AN IMPROVED HYBRID NUMERICAL METHOD BASED ENCRYPTION ALGORITHM WITH NEURAL NETWORK STEGANOGRAPHY

Sai Krishna Dugyala (GU24496), Sai Sandeep Ravuri (YL30934), Lakshman Nukala (HR39332)
Department of Computer Science and Electrical Engineering,
University of Maryland Baltimore County

Abstract

Now-a-days many encryption algorithms have been proposed for network security. In our project, a cryptographic algorithm for the network security is proposed to assist the effectiveness of network security. Here symmetric key concept is used instead of public key, and this is considered to develop the encryption – decryption algorithm. In the encryption technique we will be using the improvised hybrid numerical method for generating the cipher values. These cipher values are stored in the Neural network model by using steganography technique and Least Significant Bit (LSB) algorithm, which helps in hiding the data in the weights. This Improved Hybrid Numerical method is a combination of bisection and Newton-Raphson methods. While sending the cipher values to the decryption phase, to increase the level of masking we added garbage weight to it. In decryption phase, we start decoding values starting from neural network model to converting ascii values to characters in the end. We decrypt in a reverse manner as we implemented the encryption. In our model we have observed that we can change 57992384 number of weights and our sample model was able to achieve maximum accuracy, because of the data that we might have used. This work extends an existing implementation that used a two-dimensional CNN to perform the preparation, hiding, and extraction phases of the steganography process. The performance of the proposed method was measured by comparing the predictions which have been changed before and after the changes to the neural network model.

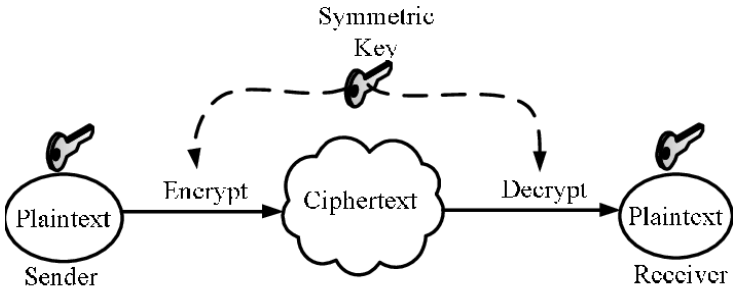
Keywords: Improved Hybrid Algorithm, Bisection Method, Newton-Raphson Method, Encryption, Decryption, Cryptography, Numerical Method, Steganography, Neural network, Symmetric Key Encryption.

Introduction

Now, network security is greatly dependent on the sending of communications in a concealed format. The study of mathematical methods relating to information security components like secrecy, data integrity, entity authentication, and data origin authentication is known as cryptography. It is the study of techniques for disguising messages so that only intended recipients can decipher them and understand the message. Information security can be provided by a variety of ways, not just cryptography. Through the processes of encryption and decryption, cryptography provides an effective solution to protect sensitive information in many applications, including personal data security, internet security, diplomatic and military communications security, etc. The art of encryption generally focuses on ways to transform information from its regular, understandable form into an unintelligible structure that renders it illegible without secret knowledge. Steganography is another method for protecting or obscuring data. This approach can be used to hide data in a variety of ways, including steganography in images, videos, audio, documents, neural networks, and more.

A cryptosystem is a collection of methods for encoding and decoding messages into plaintext and cipher text, indexed by one or more keys. The original data that needs to be encrypted is referred to as plaintext. The process of transforming plaintext into cipher text, or sporadically, a cryptogram, renders it unintelligible. The opposite procedure, known as decryption, restores the plaintext from a cipher text.

The number of keys used for encryption and decryption is used to classify and further characterize the various types of cryptographic methods. Public key cryptography, also known as asymmetric key cryptography (AKC), and secret key cryptography (SKC), are the two categories of algorithms (PKC). The encryption and decryption keys in symmetric key cryptography are symmetric, and examples of this type of algorithm include DES, AES, etc. Additionally, when using asymmetric key cryptography, the encryption and decryption keys are not the same. Examples of this type of algorithm include RSA and McEliece.



Numerous symmetric key and asymmetric key-based encryption and decryption techniques have been presented up to this point. Prior to the development of public key encryption, symmetric key cryptography algorithms were the most used. Data Encryption Standard (DES), which is commonly used in the system, is one application of symmetric key or private key cryptography. Additionally, symmetric key encryption and decryption algorithms are widely used in network security systems due to several shortcomings in asymmetric key encryption and decryption methods like RSA, etc. In this study, a secret key encryption and decryption technique based on numerical methods is created and made stronger utilizing neural network steganography. The secret is concealed using a hybrid root finding technique and neural network steganography. Also, neural network steganography is used to hide the cipher within a neural network in encryption algorithm.

Finding an approximated solution to the root of a nonlinear equation is one of the main topics of numerical analysis. An algorithm for finding x such that $f(x) = 0$ is called a root-finding algorithm. The bisection method using the intermediate value theorem is the simplest root-finding algorithm.

Note that the bisection method converges slowly but it is reliable. Tanakan suggested a modified bisection method using the concept of the secant method. On the other hand, the Newton-Raphson method using the derivative of a given nonlinear function is a root-finding algorithm which is more efficient than the bisection method. Note that the Newton-Raphson method converges quadratically although the bisection method converges linearly. Homeier suggested a modified Newton-Raphson method with cubic convergence.

Since the Newton-Raphson method may not be reliable, Altaee, Hoomod and Hussein suggested a hybrid algorithm to the bisection method and the Newton- Raphson method. In addition, Hussein, Altaee and Hoomod investigated a parallel hybrid algorithm to improve the simultaneous root-find algorithm suggested in a paper earlier.

The construction of the paper is as follows. In section 2, some prerequisite topics viz. Symmetric Key Cryptography, Neural Network Steganography, and Improved Hybrid Method are discussed. Then, in section 3, the proposed approach along with the explanation of Algorithm is discussed. In section 4, some results of the algorithms used are discussed. At last, in section 5, some conclusions are specified.

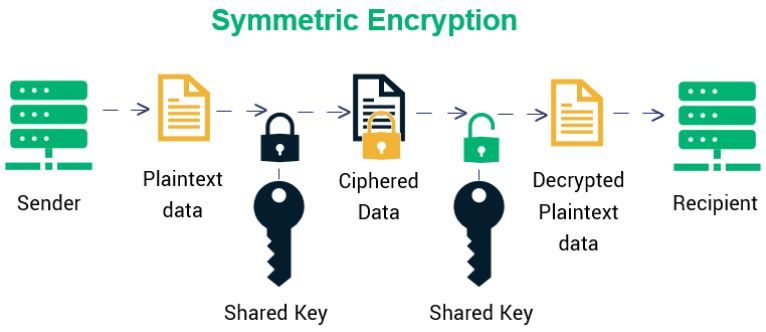
PREREQUISITE TOPICS

Here, in this section, some prerequisite subject matters and mathematics are discussed and these topics are used to develop the paper.

Secret Key Cryptography or Symmetric Key Cryptography (SKC)

There are several ways of classifying cryptographic algorithms. These are categorized based on the number of keys that are employed for encryption and decryption, and further defined by application and use. Symmetric Key Cryptography (SKC) is one of these important parts.

Symmetric cryptography is also referred to as conventional encryption or single key encryption. In symmetric cryptography the same key is used for both encryption and decryption. This technique can encrypt data, either locally by a single user to safeguard his/her files, or to be exchanged between users. If encrypted data is exchanged between two (or more) users, each must know the key to be used. Obviously, this key should be exchanged in a secure manner. Symmetric cryptography is commonly used to perform encryption. It also provides data integrity when symmetric keys are used in conjunction with other algorithms.



Neural Network Steganography

Steganography is the art of concealing sensitive or secret information within something that doesn't seem unusual. Because steganography and cryptology both work to protect sensitive information, they are sometimes confused with one another. The distinction between the two is that steganography involves concealing information while making it seem as though nothing is concealed at all. When someone sees the object where the information is hidden and is unaware that there is any hidden data, they won't try to decrypt the data. Modern-day steganography typically refers to data or a file that has been hidden inside a digital image, video, or audio file.

To guarantee data confidentiality, both steganography and encryption are employed. The primary distinction between them, though, is that with encryption, anyone can see that both parties are secretly speaking to one another. In the ideal case scenario, no one can tell that both parties are secretly conversing because steganography obscures the existence of a hidden communication. Because of this, steganography can be used for certain purposes like copyright marking. Although integrating copyright information into the file's content can help prevent it from being easily discovered and removed, adding encrypted copyright information to a file might be simple to erase. Secure communication is made possible through encryption, which requires a key to decrypt the data. Steganography offers a way to communicate privately that cannot be undone without drastically changing the data it is embedded in.

A hacker won't be able to access the implanted data unless they can find a means to identify it. Information can be concealed in picture, audio, and video files in a variety of ways. The LSB (Least Significant Byte) technique is typically used to conceal information within images. An image file is nothing more than a file that displays various colors and lighting intensities on various portions of a picture to a computer. A 24 Bit BMP (Bitmap) image is the ideal kind of image file to use for information concealment. The rationale is because this type of file is the biggest and typically has the best quality. It is much simpler to conceal and mask information when an image is high quality and resolution. Even though 24 Bit photos are the greatest because of their size for concealing information, some users may opt to utilize 8 Bit BMPs or another image format, such as GIF, because uploading huge images to the internet may raise suspicion. It's crucial to keep in mind that if you conceal information inside an image file and that file is converted to another picture format, the concealed information inside will probably be lost.

Steganalysis is the practice of finding steganography. Simply described, steganalysis is the process of identifying the presence of steganography in a file. Steganalysis focuses on finding hidden information in files rather than attempting to decrypt it. examining the file and comparing it to a different copy of the file published online can both help you spot steganography (Picture File). On the internet, photographs are frequently available in many copies, so you could wish to search for a few of them and compare the suspicious file to them. For instance, if you download a JPEG and your suspect file is also a JPEG and the two files resemble one other almost exactly, with the exception that one is larger than the other, it is highly likely that your suspect file contains concealed information.

Improved Hybrid Algorithm

At the middle of the preceding interval, we compute the x-intercept x using the Newton-Raphson approach in our improved hybrid algorithm. $[A_0, B_0]$ are configured to be [A, B]. We set $x_n = x$ and test the intermediate value theorem on $[a_{n-1}, x_n]$ and $[x_n, b_{n-1}]$ if x $[a_{n-1}, b_{n-1}]$. The interval that contains a root is identified by [an, bn] when we use the intermediate value theorem to determine it.

$$x^* \notin [a_{n-1}, b_{n-1}], \text{ then we set } x_n = \frac{a_{n-1}+b_{n-1}}{2}$$

Then test $[a_{n-1}, x_n]$ and $[x_n, b_{n-1}]$ for the intermediate value theorem. The interval that contains a root is identified by $[a_n, b_n]$ when we use the intermediate value theorem to determine it. This procedure gives us a reliable method for our algorithm's convergence. Additionally, because we combine the bisection method with the Newton-Raphson approach in our algorithm, it is more effective than the bisection-method.

	Improved Hybrid Method	
n	x_n	$f(x_n)$
1	-0.0795595	-0.0793922
2	2.4602202	1.1847268
3	1.1903304	0.8720762
4	0.5553854	0.5069685
5	-0.0088784	-0.0088782
6	0.2732535	-0.2667418
7	-0.0015345	-0.0015345
8	0.1358595	0.1350327
9	-0.0002018	-0.0002018
10	0.0678289	0.0677251

Table 2: Improved Hybrid Method for $f(x) = Tan^{-1}x$ on $[-4, 5]$

An Improved hybrid algorithm to the bisection method and the Newton-Raphson method is given as follows.

Improved Hybrid Algorithm:

Given $f(x)$, $f'(x)$, $[a, b]$ (interval) and $\delta = 1.0 \times 10^{-5}$ (tolerance error)

Step 1: $i = 1$.

Step 2: $c = \frac{a+b}{2}$.

Step 3: if $a < c - \frac{f(c)}{f'(c)} < b$, then $x_i = c - \frac{f(c)}{f'(c)}$.

Step 4: Else, $x_i = \frac{a+b}{2}$.

Step 5: If $|f(x_i)| < \delta$, then go to Step 8.

Step 6: If $f(a)f(x_i) < 0$, then $b = x_i$ and go to Step 2.

Step 7: Else, $a = x_i$ and go to Step 2.

Step 8: Stop iteration.

As we can see in Table 2, the sequence $\{x_n\}$ obtained by the improved hybrid algorithm converges although the sequence $\{x_n\}$ obtained by the hybrid algorithm. In addition, the number of iterations by the improved hybrid algorithm is 13 although the number of iterations by the bisection method is 22 when the tolerance error is 1.0×10^{-5}.

PROPOSED WORK

In this section, the overall proposed work on numerical method-based Encryption – Decryption Algorithm along with Steganography is discussed.

The Proposed Algorithms for Encryption and Decryption are given below:

Algorithm for Encryption:

Step–1: Read the characters from a text file and get the ASCII values for different characters.
Step–2: We are creating a symmetric key which will be used to form the mathematical equation, which helps in encrypting data.
Step–3: From this mathematical equation we subtract the ASCII values and equate it to zero.
Step–4: Use the hybrid root finding method to solve every equation.
Step–5: Store the root values from the above equations in a text file.
Step–6: Now by using the Neural Network Steganography we will hide the root values from the text file in the weights of the pre-trained model (Resnet152) by performing the Least Significant Bit (LSB) algorithm.
Step–7: After this we will add some noise in the form of garbage weights.

Algorithm for Decryption:

Step–1: In Decryption phase, we read the updated neural network model up to the last updated weight (excluding the garbage weights)
Step–2: Extract the least significant bits of each weight and store them in an array.
Step–3: Substitute the values from array into the mathematical equations and get the functional values.
Step–4: Convert the functional values, which are in the form ASCII values into characters and put into a text file.

1.1 Encryption Process

Create a Text File: First, we write a text message into a text file. Now using file pointer, we read the characters and store the ASCII value of these characters.
Then these values are used to form a mathematical equation (a secret key is present in this equation as mentioned above in the algorithm) and find roots for this equation using the Improved Hybrid Algorithm.

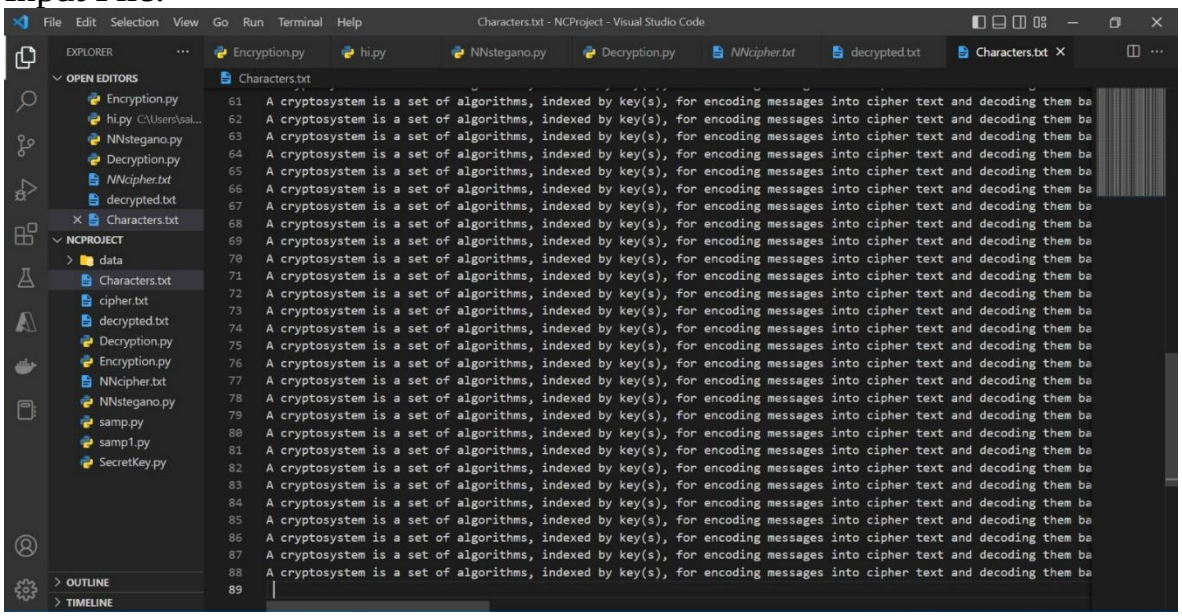
1) **Least Significant Bit (LSB):** The roots from the mathematical equation are converted to 32-bit binary value and stored in an array. We treat the last 16 bits of the neural network weights as Least Significant Bits for our case. From each 32-bit values from array every 16-bit value is used to replace the Least Significant Bits of the generated weights from he Conv2D model and then the 16-bit values are removed from the original array. We continue this process till all the stored values from the array are replaced. We are replacing the Lease significant bits only because even though these bits are modified the final output will not be affected.
2) **Put Garbage Pixels:** Using sequence or a series, put some garbage pixel to make the encryption process more secure.

1.2 Decryption Process

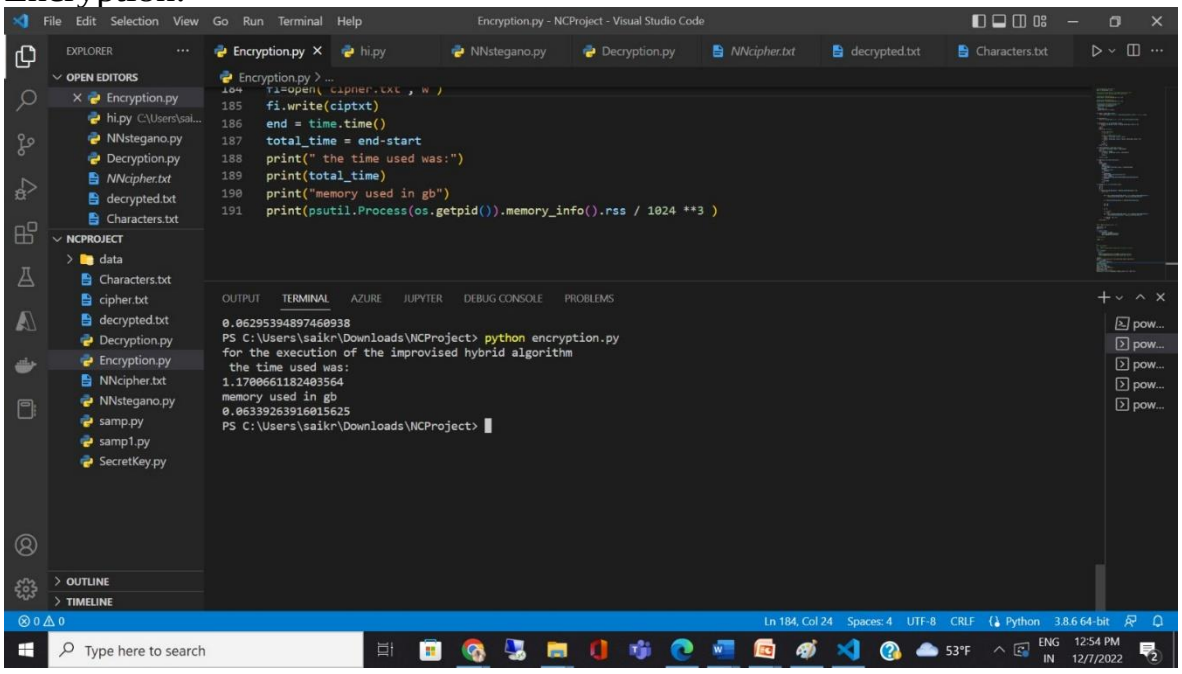
1) We extract all the LSBs from the updated neural network model and store it in an array. As these values are stored in 32-bit floating points we first change the encoding to ASCII. These ASCII values when substituted in the equation will result in the original ASCII values. These values are converted to text which generates the original data.
2) **Calculate the Functional Values to get the ASCII Values of the Characters:** Now put the solutions into the function and calculate the functional values. For example, $f(3.0805) = 76.99585$. Now rounding the result, we can get 77, which is the ASCII value of 'M'. Finally writethe character into a text file and then finding the other characters by similar way one can read andunderstand the total message.

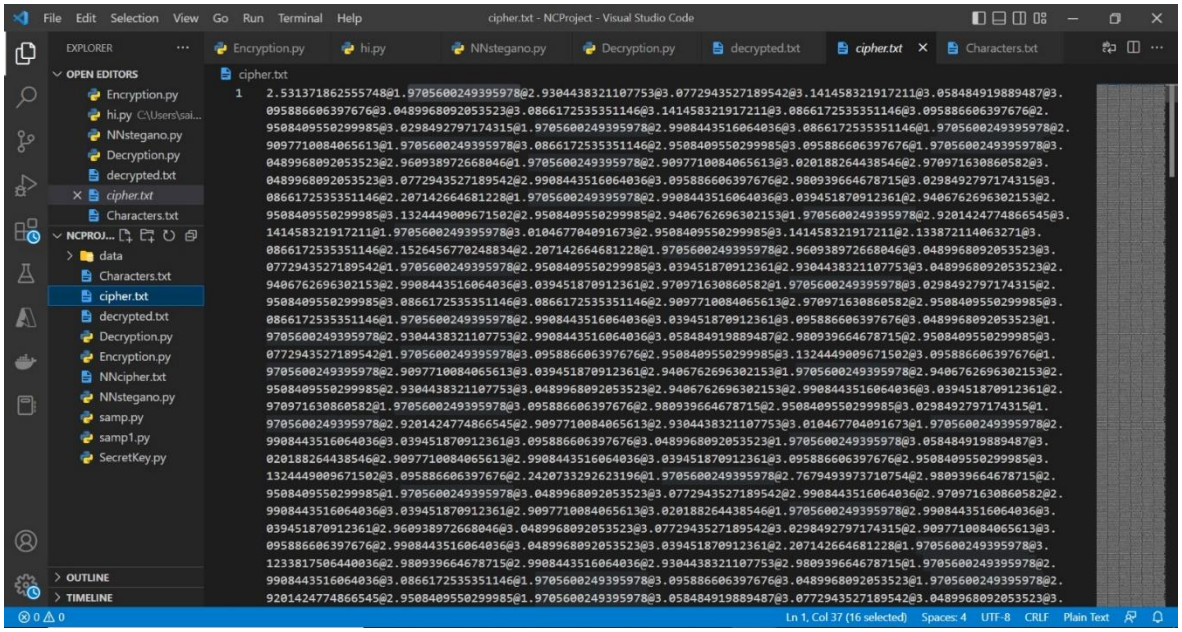
Results

Input File:



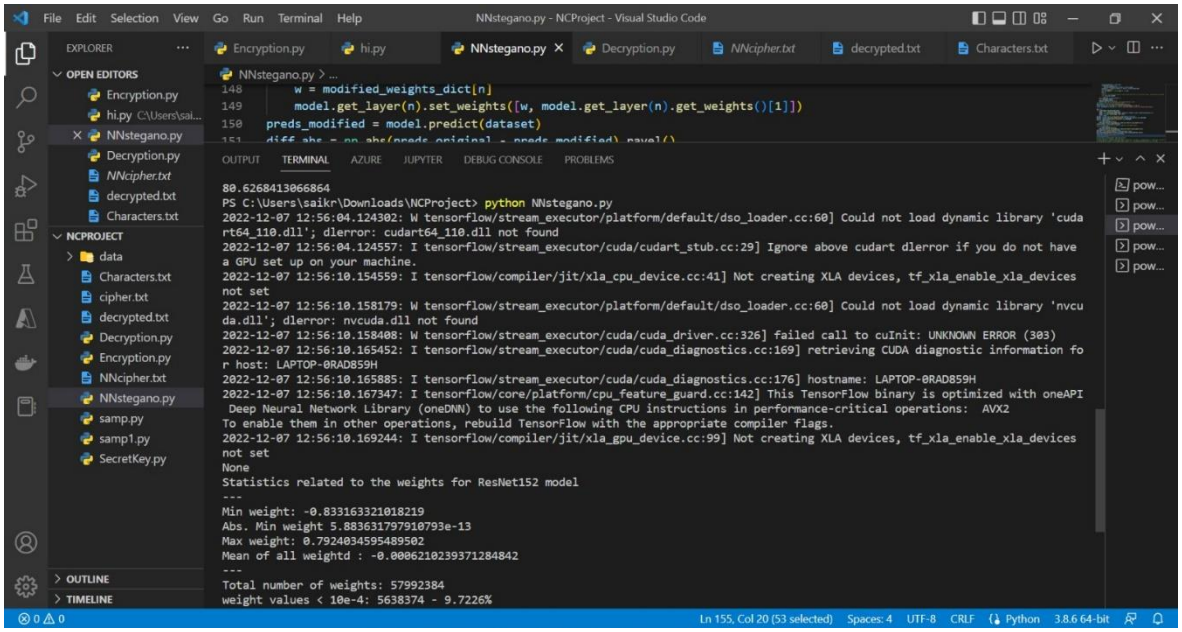
Encryption:





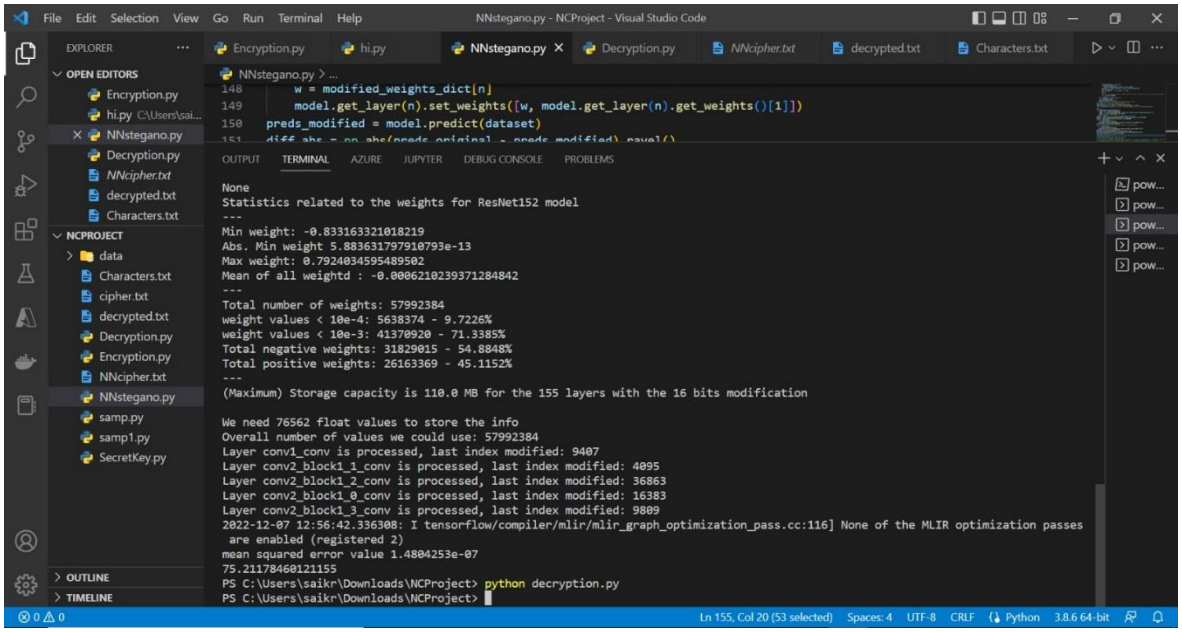
In the above screenshot we can see the roots generated by the Improvised Hybrid Algorithm.

Neural Network:



In the above screenshot we can see that the neural network model got saved with the modified weights.

Decryption:

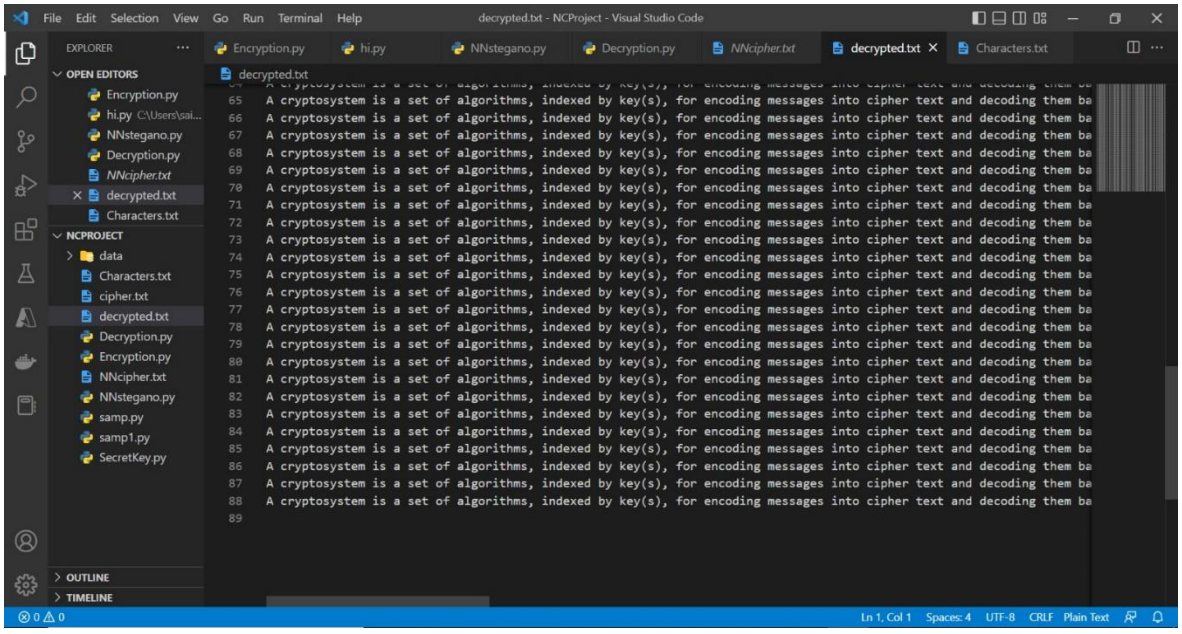

File Edit Selection View Go Run Terminal Help
NNstegano.py - NCProject - Visual Studio Code
EXPLORER
OPEN EDITORS
Encryption.py
hi.py C:\Users\sai...
NNstegano.py
Decryption.py
NNcipher.txt
decrypted.txt
Characters.txt
NCPROJECT
data
Characters.txt
cipher.txt
decrypted.txt
Decryption.py
Encryption.py
NNcipher.txt
NNstegano.py
samp.py
samp1.py
SecretKey.py
OUTLINE
TIMELINE
NNstegano.py > ...
148 w = modified_weights_dict[n]
149 model.get_layer(n).set_weights([w, model.get_layer(n).get_weights()[1]])
150 preds_modified = model.predict(dataset)
OUTPUT TERMINAL AZURE JUPYTER DEBUG CONSOLE PROBLEMS
None
Statistics related to the weights for ResNet152 model

Min weight: -0.833163321018219
Abs. Min weight 5.883631797910793e-13
Max weight: 0.7924034595489502
Mean of all weightd : -0.0006210239371284842

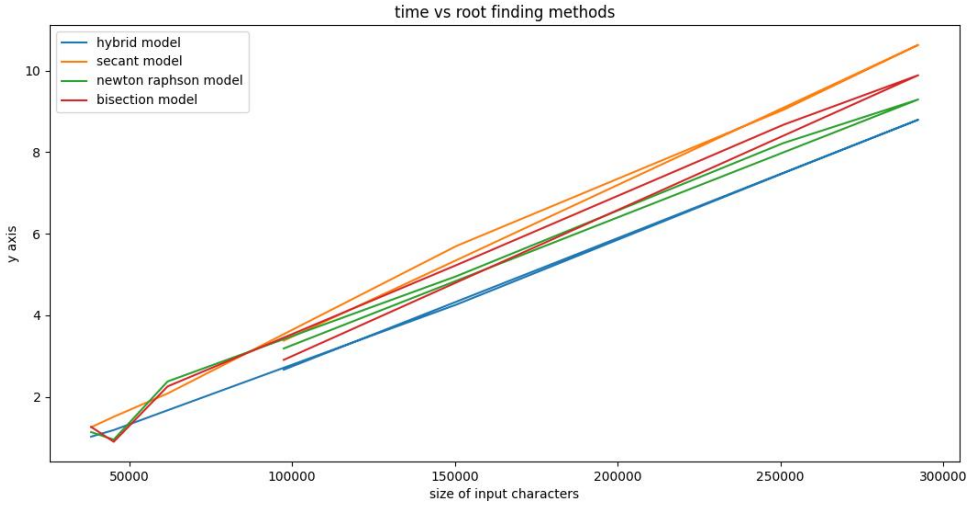
Total number of weights: 57992384
weight values < 10e-4: 5638374 - 9.7226%
weight values < 10e-3: 41370920 - 71.3385%
Total negative weights: 31829015 - 54.8848%
Total positive weights: 26163369 - 45.1152%

(Maximum) Storage capacity is 110.0 MB for the 155 layers with the 16 bits modification
We need 76562 float values to store the info
Overall number of values we could use: 57992384
Layer conv1_conv is processed, last index modified: 9407
Layer conv2_block1_1_conv is processed, last index modified: 4095
Layer conv2_block1_2_conv is processed, last index modified: 36863
Layer conv2_block1_0_conv is processed, last index modified: 16383
Layer conv2_block1_3_conv is processed, last index modified: 9809
2022-12-07 12:56:42.336308: I tensorflow/compiler/mlir/mlir_graph_optimization_pass.cc:116] None of the MLIR optimization passes are enabled (registered 2)
mean squared error value 1.4804253e-07
75.2117846012115 5
PS C:\Users\saikr\Downloads\NCProject> python decryption.py
PS C:\Users\saikr\Downloads\NCProject>
Ln 155, Col 20 (53 selected) Spaces: 4 UTF-8 CRLF Python 3.8.6 64-bit

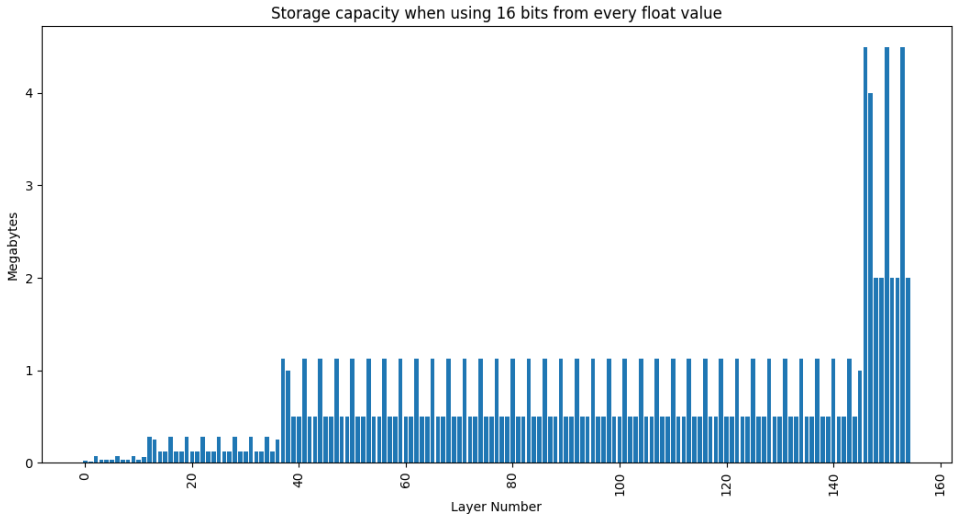
Output File:


File Edit Selection View Go Run Terminal Help
decrypted.txt - NCProject - Visual Studio Code
EXPLORER
OPEN EDITORS
Encryption.py
hi.py
NNstegano.py
Decryption.py
NNcipher.txt
decrypted.txt
Characters.txt
NCPROJECT
data
Characters.txt
cipher.txt
decrypted.txt
Decryption.py
Encryption.py
NNcipher.txt
NNstegano.py
samp.py
samp1.py
SecretKey.py
OUTLINE
TIMELINE
decrypted.txt
65 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
66 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
67 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
68 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
69 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
70 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
71 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
72 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
73 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
74 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
75 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
76 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
77 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
78 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
79 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
80 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
81 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
82 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
83 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
84 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
85 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
86 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
87 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
88 A cryptosystem is a set of algorithms, indexed by key(s), for encoding messages into cipher text and decoding them ba
89
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Plain Text

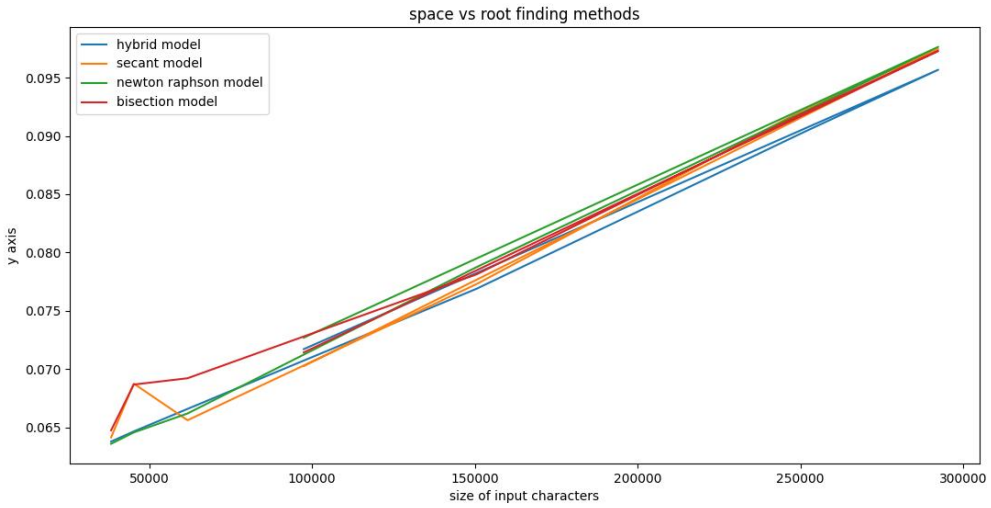
Observations and Statistics



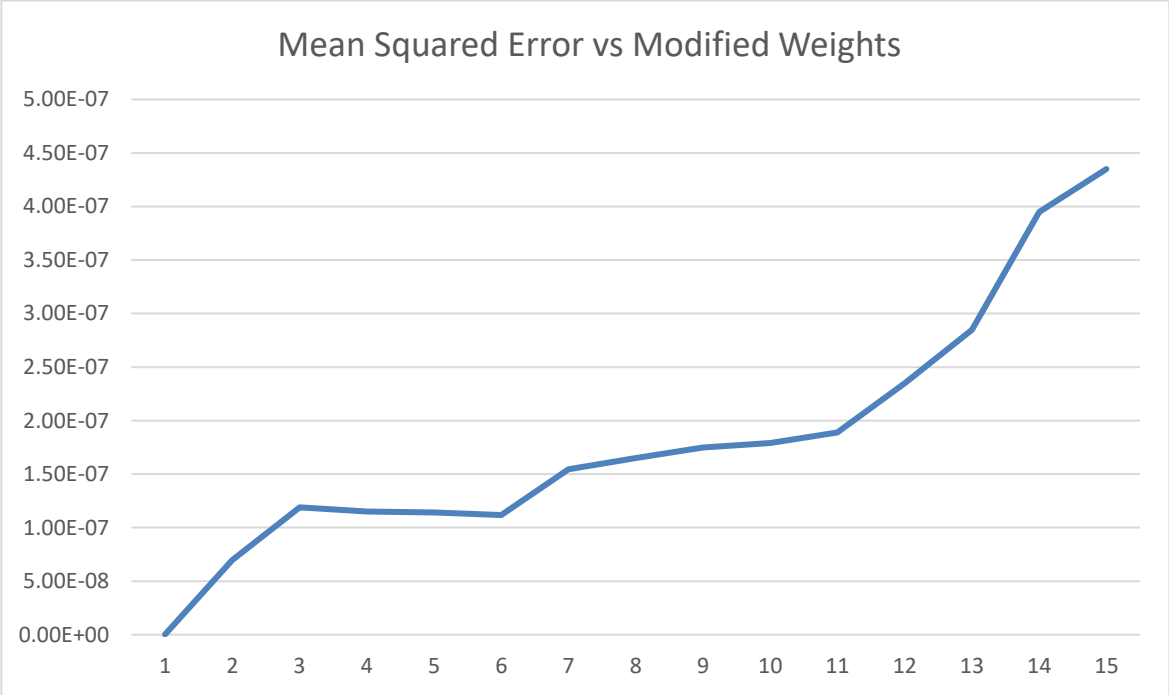
- This above graph is between the size of input characters and time. From this we can observe that our improved hybrid algorithm takes lesser time for execution from the start and continuous to perform well when compared to the secant, newton Raphson, and Bisection models.



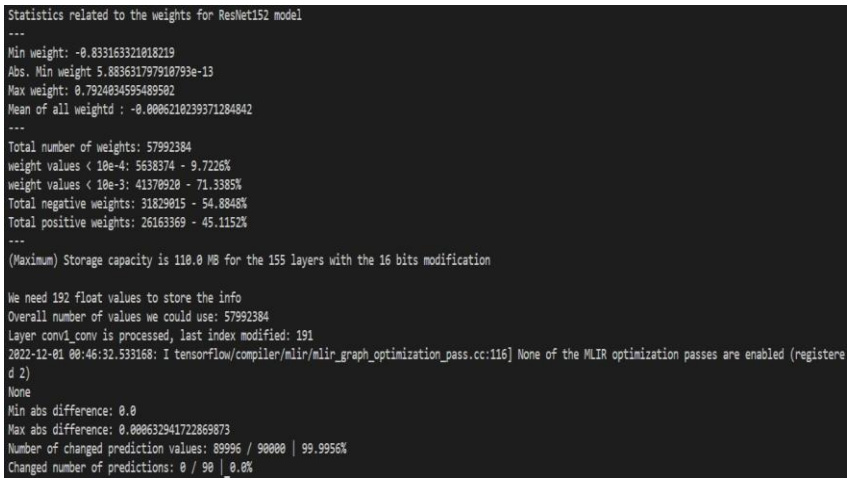
- The above graph represents the data that we can store in our neural network layers.



- This above graph is between the size of input characters and memory. From this we can observe that our improved hybrid algorithm takes lesser memory for execution from the start and continuous to require less memory when compared to the Secant, Newton Raphson, and Bisection models.



- This graph above discusses about the root mean squared error which increases as the modified weights increase in the neural network model.



- The above statistics talk about the minimum weight, maximum weigh, Mean of all weights, Absolute minimum weight, etc. about the neural network model that we are using.

Benefits

- The implemented Hybrid algorithm has a high rate of convergence and is better than the Newton-Raphson method because it can overcome the problems like Divergence, Infinite Loop, Divide by Zero, and Root Multiplicity.
- These are covered by using the Bisection method as another combination of algorithm.
- Not only that but also the Hybrid Algorithm converges to the root in a lesser number of iterations and is very much useful for complex mathematical equations.

Limitations and Future Work

- If we want to find roots for some higher derivatives, then our hybrid method computes root for only a 1st derivative. For higher derivatives there are some methods like Halley's Method, Householder's Method with the combination of bisection method to find the roots. Also, if the equation does not have any derivative, then we can use methods like Steffensen's Method, Dekker's Method, Brent's Method to find the roots. Because of the complexity of our algorithm, we don't get the rate of convergence of our improved hybrid algorithm
- By having these kinds of different numerical methods, we can generate a model which identifies the mathematical equation requirement and uses that numerical method to find the root.
- The Limitation of Least Significant Bit is that it is vulnerable to steganalysis and is not secure at all and here the alternatives would be Enhanced Least Significant Bit Replacement Algorithm.

Conclusion

In this project a new approach is proposed to secure the network by combination of cryptography and neural network steganography. The proposed algorithm is very simple in nature, more secure and less complex and this algorithm is more useful for any kind of computer configuration. Here, a secret key conception is introduced taking the idea of Improved hybrid algorithm, this algorithm converges to the root of a nonlinear equation faster than the bisection method. In addition, we show by some examples that our algorithm is more reliable than the normal hybrid algorithm. Finally, a numerical method based secret key encryption – decryption algorithm is developed using steganography to enhance the Network Security System.

References

[1] Abed Ali H. Altaee, Haider K. Hoomod and Khalid Ali Hussein, A New Approach to Find Roots of Nonlinear Equations by Hybrid Algorithm to Bisection and Newton-Raphson Algorithms, *Iraqi Journal for Information Technology,* **7** (2015), no. 1, 75-82.

[2] H. H. H. Homeier, A Modified Newton Method for Rootfinding with Cubic Convergence, *Journal of Computational and Applied Mathematics,* **157** (2003), 227-230. https://doi.org/10.1016/s0377-0427(03)00391-1

[3] Khalid Ali Hussein, Abed Ali H. Altaee and Haider K. Hoomod, Parallel Hybrid Algorithm of Bisection and Newton-Raphson Methods to Find Nonlinear Equations Roots, *IOSR Journal of Mathematics*, **11** (2015), no. 4, 32-36.

[4] D. Kincaid and W. Cheney, *Numerical Analysis*, Brooks/Cole, 1991.

[5] A. J. Maeder and S. A. Wynton, Some Parallel Methods for Polynomial Root-Finding, *Journal of Computational and Applied Mathematics,* **18** (1987), 71-81. https://doi.org/10.1016/0377-0427(87)90056-2

[6] G. Miller, *Numerical Analysis for Engineers and Scientists*, Cambridge, 2014. https://doi.org/10.1017/cbo9781139108188

[7] S. Tanakan, A New Algorithm of Modified Bisection Method for NonlinearEquation, *Applied Mathematical Sciences,* **7** (2013), no. 123, 6107-6114.

[8] Stallings, W., (2002) "Cryptography & Network Security: Principals and Practice", 3rd Edition, Prentice Hall.

[9] Menzes, A. J., Paul, C., Van Dorschot, V., Vanstone, S. A., (2001) "Handbook of Applied Cryptography", CRS Press 5th Printing.

[10] Koblitz, N., (1994) "A Course in Number Theory and Cryptography", Springer-Verlag, New York, Inc. [4] Shannon, C. E., (1949) "Communication Theory of Security System", Bell System Technical Journal, Vol. 28, No. 4, pp. 656 – 715.

[11] Ayushi, (2010) "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol. 1, No. 15, pp. 0975 – 8887.