Integration of Cryptography and Steganography

using Deep Neural Network in Image and Data Processing.

Bishal Saha

Vellore Institute Of Technology,Vellore,Tamil Nadu,India

bishal.saha2020@vitstudent.ac.in

Abstract. Today we are living in a world where data and digital information plays a vital role in our day to day life.But with the evolution of citizens to e-citizens privacy and security is becoming a huge concern for us.In this work Deep Neural Network has been employed to prevent any unaccredited access of data.In present scenario there are several kind of cryptography and steganography technique some are very much secure and some are not.In our work we have employed both cryptography as well as steganography technique simultaneously with the help of Deep Neural Networks.Our Deep Neural Network will use bitand method during steganography and bitxor method during cryptography.This approach is very much secure than any single cryptography method,because here first the message data is encrypted(using cryptography method) and then steganography process takes place on the carrier data and on encrypted data.In order to recover the original data firstly the reverse steganography takes place and follows by decryption which makes next to impossible to any hacker or any un-authorized person to get access the message.

Keyword:Neural Network,Cryptography,SteganographyEncryption,Decription.

1. Introduction

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer. The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today.

The brain routinely accomplishes perceptual recognition tasks, e.g. recognizing a familiar face embedded in an unfamiliar scene, in approximately 100-200 ms, whereas tasks of much lesser complexity may take days on a conventional computer. A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use.

It mirrors the brain in two respects –

1.Learning processes are used to capture information or raw data from the external surroundings.
2.Interconnection is established among neighboring neurons keeping in mind their weights. This is furthermore called as synaptic weights used to store the current information.

Network Architectures of ANN – Various arrangements of ANN have one thing in common which is, it has two layers the input and the output layer. Another layer exists known as the hidden layer that may exist in some cases.

On the basis of geometry of processing elements, we have 2 types of network architecture as –

1. Feedforward neural network (Single layer/Multilayer) 2.
2. Recurrent neural network
3. Back Propagation – Introduced in 1970s, faster as compared to other approaches. For problems which were insolvable earlier neural nets are used. The main objective behind back propagation solution is that the miscalculations introduced in hidden layer are ascertained by back-propagating the inaccuracies in the output layer.

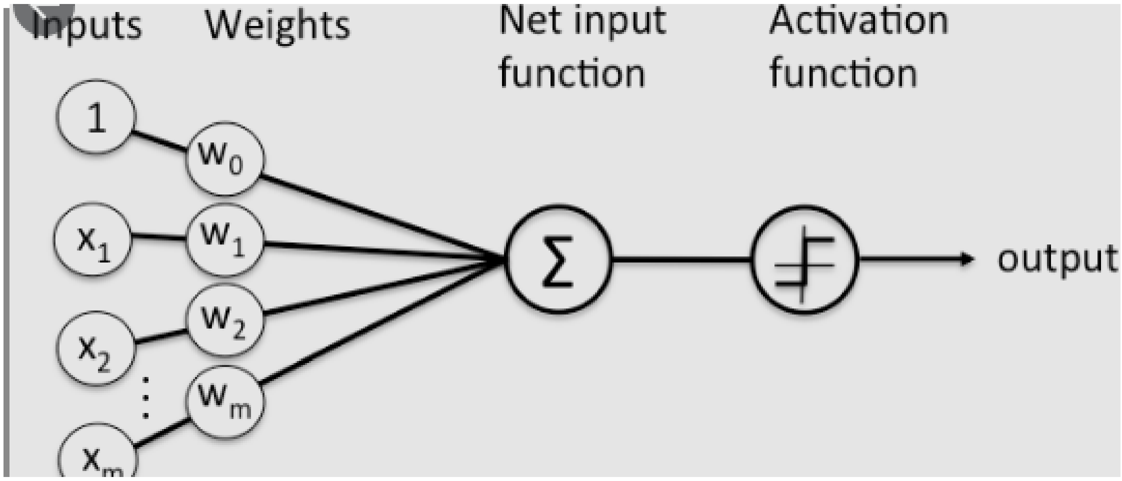


Fig 1: Single-Layered Feedforward neural Network

Cryptography

is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Types Of Cryptography

1. Symmetric Key Cryptography:
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and

receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. Hash Functions:
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography:
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

4.

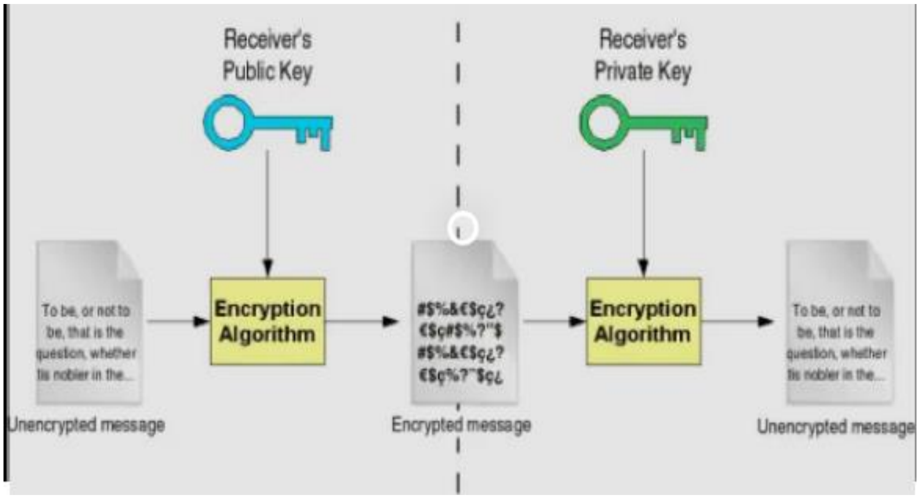


Fig 2-Cryptography flow chart

Stehanography-

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography *is* derived from the Greek words *steganos* (meaning *hidden* or c*overed*) and the Greek root *graph* (meaning *to write*).

The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It’s not a form of cryptography, because it doesn’t involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways. Where cryptography is a science that largely enables privacy, steganography is a practice that enables secrecy – and deceit.

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called *hidden text* -- is often encrypted before being incorporated into the innocuous-seeming *cover text* file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

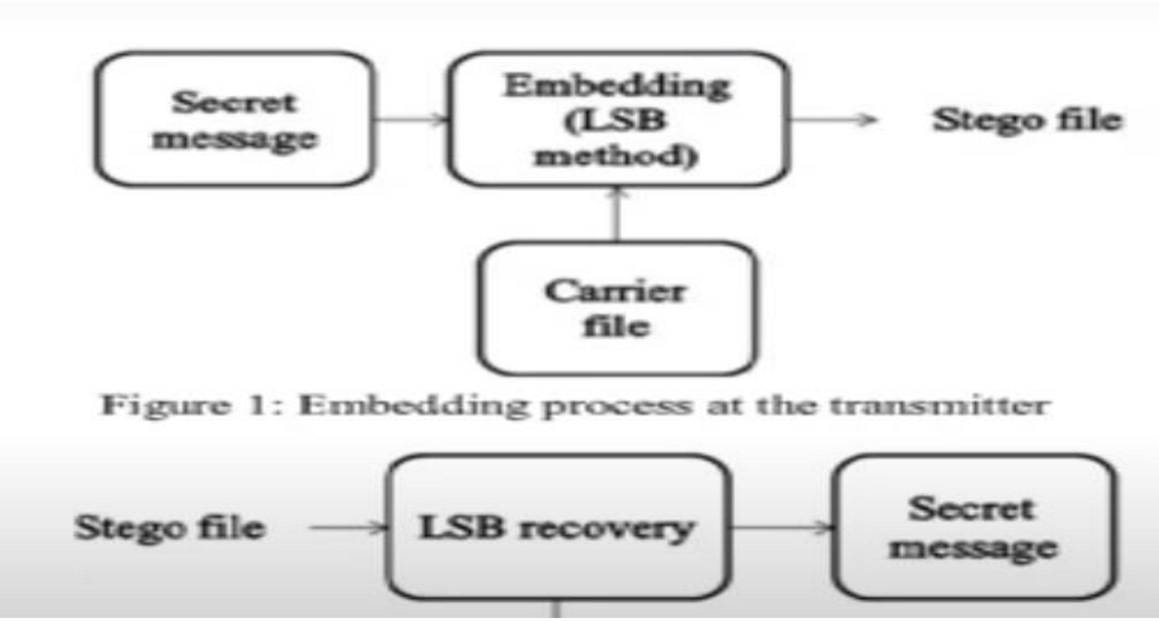


Fig 3-steganography flow chart

2.Method

In our work we have used cryptography followed by steganography simultaneously:-

Firstly have have train our deep neural network to perform the XOR operation in order to encrypt the the original message.After the encryption we have perform the steganography (in which we have overlap the encrypted data(image) with a carrier image(255 px intensity) using the AND operation.

In order to get our original image data,we first have to perform the reverse steganography process using same AND operation and then after than we have to decrypt the image data that we got from the reverse steganography process using XOR operation.while doing so,due to some noice our imagae data may loose some in tensity but it will be 99% similar to the original image data.

As a result we will get a channel where our original image data will be very much secure and it cannot be hack or crack by any un-authorised person,because in order to do that he/she fistly have to perform the reverse steganography technique and after than he must have to know the symmetric key to decryption image.

Secret image	Encryption	Encrypt+ Carrier image	steganography	channel	Reverse Steganography	Decryption	Secret image

Step by Step approach from left to right using deep neural networks.

Tables:-

BIT XOR Gate during cryptography process

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

Table -1

BIT AND Gate during Steganography process

A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

Table-2

Sample Exapmle

00110101	Secret Message
11100011	Symmetric Key
11010110	XOR operation-Encryped
Some data	BIT-AND opperation Steganography
Some data	BIT-AND operation Reverse steganography
11100011	Symmetric Key
--	--
00110101	XOR operation-Decrypted original message signal

2.1Program Code

```
clc
warning off
a=imread('Carrier.png');
nexttile;
imshow(a);
title('Carrier Image');
x=imread('SECRET.jpg');
nexttile;
imshow(x);
title('Secret Image');
[r c g]=size(a);
x=imresize(x,[r c]);
ra=a(:,:,1);
ga=a(:,:,2);
ba=a(:,:,3);
rx=x(:,:,1);
gx=x(:,:,2);
bx=x(:,:,3);
sk=uint8(rand(r,c)*255);%Secret key
rx=bitxor(rx,sk);
gx=bitxor(gx,sk);
bx=bitxor(bx,sk);
nexttile;
imshow(cat(3,rx,gx,bx));
title('Encrypted Secret Message');
for i=1:r
for j=1:c
nc(i,j)= bitand(ra(i,j),254);
ns(i,j)= bitand(rx(i,j),128);
ds(i,j)=ns(i,j)/128;
fr(i,j)=nc(i,j)+ds(i,j);
end
end
redsteg=fr;
for i=1:r
for j=1:c
nc(i,j)= bitand(ga(i,j),254);
ns(i,j)= bitand(gx(i,j),128);
ds(i,j)=ns(i,j)/128;
fr(i,j)=nc(i,j)+ds(i,j);
end
end
```

```
greensteg=fr;
for i=1:r
for j=1:c
nc(i,j)= bitand(ba(i,j),254);
ns(i,j)= bitand(bx(i,j),128);
ds(i,j)=ns(i,j)/128;
fr(i,j)=nc(i,j)+ds(i,j);
end
end
bluesteg=fr;
finalsteg=cat(3,redsteg,greensteg,bluesteg);
redstegr=finalsteg(:,:,1);
greenstegr=finalsteg(:,:,2);
bluestegr=finalsteg(:,:,3);
nexttile;
imshow(finalsteg);
title('Stegmented Image');
for i=1:r
for j=1:c
nc(i,j)=bitand(redstegr(i,j),1);
ms(i,j)=nc(i,j)*128;
end
end
recoveredr=ms;
for i=1:r
for j=1:c
nc(i,j)=bitand(greenstegr(i,j),1);
ms(i,j)=nc(i,j)*128;
end
end
recoveredg=ms;
for i=1:r
for j=1:c
nc(i,j)=bitand(bluestegr(i,j),1);
ms(i,j)=nc(i,j)*128;
end
end
recoveredb=ms;
output=cat(3,recoveredr,recoveredg,recoveredb);
nexttile;
imshow(output);
title('Recovered Encrypted Image from Steganography');
red_band=bitxor(output(:,:,1),sk);
green_band=bitxor(output(:,:,2),sk);
blue_band=bitxor(output(:,:,3),sk);
combined=cat(3,red_band,green_band,blue_band);
nexttile;
imshow(combined);
title('Decrypted secret message signal');
```

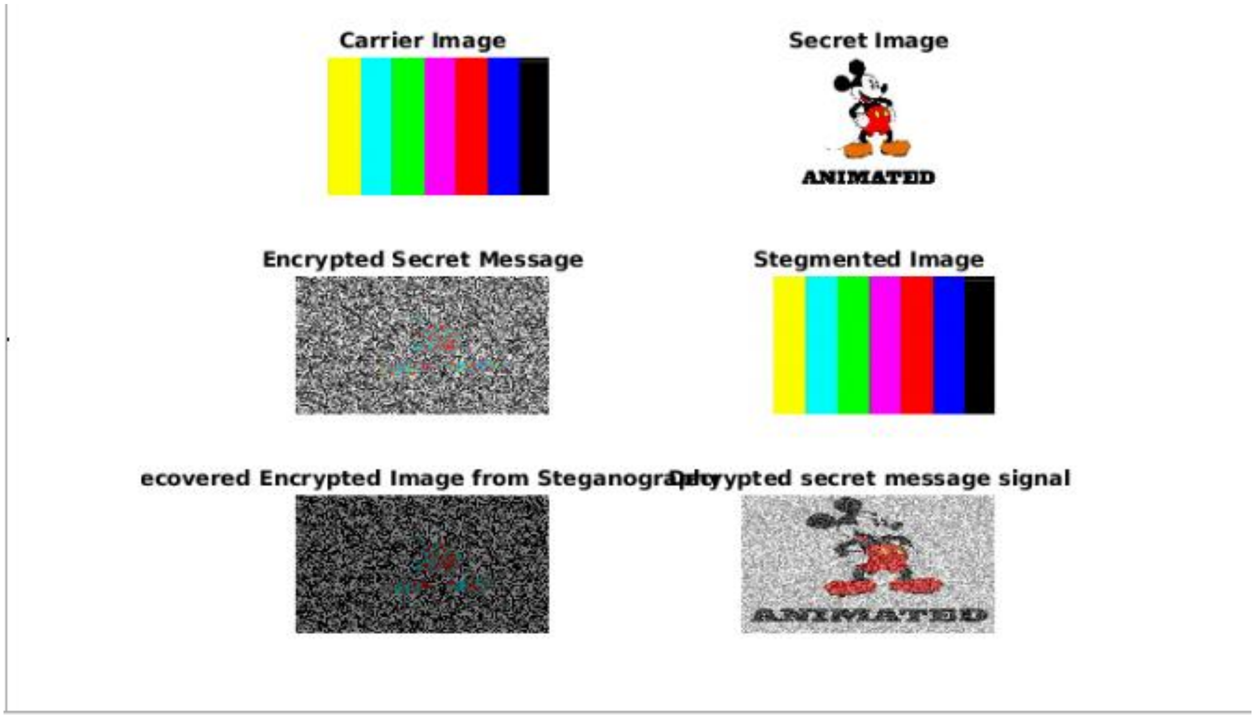
3.Result

Here we can see that we have a secret image of(Micky mouse) and a text(“Animated”) is given.So as discussed above firstly the secret message is encrypted.After the encryption the steganograpgy takes place between the carrier signal and the encrypted message which is also called segmented image.

The segamented imaged is a mixture of encryption as well as steganography.

In the recovery process,firstly the reverse steganography takes place which fetches the encrypted data(message) from the carrier image.After getting the encrypted image the encrypted image is decrypted by using a symmetric key and finally we get the original secret image.

Although the quality and intensity of the output scret image decreases because of encryption,steganography,decryption and noice by the output secret image is readable and similar.



4.Conclusion

The application of Deep neural network is quite vast and presently it is employed in all domains.one of the domain in we have make our project is the field of Information and data security.The deep learning algorithms can be used to encrypt and decrypt our data.It is also using is steganography process.But the Integration of cryptography and the Steganography using the deep neural netwoks is the intelligent way to use this powerful deep learning tool because here we get almost double security without any leakage or loss of data.

This technique is very much secure and if in our practical life if we employ both the cryptography as well as steganography technique simultaneous using thes deep neural network then it may drastically reduces the cases of hacking,cracking or any othe illegal way to accessing the privacy.

5.References

[1]Bhavya Arora; K Srishti; Nikita Khatri; Vandana Niranjan Application of Artificial Neural Network in Cryptography Published in: 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)
ISBN Information:INSPECAccessionNumber: 19319093DOI: 10.1109/PEEIC47157.2019.8976550

[2]Applications of Steganography http://datahide.org

[3] Cryptography and its Types – GeeksforGeeks https://www.geeksforgeeks.org

[4]A. Eskicioglu; L. Litwin Cryptography Published in: IEEE Potentials (Volume: 20, Issue: 1, Feb/Mar 2001) ISSN Information: INSPEC Accession Number: 6869725 DOI: 10.1109/45.913211

[5] M. E. Smid and D. K. Branstad, "The Data Encryption Standard: Past and Future," Proceedings of The IEEE, vol. 76, no. 5, pp. 550-559, 1988.

[6] C. Boyd, "Modem Data Encryption," Electronics & Communication Journal, pp. 271-278, Oct. 1993. 131 N. Bourbakis and C. Alexopoulos, "Picture Data Encryption Using SC4N Pattern," Pattern Recognition, vol. 25, no. 6, pp. 567-581, 1992.

[7] J. C. Yen and J. I. GUO, "A New Image Encryption Algorithm and Its VLSI Architecture," 1999 IEEE Workshop on Signal Procs. Systems, Grand Hotel, Taipei, Taiwan, Oct. 18-22, pp. 430-437, 1999.

[8] C. J. Kuo and M. S. Chen, "A New Signal Encryption Technique and Its Attack Study," IEEE International Conference on Security Technology, Taipei, Taiwan,

[9] C. W. Wu and N. F. Rulkov, "Studying chaos via 1-D maps - A tutorial," IEEE Trans. on Circuits and Systems I-Fundamental Theory and Applications, vol. 40, no. 10, pp. 707-721, 1993.

[10] T. S. Parker and L. 0. Chua, "Chaos - A tutorial for engineers," IEEE Proc., vol. 75, pp. 982-1008, 1987.

[11]Haykin, Simon. Neural Networks, A Comprehensive Foundation. MacMillin College Publishing CO, New York. 1994.

[12]"Machine Learning, Neural and Statistical Classification" by D. Michie, D.J. Spiegelhalter, C.C. Taylor February 17, 1994

[13] "Design and Realization of A New Chaotic Neural Encryption/Decryption Network" by Scott Su, Alvin Lin, and Jui-Cheng Yen.

[14] “Capacity of Several Neural Networks With Respect to Digital Adder and Multiplier” by Daniel C. Biederman and Esther Ososanya

[15]"Artificial Intelligence A Modern Approach" by Stuart J. Russell and Peter Norvig

[16]Bhavya Arora; K Srishti; Nikita Khatri; Vandana Niranjan Application of Artificial Neural Network in Cryptography Published in: 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)
ISBN Information:INSPECAccessionNumber: 19319093DOI: 10.1109/PEEIC47157.2019.8976550

[17]Applications of Steganography http://datahide.org

[18] Cryptography and its Types – GeeksforGeeks https://www.geeksforgeeks.org

A. Eskicioglu; L. Litwin Cryptography Published in**:** IEEE Potentials (Volume: 20, Issue: 1, Feb/Mar 2001)
ISSN Information: INSPEC Accession Number**:** 6869725 DOI: 10.1109/45.913211