017 IEEE INTERNATIONAL WORKSHOP ON MACHINE LEARNING FOR SIGNAL PROCESSING, SEPT. 25–28, 2017, TOKYO, JAPAN"TEXT TO IMAGE GENERATIVE MODEL USING CONSTRAINED EMBEDDING SPACE MAPPING".

[10] Rupesh Gupta Dr.Tanu Preet Singh. Computer Science and Engineering DepartmentACET Amritsar, PTU Jalandhar, Indi ACET Amritsar, PTU Jalandhar, India gupta_rupesh_mani@yahoo.co.in

[11] G.Prashanti Information Technology Vignan's Lara ammulu1310@gmail.com."Data Confidentiality Using Steganography and Cryptographic Techniques".

[12] Ammad Ul Islam1, Faiza Khalid2, Mohsin Shah2 "An Improved Image Steganography Technique based on MSB using Bit Differencing".

[13] Lisa M. Marvel and Charles T. Retter U.S. Army Research Laboratory "Hiding Information in Images".

[14] Garima Gupta (*M.Tech Student*) Department of Computer Science Engineering Department, Poornima College of Engineering, Jaipur(Rajasthan),India" Hiding Text Data in Image through Image Watermarking using DCT & DWT".

[15] MENG Yan-yan, GAO Bao-jian, Qiang Yuan,Yu Fu-gen,Wang Cui-fang " A Novel Steganalysis of Data Hiding in Binary Text Images"

[16] Amarjit Roy, Rabul Hussain Laskar ECE Department NIT Silchar Silchar, India" Impulse noise removal based on SVM classification "