International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 10 | Oct 2023 www.irjet.net p-ISSN: 2395-0072

Cryptanalysis of Cipher texts using Artificial Neural Networks: A comparative study

Jaeson Karter Joseph[1], Ritu[2], Shresth Dewan[3]

[1]*Jaeson Karter Joseph, School of Computer Science Engineering, Vellore Institute of Technology, Vellore*
[2]*Ritu, School of Computer Science Engineering, Vellore Institute of Technology, Vellore*
[3]*Shresth Dewan, School of Computer Science Engineering, Vellore Institute of Technology, Vellore*

Abstract - *In the present times where everyone is using the Internet to connect with people, socialize with them, share some information or to even find some information regarding anything or everything, the information one needs is available on the Internet. When everyone is using the Internet which is available to everyone, it is a threat to an individual's privacy and the individual's information stored on the Internet. As per the report by Cybersecurity ventures in 2019, the number of cyber-attacks is 158,727 per hour, 2,645 per minute and 44 attacks every second all around the world. To protect the data and information companies use cryptographic algorithms and security software's. The neural networks are used in various fields like weather forecasting, fraud detection, risk assessment and many due to its ability to mimic human operations and predict relationships between the vast data provided. Through Cryptography the integrity of data is ensured by using hashing algorithms and message digests. It is done by adding codes and digital keys to ensure that what is received is genuine and is from the intended sender, the receiver is assured that the data received has not been tampered with during transmission, thus making the data reliable.*

Key Words: Cryptography, Artificial Neural Networks, CNN (Convolutional Neural Network), Hash functions, RNN (Recurrent Neural Network), FC NN (Fully connected Neural Network)

1. Introduction

Cryptanalysis is a highly studied field with lots of active research going on to find better solutions to crack down the complex ciphers built over time such as DES, AES, blowfish cipher, RSA, improve the weaknesses of ciphers being developed, and improve the current systems deployed in various organizations relating to military, government, public data, and confidential data incorporates.

With the advent of Machine Learning approaches and Deep learning-based implementations, cryptanalysis has got a new face of exploration, with many advantages over the old techniques, such as brute force, statistical analysis, differential analysis, etc., in terms of speed, search space, and efficiency in general.

As these techniques mature with time, we can expect lots of improvement in the results that we currently get by using different techniques of classification of cryptographic algorithms used, generations of keys, or finding the characteristics of the plaintext data.

Our project proposes to perform the currently available neural networks, with varying configurations in terms of their designs, hidden layers, and the number of neurons in them. We look forward to performing an analysis of the ciphertext to gauge the algorithm used to generate the ciphertext and the type of plaintext used such as whether a text input was used or a binary one.

This will help us to compare the varying efficiencies of different neural networks like RNN, LSTM, which maintain the varying amount of state data from the past, and CNN which helps with deeper analysis of graphics, speech, and natural language.

2. Literature Survey

[1]The paper throws a light on the commonly used techniques in analyzing the symmetric ciphers using techniques such as boomerang technique (which does a differential analysis of the cipher and the plain text when some amount of the plain text is changed), brute force attack (generates all possible keys and compares the cipher text to the plain text or the semantic analysis of the generated plain text), linear cryptanalysis (to find subkeys in different rounds by doing a statistical analysis of the randomness trying to reduce it, by using a large number of cipher and plain texts.). The cryptanalysis used in the system helps with the analysis of the complexity of the various ciphers employed by various organizations, to see if they are well protected against attackers. It can be also used to check the usage of new ciphers being developed and in counteracting against illegal organizations. There are some advantages to some techniques over others, like

some provide lesser time complexity, while some provide completeness and deterministic results.

Performing cryptanalysis, requires large computation power, and vast amounts of data in the form of plaintext - ciphertext pairs, for getting meaningful results and still would be very difficult to perform on advanced ciphers like AES.

[2] DL based framework, and designs a DNN, using the TensorFlow library. The attack on simple ciphers like S-DES, Simon and speck ciphers is performed to find the text-based key used in the above ciphers. The S-DES cipher was broken with a success probability of ~0.9, and ~2^8 given cipher texts which reduces the search space by a factor of 8. Similarly, the Simon and speck algorithms were broken and 56 bits of plaintext with about ~2^12 given plaintexts. The key-space was restricted to a text-based key, which is uncommon which was done so that it is easier to find meaningful relations between input and output texts. If the key space was not limited then the DL based approach failed to attack the block ciphers.

[3] Feedforward BP neural network and cascaded feedforward BP neural networks are used to carry out the experiment. Multiple layers (~4) of varying number of neurons are used in the BP neural network with a mean square error (MSE) error function and the limit is set at 0.05. Attack difficulty and data requirements are reduced in using a Neural Network based approach for cryptanalysis. Neural networks can easily simulate the black box problem that cryptanalysis poses. It approaches the cryptanalysis problem, and finally get the algorithm equivalent to the encryption and decryption algorithm. Also,

Neural networks can effectively achieve the corresponding Cryptanalysis results with smaller datasets. The technique of using Artificial neural networks for cryptanalysis is relatively new and doesn't provide highly accurate results for complex block ciphers. Also, information regarding the cipher text may not always be available like the algorithm used, etc., and this leads to larger search space and more randomness in the estimation of the keys and plaintext.

[4] Performance analysis could be done with measures like analysis of MARS and AES, Speed comparison with encryption and decryption cycles, key setup and key initialization, analysis of various key sizes, and fair speed. Rijndael is more secure and strong when compared to the MARS algorithm. Mars is not suitable for Smart card implementation.

[5] Using the Hopfield neural network to generate binary sequences and proper masking of plaintext by permutation and calculation of generated binary sequences.

It is fast, efficient and more practical in the secure transmission of large multimedia files over public data communication network

3. Overview

Cryptography has come a long way from its beginnings in 1900 BC to current day advanced cryptography systems using complex mathematics and resilient implementations to protect the large amounts of data being produced in today's society. As we continue our journey in the data driven world, so does the need to combat new data protection problems arise and the research for better algorithms continue.

Cryptanalysis is one such threat to cryptography algorithms and it is the process and study of finding vulnerabilities either in the mathematics of the algorithm itself or the implementation of those algorithms.

With the ever-increasing amount of data, we have newer techniques to deal with the cryptanalysis of such data, which involves using ML models to find patterns in the ciphers, which helps in deciphering and code-breaking encrypted messages.

The goal of using Machine learning is to identify the type of cryptographic function used based on the input and output parameters, finding the secret key, etc.

4. Proposed System and Results

Here we propose to find out the accuracy of correctly predicting certain characteristics of the original plaintext using different neural networks, with varying numbers of hidden layers in the network.

Some random data is generated using a dictionary data set, and that is encrypted using different encryption algorithms. The encrypted data is then used to predict the characteristics of original data such as, the type of input data (binary or UTF-8 format) and the cipher function used.

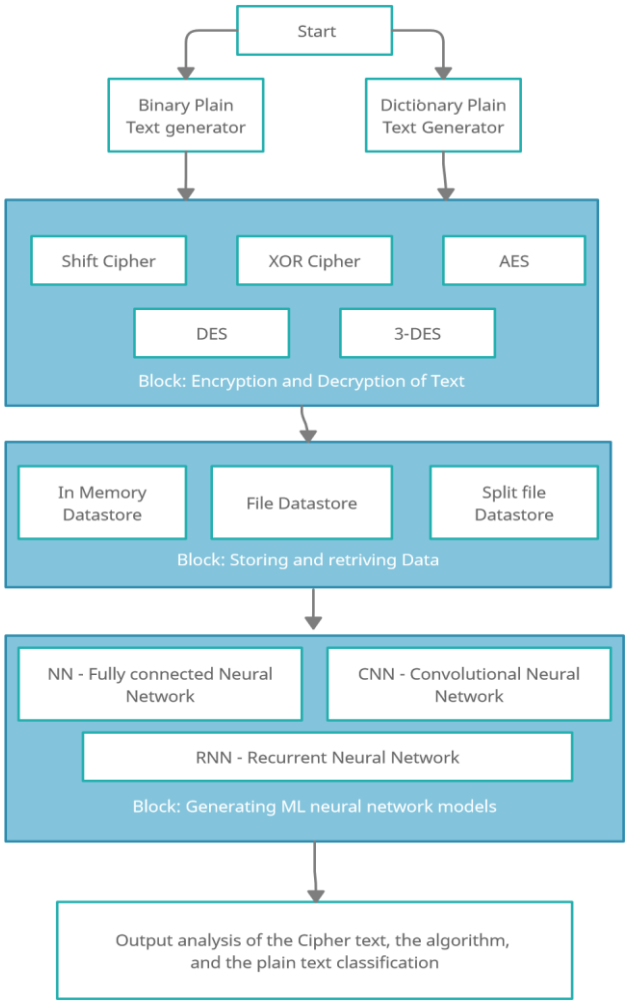

Fig -1: Flowchart of the proposed model

A series of trials were carried out on cipher texts using artificial neural networks to check whether the developed system can predict the cryptographic algorithm used on the plain text to obtain the input cipher text, or the type of input text. The following results were obtained during the trails:

Table-1: Result Obtained

S. No.	Test	Cipher used	Result
1.	Plaintext classification - FC NN with 1 hidden layer	N.A.	100% accuracy was achieved
2.	Cipher text classification - FC NN with 1 hidden layer	Shift Cipher	100% accuracy was achieved
3.	Cipher text classification - FC NN with 1 hidden layer	XOR Cipher	100 % accuracy was achieved
4.	Cipher classification - FC NN with 5 hidden layers	SHIFT and XOR cipher	100% accuracy was achieved
5.	Cipher text classification - FC NN with 5 hidden layers	AES cipher	54% accuracy was achieved
6.	Cipher text classification - FC NN with 5 hidden layers	DES cipher	70% accuracy was achieved

5. Conclusion

In today's world, when any information can be easily found on the internet, it is important to protect the information regarding any individual such as their bank account information, the passwords, their day-to-day activities, etc. This is when cryptography plays a predominant role and helps the companies to ensure their customers' information is safe and not exploited by anyone. Cryptography in the digital world is able to offer the protection for an individual's data from an unauthorized use of your data and fraud. Cryptography grants people the right to carry over the confidence found in the physical world to the electronic world. It ensures people the safety to do business electronically without worries of deception. Cryptography along with the neural networks strengthens the security and builds the confidence of people about using the internet without the fear of someone exploiting their information.

6. References

1. International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-3, Issue-2, May 2013

2. Hindawi Security and Communication Networks Volume 2020, Article ID 3701067, https://doi.org/10.1155/2020/3701067

3. Hindawi Security and Communication Networks, Volume 2018, Article ID 6868506, https://doi.org/10.1155/2018/6868506

4. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814 www.IJCSI.org

5. Chaotic neural network, received 15 March 1989, Revised 2 October 1989, Accepted 9 January 1990, Available online 28 August 2002, Communicated by A.P. Fordy