IHJPAS. 36(1)2023

Ibn Al-Haitham Journal for Pure and Applied Sciences

Journal homepage: jih.uobaghdad.edu.iq

Block Ciphers Analysis Based on a Fully Connected Neural Network

Ali H. Alwan
Department of Computer Sciences , College of Science, University of Baghdad, Baghdad, Iraq.
ali.hussein1201a@sc.uobaghdad.edu.iq

Ali H. Kashmar
Department of Computer Sciences , College of Science, University of Baghdad, Baghdad, Iraq.
ali.kashmar@sc.uobaghdad.edu.iq

Article history: Received 10 October 2022, Accepted 6 November 2022, Published in January 2023.

doi.org/10.30526/36.1.3058

Abstract

With the development of high-speed network technologies, there has been a recent rise in the transfer of significant amounts of sensitive data across the Internet and other open channels. The data will be encrypted using the same key for both Triple Data Encryption Standard (TDES) and Advanced Encryption Standard (AES), with block cipher modes called cipher Block Chaining (CBC) and Electronic Codebook (ECB). Block ciphers are often used for secure data storage in fixed hard drives, portable devices, and safe network data transport. Therefore, to assess the security of the encryption method, it is necessary to become familiar with and evaluate the algorithms of cryptographic systems. Block cipher users need to be sure that the ciphers they employ are secure against various attacks.

A Fully Connected Neural Network (FCNN) model was initially used to assess how well the models were classified. Then, all models, including encoder models, were assessed using True Positive (TP) measures for successful classification of the discovered encoder and False Positive (FP) measures for imprecise categorization. The accuracy value, retrieval, loss, precision value, and F1 score were then calculated using a confusion matrix to assess the model's efficacy (abbreviated as F1). ECB results with an accuracy of 85% and CBC results with an accuracy of 88% were produced, and the parameters of the FCNN model were tweaked to provide better results. These results helped to identify the encryption algorithm more precisely and evaluate it.

Keywords: FCNN Models, Diagnosis, Analysis, Symmetric Key, Block Cipher.

1. Introduction

Numerous cryptanalysis methods now in use are intended for specific encryption algorithms. As a result, one of the most crucial tasks for cryptanalysis in the era of large data is identifying encryption methods. The ability to resist the encryption algorithm can be used to gauge an algorithm's security, offering a useful benchmark for algorithm creation. The majority of

This work is licensed under a Creative Commons Attribution 4.0 International License

classification techniques currently in use are based on statistics and machine learning. The primary functions of statistical methods are the classification and identification of associated statistical indicators, such as the frequency of occurrence of letters. The deep learning approach compares categorizing algorithms to other typical classification tasks. Deep learning techniques are used to conduct most current research [1].

The ciphertext alone is supposed to make it harder to identify the encryption algorithm. Only some papers in this field take block ciphers or symmetric key ciphers into account [2]. The encryption algorithm is determined by cryptanalysis of the encrypted text the invaders sent. It is challenging to infer the encryption algorithm being used only from the ciphertext. The majority of the time, techniques based on statistics and deep learning are taken into account when attempting to decipher the encryption algorithm from the ciphertext. Statistical approaches used the frequency of occurrence of alphabetic elements and their n-grams. In deep learning-based approaches, the encryption algorithm is determined [3,4].

In fact, a cryptanalyst frequently needs to learn which cryptographic technique is used while deciphering particular cipher messages. The first task for a cryptanalyst, is to determine the cryptographic algorithm of the cipher text. The cryptanalyst can then use several methods to decipher the encrypted text, such as brute force, dictionary, rainbow table, math, etc. **Figure 1** shows how an identification system for encryption methods works with merely ciphertext knowledge [5].

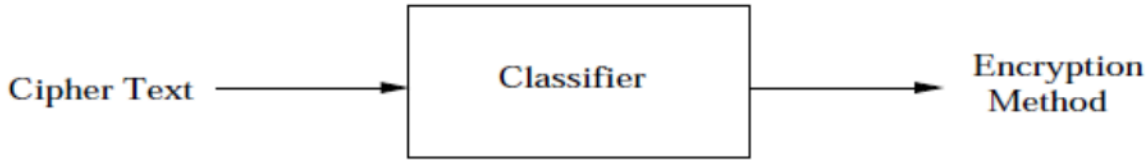

Figure 1. Recognition of an encryption technique from a ciphertext [6].

This paper reviews three encryption algorithms—AES, 3DES, and Blowfish—that operate in pattern mode (CBC) and mode (ECB) of cryptographic techniques. Our detection methodology is built on the Fully Connected Neural Network (FCNN) technology, a type of deep learning-based method, which includes additional modes like Output Feedback Mode (OFB), Cipher Feedback Mode (CFB), and Counter mode (CTR). The form must first be used to extract the features of each ciphertext. After entering the ciphertext into the identification form, it can establish the proper encryption algorithm.

Nonetheless, DL models can be utilized as ways to accomplish these jobs more effectively and to aid in the goal of diagnosis and analysis, which is important in this discipline. The techniques used can be examined to ciphertext using this trained or learned model. An example would be a program that could be trained and tested using various classifiers to detect and analyze the cryptographic techniques employed. This research focuses on using DL techniques to perform cryptanalysis on block ciphers in general. This investigation aims to diagnose and analyze the cryptography algorithms utilized to generate the ciphertext message [7].

Background

Below are some brief explanations of deep learning and Symmetric Key Algorithms, the two particular models he utilizes in this research that have various architectures.

2.1 Deep Learning

Different deep networks make up deep learning models. Among them, unsupervised learning models include autoencoders, Restricted Boltzmann Machines (RBMs), and Generative Adversarial Networks (GANs). Deep brief networks (DBNs), deep neural networks (DNNs), convolutional neural networks (CNNs), and Rurrent Neural Networks (RNNs) are supervised learning models, as shown in **Figure 2**. The amount of deep learning experiments using the identification of encryption schemes has grown significantly in recent years. Without the need for manual feature engineering, deep learning models immediately learn feature representations from the original data, such as images and texts. Deep learning techniques can therefore be used end to end. Deep learning techniques significantly outperform shallow models for massive datasets. Network design, hyperparameter selection, and optimization approach are the three main focuses of deep learning research [8].

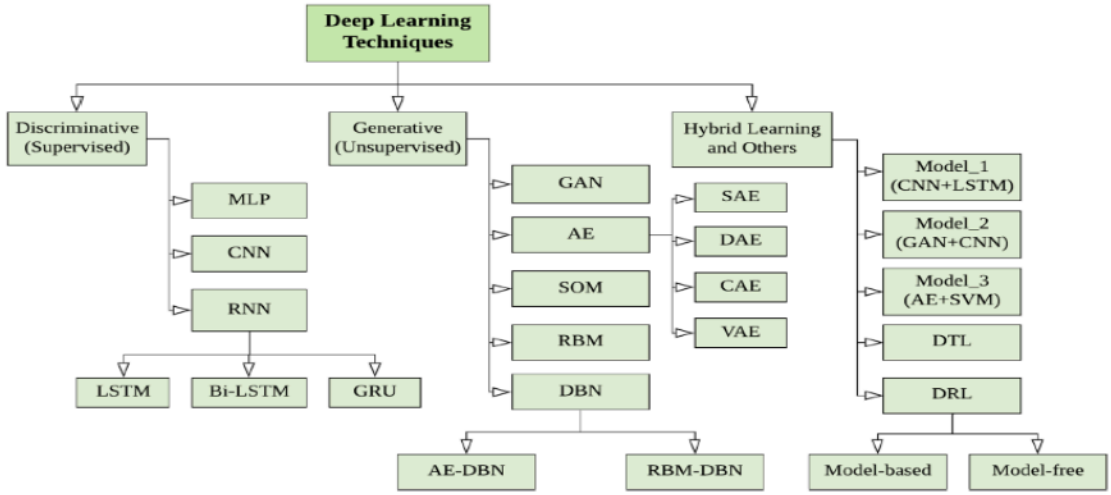

Figure 2. Type Deep Learning Techniques [9].

2.2Symmetric Key Algorithms Used with in Our Experiments

2.2.1 Blowfish

Bruce Schneier invented blowfish. Although it uses symmetric keys and is similar to DES, the key size can range from 32 to 448 bits. It is a block cipher of 64 bits. The two components of the blowfish algorithm are key expansion and data encryption. Prior to the data encryption procedure, there is a step called "key expansion" when the key is divided into numerous subkeys. A Feistel function is used in the data encryption process and is repeated 16 times or 16 rounds, of the method. A key-dependent permutation and a key-and-data-dependent replacement are both used in each cycle. The S-array uses the four bytes that the Feistel function divides from the 32-bit input as its indices. The lookup results are added, and their XOR operation is carried out to produce the output [**10]**

2.2.2 Advanced Encryption Standard (AES)

NIST introduced AES or Rijndael in 2001. A 4*4 matrix, commonly referred to as a state matrix, is used by AES. It is a symmetric key algorithm that runs for 10, 12, and 14 cycles with

keys of 128, 192, and 256 bits, respectively. AES divides the data into four blocks or an array of bytes that create 4*4 matrices to perform rounds. AES has three rounds: an initial round, a final round, and a key expansion. AES uses permutations and combinations in each round. The same procedures must be carried out on the state matrix during every AES cycle except the final one. The following are these operations [10]:

Substitute Bytes: These comprise processes built on specially created substitution boxes. This operation's primary goal is to stop numerous attacks, including mathematical attacks, differential cryptanalysis, and linear cryptanalysis.

Shift Rows: This basic linear procedure is carried out on state matrices. The procedure is carried out with the intention of causing diffusion.

Mix Columns: Similar to the shift row operation, this is likewise a fundamental operation. Matrix multiplication is involved.

Add round Key: This simple procedure conducts an exclusive operation between the state matrix and the key of that round. This operation's goal is to cause confusion [10]. The outcome is applied in the following round.

2.2.3Triple Data Encryption Standard (Triple-DES)

Similar to how technology advances. There were various cryptanalytic attacks, such as Brute force, which broke the key to deciphering the ciphertext, limiting the use of DES. To prevent these attacks, the DES cipher was reconfirmed as the triple data encryption standard (3DES), using the DES cipher three times, i.e., enciphering -decryption- enciphering to encipher the 64-bit plain text into a 64-bit cipher text. This can be done using a 192-bit key composed of Key 1, Key 2, and Key 3 of 64-bit each for enciphering, deciphering, and enciphering, respectively, as depicted in **Figure 3** [11].

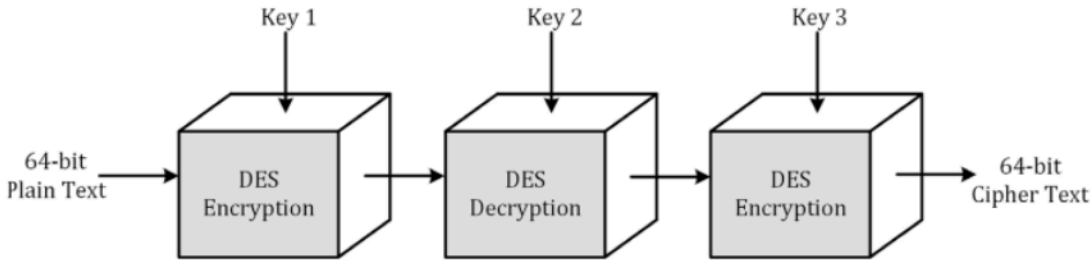

Figure 3. Triple Data Encryption Standard of block diagram [11].

2. Related works

Nagireddy, S. **In (2019)** [12]: The proposal in this study, "Identification of the encryption techniques of block ciphers," is a type of cryptanalysis attack. This is the main attack used to evaluate how secure block ciphers are. This task has two issues: (1) identifying the encryption model. (2) Determining the encryption methods used by block ciphers is a pattern classification issue. Early methods for identifying patterns in block ciphers included the histogram matching approach, Support Vector Machines (SVM), and Gaussian mixture models. To create a variety of attack methods, including ciphertext-only assault, known-plaintext attack, and side-channel attack.

Hu, X.; Zhao, Y. **In (2019, February)** [13]: The outcomes show that ciphertext data may be successfully extracted using the created features. This study developed a novel methodology by building a feature based on ciphertext recombination and location detection. Eight block ciphers of the Electronic Codebook mode (ECB) and eight Cipher Block Chaining mode (CBC) were classified using a random forest classifier. In ECB mode, eight algorithms can classify objects with more than 87% accuracy. Additionally, it can classify more accurately in CBC mode than at random.

Kopal, N., **In (2020, May)** [14]: The proposed cryptanalysis in this research has developed an artificial Neural Network that is now able to recognize five classical ciphers: simple monoalphabetic substitution, Vigen'ere, Playfair, Hill, and transposition. The network is based on Google's TensorFlow library as well as Keras. This paper presented the current progress in the research on using such Artificial Neural Networks (ANN) to diagnose the cryptography type. Artificial neural networks (ANN) can categorize about 90% of the ciphertexts correctly. Using an artificial Neural Network provides 54% computation time for categories of cipher kinds.

Yang, W.; Park, Y. **In (2021, Jan)** [15]: This study presents a new technique to identify symmetric key algorithms using a Convolutional Neural Network (CNN) for traces extracted from Intel Processor Trace (IPT). The IPT interrupts the running of software. The IPT is used to remove the trace that has been symmetric key ciphered first. It is then transformed into an image and fed into CNN. Two different datasets were used for the experiment. The training results from the first dataset, which contained traces extracted using various symmetric key algorithms, were categorized into nine classes with 100% accuracy. The second dataset contained traces for each type of symmetric key algorithm, along with the block cipher modes and various bit sizes of the security keys. The accuracy of the classification of the training results into 36 classes was 70.55 percent. This study used a CNN to determine the number of key bits and the block-cipher modes in addition to the types of encryption algorithms that studies have previously identified.

3. Proposed model

This study suggests a deep learning strategy for determining the encryption algorithm from the cipher text, using the algorithm Fully Connected Neural Networks (FCNNs). The deep learning strategy is suggested for determining and analyzing the encryption algorithm (secret key) from the cipher text using the Fully Connected Neural Networks model (FCNNs). The fully connected Neural Network model (FCNN), a multi-layered feedforward Neural Network model, is one of the most important deep learning models. FCNN uses the spatial concept to extract characteristics. FCNN is better able to classify and more efficient in using big data and reducing complexity and can store training data. Text categorization problems today frequently employ this network design. A fully connected layer multiplies the input by a weight matrix before adding a bias vector. One or more fully connected layers are added after the convolutional (and down-sampling) layers. As the name implies, every neuron in a fully connected layer connects to every neuron in the layer above it. FCNN is the last layer in CNN that performs classification. It delivers the results and communicates the activation function "SoftMax," where FCNN has more layers like a multiple-layer perceptron, as shown in **Figure 4,** fully connected Neural Network model.

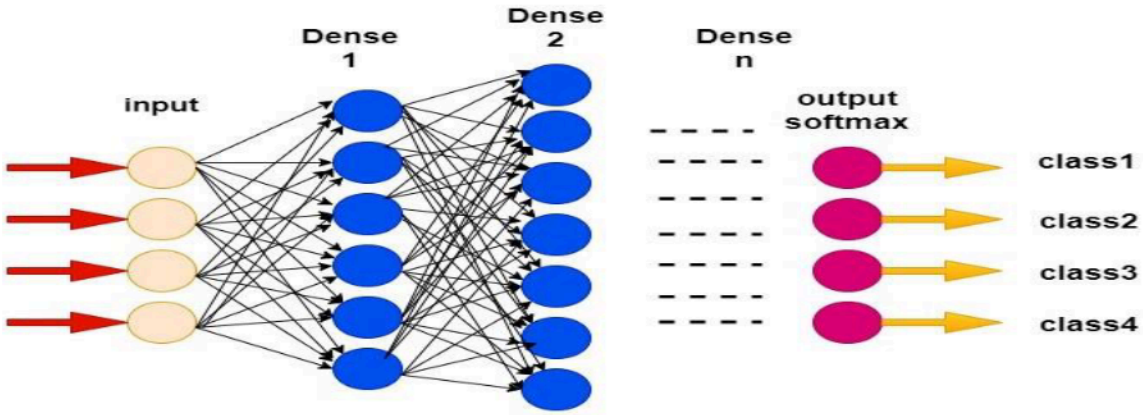

Figure 4 .Structure Fully Connected Neural Network.

4. Experimental Process

4.1Data Set

In this research, cipher texts retrieved from the Kaggle website containing ciphertext and plaintext, an unlabeled dataset [16], will be used to construct the ciphertext from plaintext data and encrypt data with both the same key and different keys using encryption algorithms. The data will be encrypted and stored in a dictionary, with an 80% discount for training data and 20% for testing taken from ciphertexts in the dataset for the test. After the model is trained and run, the unlabeled dataset will be entered to evaluate the model using a confusion matrix to determine the coding algorithm.1,000 samples were randomly chosen from a selection of 45,133 samples for this study. The unlabeled dataset will be entered after the model has been trained and tested. The model can be assessed using the confusion matrix to identify and analyze the cryptographic technique.

4.2.System model

The deep learning algorithm Fully Connected Neural Network (FCNN) was applied. Preparing encrypted data for the Fully Connected Neural Network model's training, cross-validation, and testing was the first step in the experiment. Then, the forms were evaluated using a set of accurate measurements. in Fully Connected Neural Network model using the activation function SoftMax. When applying FCNN to classification issues, some common model parameters can be changed. This includes the number of layers and adjusting the weights. To maximize form development, the learning rate could also be modified during the training phase. These were modified as part of the experiment design and model optimization. However, the depth of the forms was modified or, more precisely, raised to assess the efficacy of deeper forms because one of the research hypotheses is to investigate the effects of deep learning algorithm depth on this classification problem. Deep architecture is the essential FCNN characteristic. Other recent studies show that the more profound the layers, the better the algorithms detect minor patterns in encrypted data. The number of hidden layers also increases as training rounds. Each model was trained over 100 epochs and 1000 samples. The limited research resources available and the lengthy training period were the main reasons for the short training cycle. The validation loss and accuracy reach saturation by the middle of the training stage, where the following training visualization group demonstrates that the training epochs are adequate. The form responded fast to the training dataset due to the pre-training model setup. As illustrated in **Figure 5**, the data is preprocessed before being utilized for training the FCNN network. The feature information retrieved by FCNN, as well as the FCNN outputs, are then classified by SoftMax.

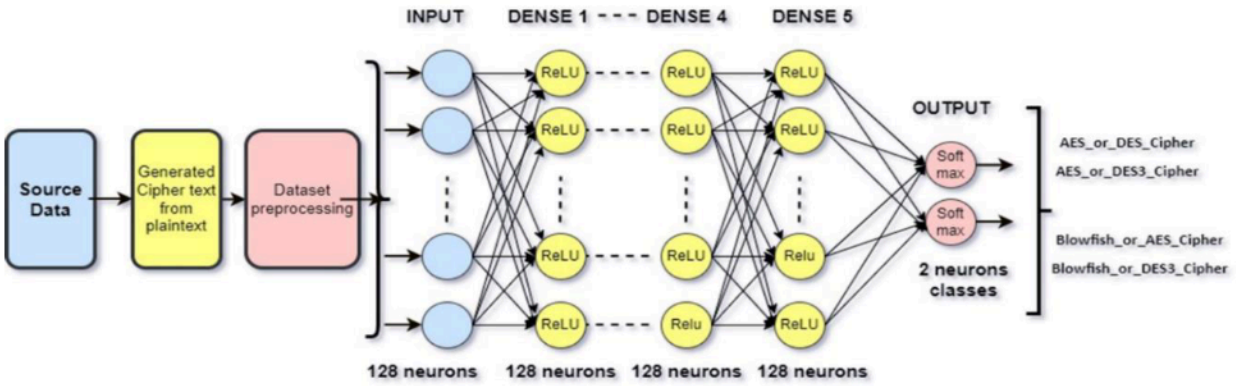

Figure 5. Structure Diagram Fully Connected Neural Networks (FCNNs)

AES, 3DES, and Blowfish are three encryption algorithms that cooperate with the block cipher modes of the process cipher algorithms. In this study, we explore the cryptographic cipher Blockchain mode (CBC) and Electronic Cipher Book mode (ECB) using the same encryption key. Our detection algorithm is also built using fully connected Neural Network (FCNN) technology, a deep learning technique. We must first utilize the model to extract each ciphertext's feature. Once the ciphertext has been entered into the identification form, it is feasible to choose the proper encryption algorithm. The results show that performance is good when utilizing the same key in cipher using the proposed method in the diagnostic and analysis of symmetric key cryptosystems. It indicates that the suggested approach produces good results.

Regular fully connected neural networks model will build a dense FCNN of n layers. The model workflow is shown in algorithm 1. Its structure will consist of 5 hidden layers, each layer consisting of 128 neurons, hidden layers activation Relu except for the output layer, which consists of two classifiers and used activations SoftMax, as displayed in **Figure 6** and **algorithm 1**.

Figure 6. Structure FCNN model.

ALGORITHM 1: DIAGNOSIS AND ANALYSIS FOR SYMMETRIC KEY CRYPTOSYSTEM

INPUT	Dnn algorithm, encryption algorithm 1 and encryption algorithm 2
OUTPUT	Metrices and confusion matrix.
STEP 1	Fcnn algorithm type, encryption algorithm 1 and encryption algorithm 2, get data from the dataset.
STEP 2	Generate random plaintext (paragraph) 1000 to 3000.
STEP 3	Generate cipher from plaintext for two crypto algorithms at the same time by using the same key, different key.
STEP 4	Get cipher text generated (en1+en2), number of trains (epoch) 50, number of steps in each train (iteration) 100,
STEP 5	Get cipher from dataset for test
STEP 6	Evaluate trained test results
STEP 7	Optimized results
STEP 8	Show final results
STEP 9	End

5. Evaluation

The trained models were evaluated or tested using a test data set that used a confusion matrix, the same set of cryptographic algorithms that will use the same key at random. Furthermore, it will be used with block cipher modes of operation used in cryptography, including the Cipher Block Chaining (CBC) mode and electronic codebook (ECB) mode. The evaluation was carried out using three different encryption systems. The comparison list used in the test is shown in **Table1**.

Table 1 .The Test's Comparability List

Cipher Block Chaining (CBC) mode Electronic Codebook (ECB) mode
Blowfish or_ AES _Cipher Same key
Blowfish_or_3DES_Cipher Same key

A confusion matrix can be utilized to test how successfully classification algorithms can analyze symmetric key methods, identify them, and categorize the many kinds of encryption algorithms identified. The columns denote the actual class, and the rows the anticipated class. The confusion matrix's TP and TN values represent the proportion of accurate positive and negative classifications. FP and FN represent the proportion of incorrectly identified negative and positive instances. The confusion matrix can display a number of widely used metrics for rating the classifier's performance at various evaluation levels [17].

$$PRECISION = \frac{TP}{TP + FP} \quad (1)$$

$$RECALL = \frac{TP}{TP + FN} \quad (2)$$

$$ACCURACY = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

$$F1 = 2 * \frac{PRECISION * RECALL}{PRECISION + RECALL} \quad (4)$$

$$misclassification = \frac{FP + FN}{TP + TN + FP + FN} \quad (5)$$

In this work, three encryption techniques' categorization tests were used. Multiclass categorization can easily be performed by extending this. The classification results were examined once the tests were finished to evaluate the effectiveness of the taught forms. The categorization of all forms is assessed in the first set of analyses. The tables below indicate the evaluation of the confusion matrix for the fundamental models utilized in this research, accuracy, and loss, as well as the most secure modes and algorithm by applying the suggested approach (FCNN) to identify and analyze the symmetric key algorithm.

By applying an FCNN to the Blowfish vs. AES model with the same key and employing CBC mode and ECB mode block ciphers, this study proved the viability of identifying symmetric key techniques. Using the same key and CBC mode, the accuracy in classifying the different symmetric key algorithms was 81%, and the loss was 41%, as shown in **Figure 7** and **Table 2** below.

Table 2. Blowfish vs AES _Cipher Same key_ CBC Mode

Accuracy	Loss	Precision value	Recall	F1-score	Support
0.81	0.41	0.81	0.81	0.81	1000

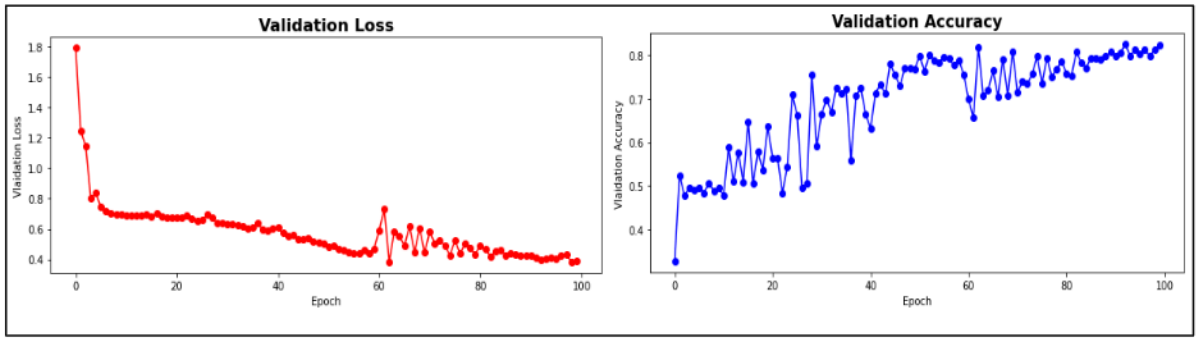

Figure 7. Accuracy and Loss AES_or_DES_Cipher_Same key_ CBC Mode

Figure 8 illustrates this. The confusion matrix is a (N x N) matrix used to assess the performance of a categorization form, where (N) is the number of target classes. An individual could determine the model's accuracy by observing the diagonal values for measuring the number of correct categorizations by visualizing the confusion matrix. The model has proven to be successful.

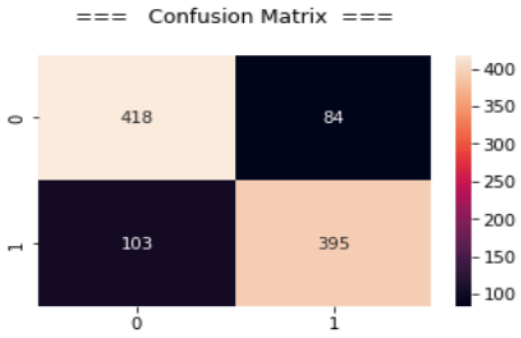

Figure 8. Confusion Matrix Blowfish vs AES _Cipher Same key_ CBC Mode

Furthermore, **Table 3** demonstrates the possibility of detecting symmetric key algorithms by using an FCNN on the Blowfish vs. AES model, which uses the same key with the ECB mode block cipher. As shown in **Figure 9**, the performance was 81 % accurate in identifying the types of symmetric key algorithms using the same key with ECB mode, and 40 % loss. Furthermore, as shown in **Figure 10**, a confusion matrix was used to determine whether the model was successful.

Table 3. Blowfish vs AES _Cipher Same key_ ECB Mode

Accuracy	Loss	Precision value	Recall	F1-score	Support
0.81	0.40	0.81	0.81	0.81	1000

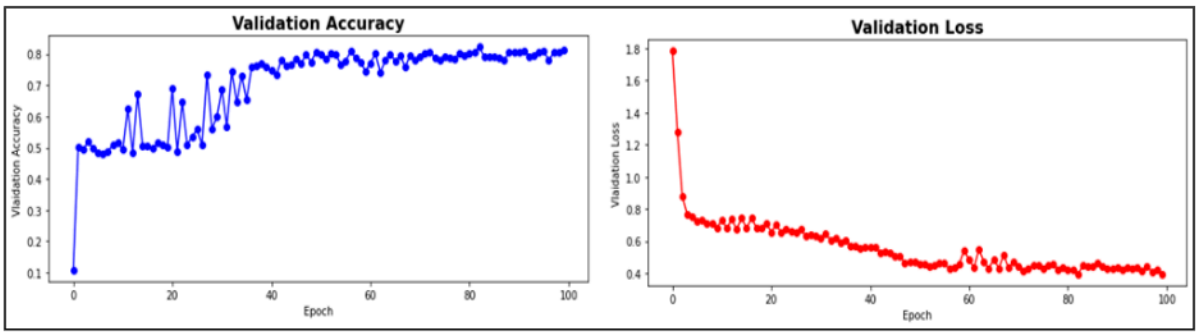

Figure 9. Accuracy and Loss Blowfish vs AES _Cipher Same key_ ECB Mode

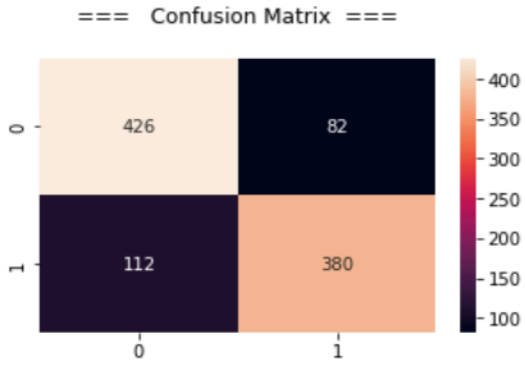

Figure 10. Confusion Matrix Blowfish vs AES _Cipher Same key_ ECB Mode

The ability to detect symmetric-key algorithms is shown in Table 4. The same keys are used with CBC mode block ciphers by Blowfish vs. 3DES. Accuracy in classifying the various symmetric key algorithms using an identical key and CBC mode was 88%. There was a loss of 30%, according to **Figure 11**.

Table 4. Blowfish_or_3DES_Cipher_Same key_ CBC Mode

Accuracy	Loss	Precision value	Recall	F1-score	Support
0.88	0.30	0.88	0.88	0.88	1000

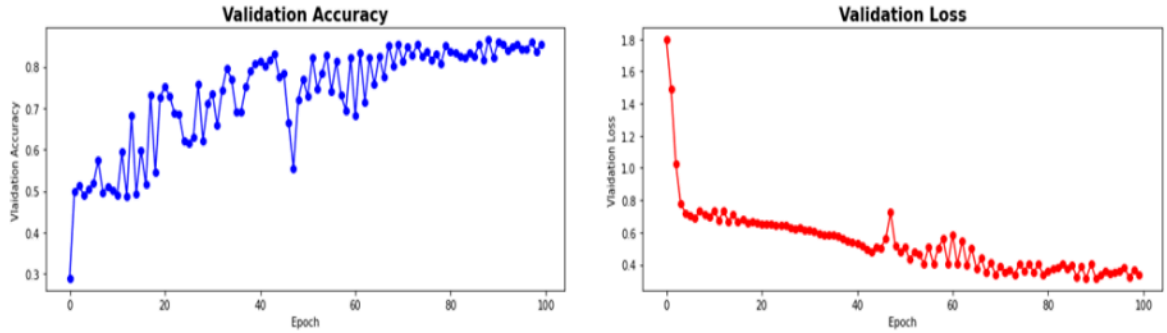

Figure 11. Accuracy and Loss Blowfish_or_3DES_Cipher_same key_ CBC Mode.

A confusion matrix was also used to evaluate the model's effectiveness, as shown in **Figure 12**. One might assess the model's correctness by displaying the confusion matrix and observing the

diagonal values for the number of correct categorizations. The efficacy of the model has been established.

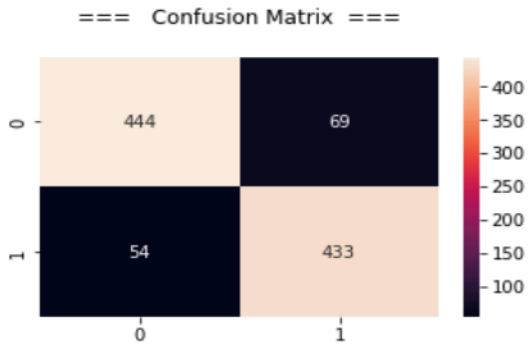

Figure 12. Confusion Matrix Blowfish_or_3DES_Cipher_same key_ CBC Mode

Table 5 displays the potential for finding symmetric key algorithms. With CBC mode block ciphers, Blowfish vs. 3DES using the duplicate keys. The performance showed an accuracy of 85%, a loss of 34%, and high accuracy in identifying the types of symmetric key algorithms, as depicted in **Figure 13**.

Table 5. Blowfish_or_3DES_Cipher_Same key_ ECB Mode

Accuracy	Loss	Precision value	Recall	F1-score	Support
0.85	0.34	0.85	0.85	0.85	1000

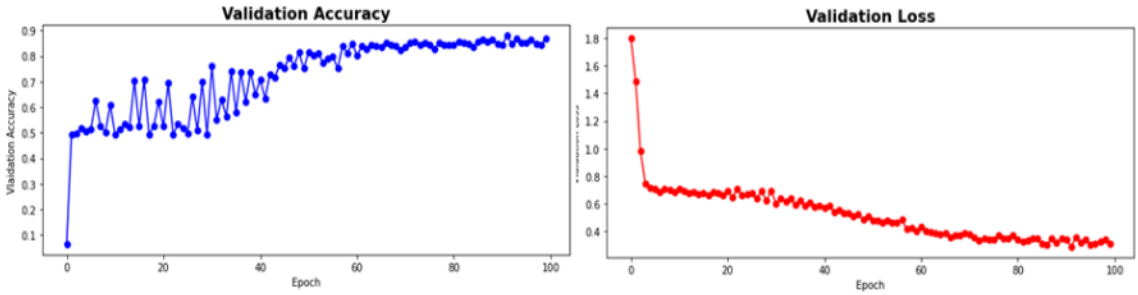

Figure 13. Accuracy and Loss Blowfish_or_3DES_Cipher_Same key_ ECB Mode.

As illustrated in **Figure 14**, a confusion matrix was also utilized to assess the model's effectiveness. One can evaluate the model's validity by displaying the confusion matrix and examining the diagonal values for the number of correct categorizations. The model's efficacy has been established.

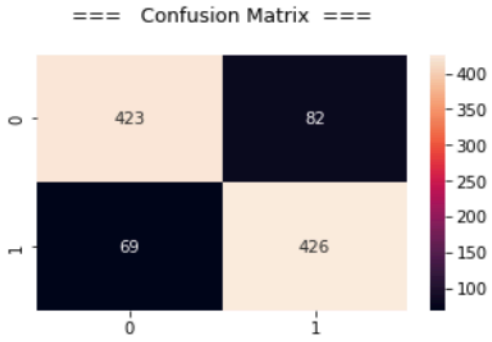

Figure 14. Confusion Matrix Blowfish_or_3DES_Cipher_Same key_ ECB Mode

6. Comparing Outcomes

It is evident from **Table 6** that the classification model proposed in this research can successfully classify the four algorithms in ECB and CBC mode with an average accuracy of 85%, compared to the source [1], with an accuracy of 87.9%. As for the algorithms in the CBC mode, the percentage reached 88% by the method proposed in the research. As for the source, the accuracy was 12.64%, which is much lower than what we found. Both use the same key in encryption. Moreover, the security is not high, and it is easier to classify it than others in both CBC and ECB; compared to the current research, the accuracy rate is the highest and best in this research.

Table 6. Comparison of Block Ciphers' Classification Accuracy in Ecb and Cbc Mode.

Mode	The proposed method Accuracy	Source [1] Accuracy
ECB	85%	87.9%
CBC	**88%**	12.64%

The suggested technique, which uses the same key and encryption with CBC mode, is superior to the source [4], which also uses the same key in encryption with CBC mode, according to a performance comparison shown in **Table 7**.

Table 7. Comparisons of Cbc Mode Block Ciphers Using the Same Key For Classification Accuracy.

Mode	The proposed method Accuracy	Source [4] Accuracy
	same key	same key
CBC	**88%**	87%

7. Conclusions

This work categorizes ciphertexts generated by three different algorithms, including two model block ciphers operating in ECB mode and two model block ciphers running in CBC mode. The objective is to identify the most accurate classification algorithm for these three block ciphers, 3DES, AES, and blowfish, using block cipher modes (CBC, ECB). In this paper, classified fully connected neural networks are used for identifying the encryption method, and their accuracy is evaluated with a confusion matrix. The same keys are used for different text data. The paper results show FCNN classifier has the highest classification accuracy for identifying encryption methods for ciphered data. The accuracy is in CBC mode at 88% and ECB mode at 85% using the same key. Through this research, the algorithms and their security are evaluated, as well as the modes of security. Hence new techniques have to develop to identify encryption methods. In the future,

using the properties of encryption techniques, we would build efficient categorization features based on the security mode, such as other modes. Stream ciphers and public key ciphers are candidates for ciphertext classification study simultaneously.

References

1. Hu, X.; Zhao, Y. Block ciphers classification based on random forest. *In Journal of Physics: IOP Publishing*. Conference Series **2019 Feb 1**, *1168, 3*, 032015.
2. Manjula, R.; Anitha, R. Identification of encryption algorithm using decision tree. In International Conference on Computer Science and Information Technology, *Springer,* Berlin, Heidelberg.**2011, January**, 237-246.
3. Swapna, S.; Dileep, AD.; Sekhar, CC.; Kant, S. Block cipher identification using support vector classification and regression,*Journal of Discrete Mathematical Sciences and Cryptography*. **2010 Aug 1**, *13(4),*305-18.
4. Dileep, AD.; Sekhar, CC. Identification of block ciphers using support vector machines. In The 2006 IEEE International Joint Conference on Neural Network Proceedings, IEEE.**2006 Jul 16**, 2696-2701.
5. Tan, C.; Ji, Q. An approach to identifying cryptographic algorithm from ciphertext. In2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), IEEE. **2016 Jun 4**, 19-23.
6. Nagireddy, S. A Pattern Recognition Approach to Block Cipher Identification. Master of Science Dissertation–Indian Institute of Technology Madras,**2008**.
7. Krishna, Nivedhitha Ramarathnam. Classifying Classic Ciphers using Machine Learning **2019**.
8. Liu, H.; Lang, B. Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences. **2019 Oct 17**, *9(20),*4396.
9. Sarker, IH. Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN Computer Science. **2021 Nov**, *2(6),*1-20.
10. Sohal, M.; Sharma, S. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University-Computer and Information Sciences*. **2022 Jan 1**, *34(1):1417-25*.
11. Vuppala, A.; Roshan, RS.; Nawaz, S.; Ravindra, JV. An efficient optimization and secured triple data encryption standard using enhanced key scheduling algorithm. Procedia Computer Science**. 2020 Jan 1**, *171,1054-63*.
12. Nagireddy, S. A pattern recognition approach to block cipher identification. LAP LAMBERT Academic Publishing.**2019**.
13. Hu, X.; Zhao, Y. Block ciphers classification based on random forest. *In Journal of Physics: Conference Series*, IOP Publishing. **2019 Feb 1**, *1168, 3*, 032015.
14. Kopal, N. Of ciphers and neurons–detecting the type of ciphers using artificial neural networks. In Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt **2020 May 19**, *171*, 77-86.
15. Yang, W.; Park, Y. Identifying Symmetric-Key Algorithms Using CNN in Intel Processor Trace. Electronics. **2021 Oct 13**, *10(20),*2491.
16. Dataset Kaggle website [online] https://www.kaggle.com/code/lemonkoala/cipher-difficulty-1-solution/data?select=plaintext_encrypt1.csv . **[Accessed 14 4 2022].**
17. Alhijaj, TB.; Hameed, SM.; Bara'a, AA. A Decision Tree-Aware Genetic Algorithm for Botnet Detection. *Iraqi Journal of Science*. **2021 Jul 3**1, 2454-62.