Identification Of Cryptosystem Based on Deep Neural Network

Yixuan Geng *

School of Cybersecurity, Northwestern Polytechnical University, Xi'an, China 710129

* Corresponding Author Email: gyx54138@gmail.com

Abstract. In network security, deep learning plays a particularly crucial role, where deep learning-based neural networks contribute to data security and accelerate analytical processes. This paper investigates cryptosystem identification using *CNNs* through controlled experiments and systematic analysis, including control-variable approaches, and the encryption algorithms, parameters and modes of operation are comprehensively explored to evaluate cryptosystems through the construction and innovation of feature engineering and model structures, as well as the continuous adjustment of optimization parameters. Comprehensive experiments reveal that the proposed methodology achieves identification accuracy between 25% and 65% under varying cryptographic configurations, demonstrating its adaptability and effectiveness in practical scenarios such as cryptographic identification, and provides strong support for the wider application of deep learning models in the field of network security.

Keywords: Neural Network, Cryptographic System, Deep Learning, Feature Program.

1. Introduction

1.1. Background

In the era of rapid digital transformation, deep learning technologies, particularly *CNN*s with advanced feature extraction and pattern identification capabilities, have demonstrated exceptional performance across interdisciplinary domains including computer vision and natural language processing. Their expanding applications have further revealed significant potential in cybersecurity, where cryptographic systems serve as critical safeguards for protecting sensitive model parameters and confidential data. The precise identification of cryptographic mechanisms is essential to ensure operational security and mitigate malicious attacks (e.g., integral and related-key attacks) [1]. Adversaries increasingly exploit sophisticated techniques to compromise cryptographic protocols, thereby escalating security risks. Thereby, developing *CNN*-based frameworks capable of accurately recognizing cryptographic systems not only enhances operational efficiency but also strengthens defensive resilience against evolving cyber threats.

1.2. Related Work

Through systematic literature review, this research advances the understanding of neural networks and their cryptographic applications. Li et al. [2] make a comprehensive analysis of *CNNs*. This seminal work systematically examines *CNN* structures, functionality optimization, and hyperparameter selection strategies through empirical studies, establishing a theoretical foundation for our experimental design.

Nitaj et al. [3] substantiated the interdisciplinary potential of neural networks in cryptography. Using deep learning with a complex artificial neural network structure, they experimented with the feasibility of enhancing the security of encryption systems through four important systems in modern cryptography, and summarized the possible problems, providing a theoretical basis and examples for this experiment.

Wang et al. [4] address critical vulnerabilities in public-key cryptosystems through their *DBSCAN-CNN* hybrid methodology. By mitigating outlier interference in clustering-based side-channel analysis (specifically targeting simple power analysis vulnerabilities in digital signatures), their approach achieves a 23.4% improvement in key recovery success rates compared to conventional techniques - a significant advancement for practical cryptanalysis applications.

In encrypted traffic classification, Lotfollahi et al. [5] present DeepPacket, a *CNN*-based model achieving 98.7% accuracy in HTTPS/Tor traffic classification through raw byte-level feature learning. This validates *CNN*'s efficacy in cryptographic protocol identification and inspires our feature engineering strategy for cryptographic algorithm identification.

Building upon image processing breakthroughs from Dong et al. [6] and Simonyan et al. [7], they innovatively adapt *SRCNN* and *VGG* structures to cryptographic contexts. Inspired by them, our novel ciphertext-to-image transformation protocol enables *CNN*-based feature extraction from encrypted data, while network layer optimizations derived from these works enhance identification model performance.

1.3. Our work

This paper aims to identify cryptosystems, and to construct a set of cryptosystem identification systems based on deep *CNN*s through improvement and innovation based on the identification of cryptographic algorithms [8].

In the process of encryption algorithm identification, we use seven international standard encryption algorithms, namely *AES*, *3DES*, *RSA*, *Kasumi*, *Blowfish*, *CAST*, and *ChaCha20*, to encrypt the *H.264* - encoded standard test video. Regarding feature engineering, a multi - dimensional hybrid feature space is innovatively constructed, ultimately forming a 1024 - dimensional eigenvector. What's more, the *SMOTE* oversampling technique is applied to expand the minority samples to achieve a balanced distribution [9]. In terms of model structure design, the *DPCNN* is adopted in the experiment. This model consists of five convolution modules. In the fully - connected part, a dynamic dropout mechanism is introduced, and a three - layer structure is used for feature compression. Under the TensorFlow framework, the Adam optimizer is used. Through the early - stop mechanism and the model checkpoint callback function to achieve the optimization.

Moreover, numerous innovative practices are carried out in this experiment to obtain superior experimental results. Firstly, a novel hybrid structure integrating cryptographic statistical features and deep learning is proposed. Secondly, a multi - scale convolutional kernel collaborative working mechanism is designed. Last, besides encryption algorithm identification, the identification of parameter and mode of operation are also conducted. Multiple scenarios are comprehensively considered, and improvements are made to feature engineering selection and model construction to achieve better experimental outcomes.

The experimental results show that the overall accuracy of multiple models for cryptosystem identification is 30%-65% on the test set, and the identification accuracy of the encryption algorithm is significantly higher than that of other identification models, reaching 62.6%.

2. Preliminary

2.1. Cryptographic system

Definition 1 Symmetric Cipher

Symmetric Cipher employs the same key for both encryption and decryption processes. They are characterized by high - speed encryption and relatively low computational requirements. Commonly used block ciphers include *AES*, *Blowfish* and *3DES* [10].

Definition 2 Asymmetric Cipher

Asymmetric Cipher uses two keys, a public key and a private key, and common encryption algorithms are *RSA* and *DSA* [11].

Definition 3 Mode of operation

Block ciphers are designed to encrypt plaintext of a fixed length. However, in practical applications, users often need to encrypt not just a single plaintext group of 8 bytes or 16 bytes, but larger files, emails, etc. For plaintext of arbitrary length that requires encryption, it is necessary to iterate the block cipher. The iteration method of the block cipher is known as the mode of operation. The modes of operation include *ECB.CBC.CFB.OFB* and *CTR* [12].

2.2. Neural network

In the field of machine learning and cognitive science, Neural network is a mathematical model or computational model that mimics the structure and function of biological neural networks (the central nervous system of animals, especially the brain), which is used to estimate or approximate functions. Figure 1 shows the structure of the neural network.

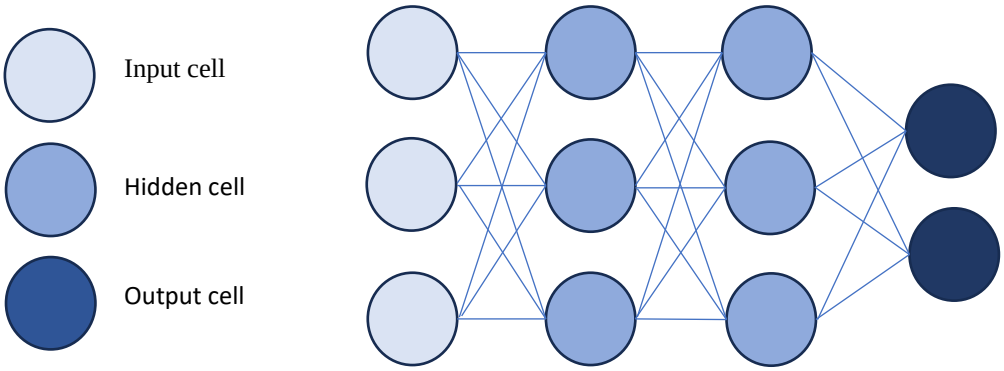

Figure 1. Neural network structure

Definition 4 Convolutional neural network

A *CNN* is a type of feed - forward neural network where artificial neurons can respond to a local region of the surrounding cells within the receptive field. As shown in Figure 2, *CNNs* are highly effective in large - scale image processing. A *CNN* typically consists of one or more convolutional layers, a fully - connected layer at the top, along with associated weights and pooling layers.

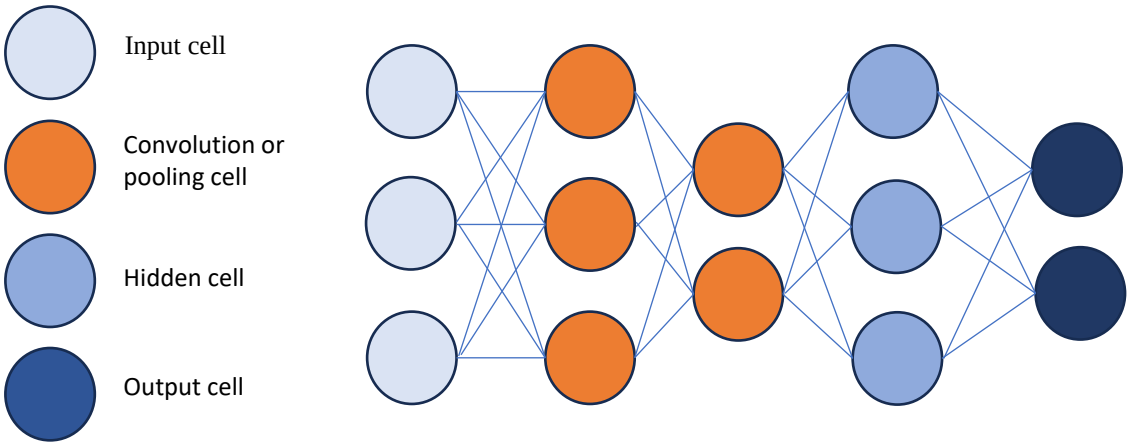

Figure 2. *CNN* structure

2.3. Feature engineering

Features, also referred to as dimensions, are the input variables used to generate model predictions. Feature engineering is the process of transforming raw data into relevant information that can be utilized by machine - learning models. In other words, it is the process of creating features for predictive models [13].

2.4. Notations

The symbols used in the paper are listed in Table 1.

Table 1. Symbol description

Symbol	Description
CNN	Convolutional Neural Network
DPCNN	Deep Pyramid Convolutional Neural Network
SRCNN	Super-Resolution Convolutional Neural Networks
VGG	Visual Geometry Group
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Standard
CAST	Cipher - Alberta
RSA	Rivest - Shamir - Adleman
DSA	Digital Signature Algorithm
ECB	Electronic Code Book mode
CBC	Cipher Block Chaining mode
CFB	Cipher Feedback mode
OFB	Output Feedback mode
CTR	Counter mode
GF(2)	A finite field consisting of two elements 0 and 1
SMOTE	An oversampling technique used to solve class imbalance problems
LFSR	Linear Feedback Shift Register
ReLU	Rectified Linear Unit
LeakyReLU	Leaky Rectified Linear Unit

3. Identification of Cryptosystem

This paper conducted extensive research on cryptographic system identification, encompassing plaintext data collection, encryption, ciphertext labeling, feature engineering, model structure design and optimization, and result visualization.

3.1. Model Constructions

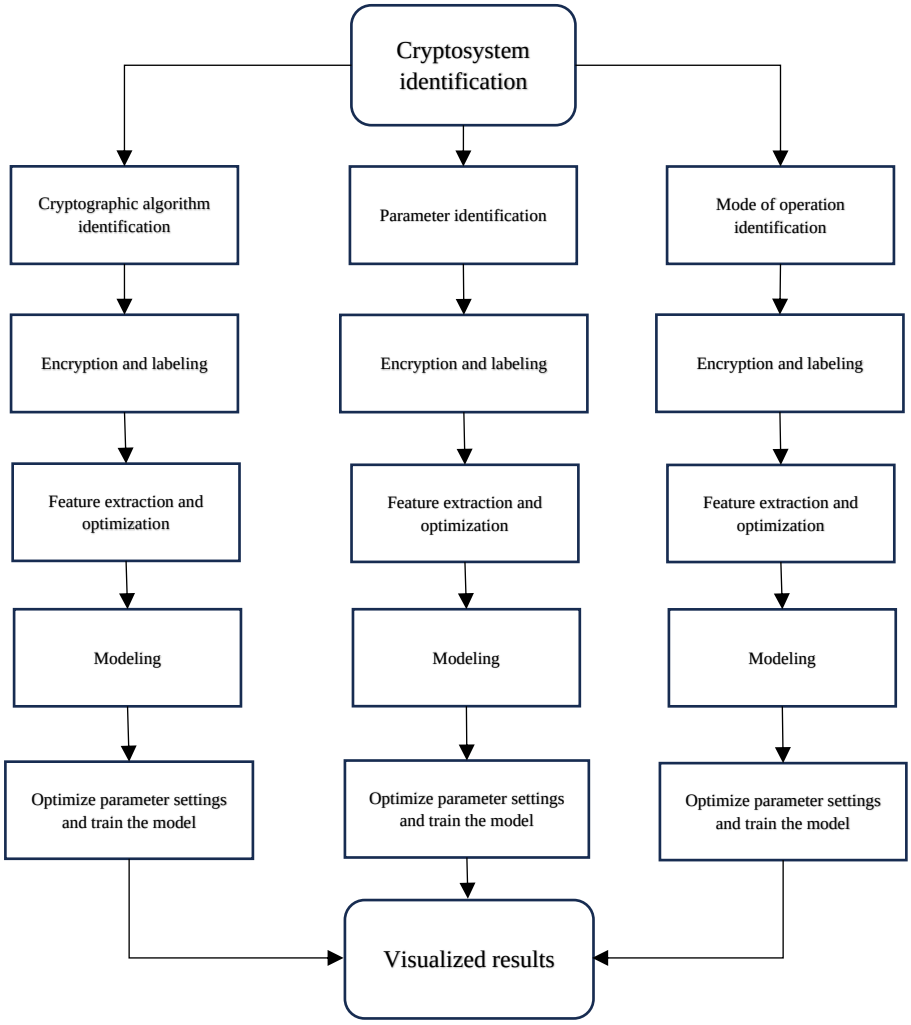

Figure 3. Operational flow diagram

Figure 3 shows the process of cryptosystem identification. Firstly, the plaintext is encrypted using encryption algorithms, and the ciphertext is labeled. Secondly, according to different identification requirements, different feature engineering and model structures were created. Among them, the feature engineering includes the Shannon entropy and block entropy of ciphertext, the amplitude spectrum features of discrete Fourier transform, the frequency distribution, mean value and variance of bytes, the rank of binary matrix, linear complexity, the texture features of Sobel gradient histogram and local binary mode, differential entropy, bit distribution uniformity, continuous bit correlation, and the length and size of ciphertext blocks, etc., and are optimized by *SMOTE* and other technologies to form 1024 and 512-dimensional eigenvectors respectively. Finally, in the process of model construction, a 5-module *CNN* and two dual-module *CNN*s were finally formed through experiments, and good results were finally obtained by optimizing the parameter settings and multiple trainings.

3.2. Feature engineering

Through literature review and empirical validation, twelve critical features were selected
(1) Frequency distribution, mean, and variance of bytes
Includes frequency distribution, mean, and variance of byte values.
(2) Ciphertext Block Length/Size
Length of data blocks in the ciphertext.
(3) Bit Distribution Uniformity
Measures the balance of binary bit distribution.

(4) Shannon Entropy

$$H(x) = -\sum_{i=1}^{n} P(x_i) log_2 P(x_i) \quad (1)$$

Measures the average uncertainty in a random variable x, $P(x_i)$ is the probability of symbol x_i, higher entropy indicates greater randomness.

(1) Block Entropy

Computes entropy for contiguous data chunks (degenerates to Shannon entropy when k=1).

(2) Differential Entropy

Measures information content for continuous random variables.

(3) Discrete Fourier Transform

Converts time-domain signals into frequency-domain representations [14].

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-i\frac{2\pi}{N}nk}, (k = 0,1,2, \dots, N-1) \quad (2)$$

(4) Binary Matrix Rank

Determines the rank of a matrix over the *GF(2)* field, representing the dimension of its vector space.

(5) Linear Complexity

Defines the length of the shortest *LFSR* required to generate a binary sequence.

(6) Sobel Gradient Histogram

Computes gradient magnitude and direction histograms for grayscale images using Sobel operators [15].

Gradient amplitude

$$G(x,y) = \sqrt{G_x(x,y)^2 + G_y(x,y)^2} \quad (3)$$

Gradient direction

$$\theta(x,y) = \arctan\left(\frac{G_y(x,y)}{G_x(x,y)}\right) \quad (4)$$

(7) Local Binary Mode Texture Features

Encodes local texture features by thresholding pixel neighborhoods in a 3×3 window [16].

(12) Consecutive Bit Correlation

Evaluates interdependencies between adjacent or nearby bits in a digital sequence.

3.3. *CNN* constructions

In the cryptographic algorithm identification model, *CNN* has five hierarchical modules. Module 1 is 64-channel 3×3 convolution and maximum pooling (2×2 windows) for basic texture extraction. Module 2 is a 128-channel 3×3 convolution for higher-order statistics. Modules 3 and 4 are 256-channel and 512-channel 5×5 convolutions for global pattern identification. Module 5 is a 1024-channel 3×3 convolution with batch normalization and *ReLU* activation for feature optimization. The flat layer is then connected for flattening and the output is sent to a fully connected layer (2048-1024-512 neurons) with a dynamic dropout (rate=0.3). Model training leverages the Adam optimizer (initial learning rate = 1e-4, exponential decay = 1e-5), early stops, and checkpoints to achieve convergence within 85 epochs. There are two modules for the *CNN* of the parameter identification model. Module 1 is a 32-channel 3×3 convolution with "identical" filling, batch normalization, and *LeakyReLU* (α=0.1) [17]. Module 2 is a 64-channel 3×3 convolution with a single fully connected layer (128 neurons). Use a similar optimization strategy to end the training within 50 epochs. The mode of

operation identification model has a two-module *CNN* structure with L2 regularization (λ=0.001). Module 1 is a 32-channel 3×3 convolution with padding and batch normalization. Module 2 is 64-channel 3×3 convolution. A fully connected layer of 256 neurons achieves optimal performance within 150 epochs.

4. Results

The results are shown in Figure 4 and 5.

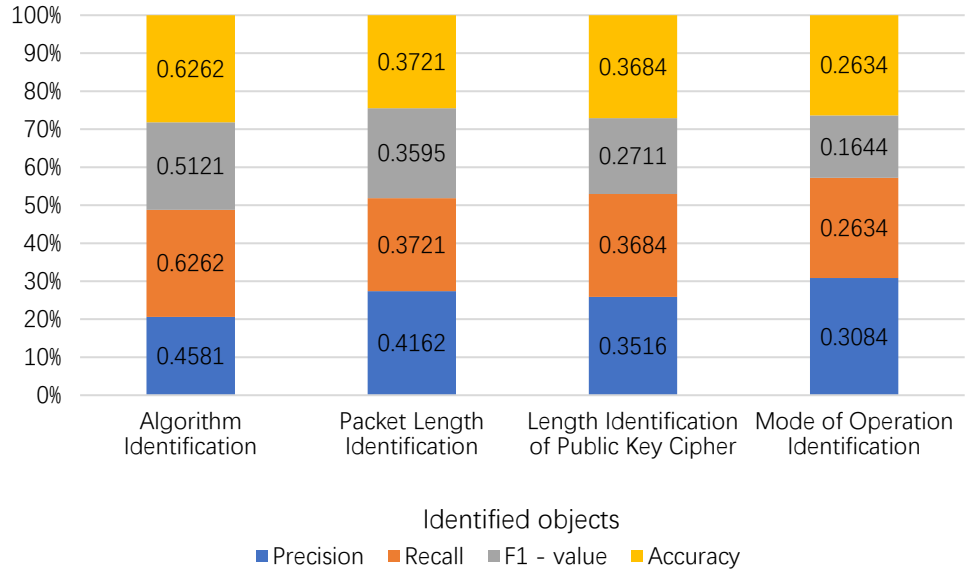

Figure 4. Percentage stack histogram of identification

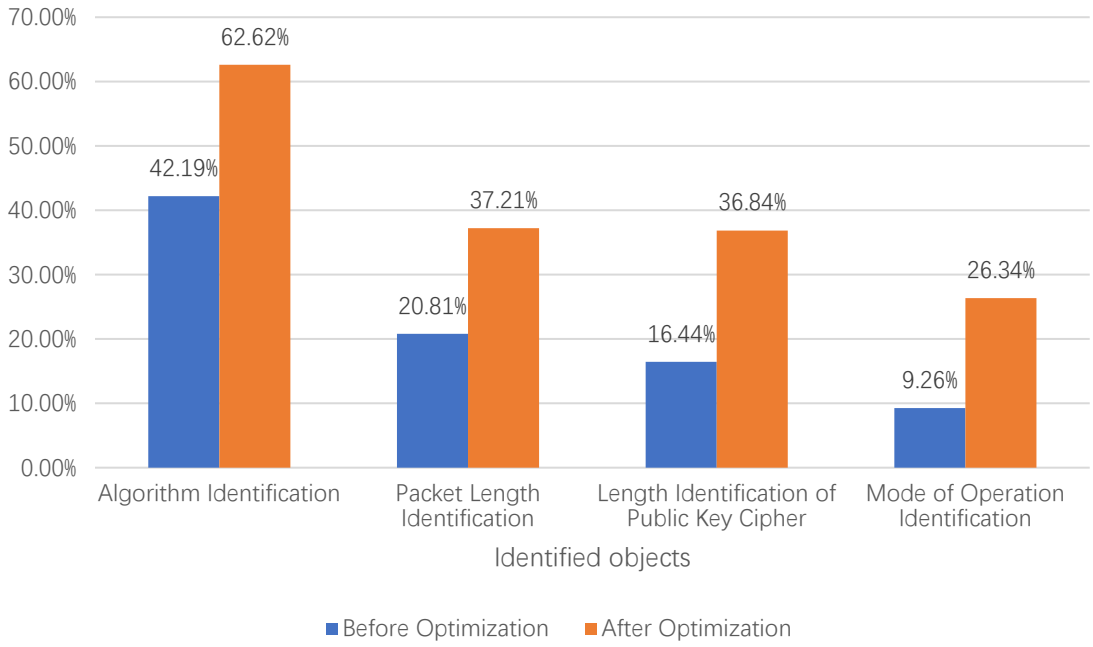

Figure 5. Comparison of accuracy before and after optimization

Figure 4 and 5 shows the depicts the situation of cryptosystem identification, the results will be analyzed in detail.

4.1. Cryptographic algorithm identification

As can be seen from the figure, the encryption algorithm identification model has a good identification effect, and each coefficient is higher than that of other models. In the early stage of model design, through control experiments, the method of control variables was adopted, and the feature engineering, neural network structure and various optimization parameters were used as control points, and the necessity of these optimization points was finally determined. In the follow-up experiments, through continuous analysis and adjustment of feature engineering, neural network structure and optimization parameters, the identification accuracy of the model was finally improved from 42.19% at the beginning to 62.62% at present. During the overall model training and testing, false positives mainly occur between *Blowfish* and *ChaCha20*, because some cryptographic features and data patterns may be similar and do not affect the performance of the model itself.

4.2. Cryptographic parameter identification

At this stage, the identification of cipher parameters is mainly studied from two aspects: block cipher length identification and public key cipher length identification. The results of the two models are slightly lower than those of the cipher algorithm identification model, mainly because the model appears overfitting phenomenon during training, which makes the accuracy greatly reduced. However, by further screening feature engineering and simplifying the structure of neural network, while adjusting the optimization parameters, its accuracy can still be improved from 20.81% and 16.44% to 37.21% and 36.84% respectively, showing a certain identification ability. During training and testing, the packet length identification is typically identified as 32 lengths, while the public key length is typically identified as 1024 lengths.

4.3. Cryptographic mode identification

In the identification of modes of operation, it is more often identified as ECB. The result of the mode of operation identification model is similar to that of the parameter identification model, but the accuracy rate is low. The reason is still the phenomenon of overfitting. However, by adding feature engineering, simplifying neural network structure and adjusting optimized parameters, the identification accuracy is improved from 9.26% to 26.34%. Because the mode of operation of block cipher involves more concepts and parameters, the stringency requirement for each parameter assignment is higher. In the subsequent work, it is necessary to further try each parameter to improve the accuracy.

5. Conclusions

This paper centers on the identification of cryptographic systems using deep - learning - based *CNN*s, it delves into encryption algorithms, cryptographic parameters, and modes of operation. By simulating the video encryption process, constructing a multi-dimensional hybrid feature space, and building a deep pyramid convolutional neural network model to achieve the identification purpose, innovative methods are used in feature engineering and model construction to improve the accuracy. Nevertheless, in the identification of cryptographic parameters and modes of operation, issues such as overfitting and sub - optimal optimization parameters still exist. Considerable time is still required in subsequent studies and experiments to improve features, the neural network structure, and optimization parameters. Continuous trial - and - error efforts are needed to explore the most suitable data for experimental operations. The final experimental results demonstrate that the overall model has an accuracy ranging from 30% to 65% for the cryptosystem, and the identification accuracy of the encryption algorithm even reaches as high as 62.6%.

This paper offers robust support for the extensive application of deep - learning models in the field of network security. In the future, we can improve the code based on this experiment, further extend it to quantum encryption feature extraction method, conform to the trend of the times, and deeply expand and integrate deep learning into the field of cyberspace security.

References

[1] Alzaidy S, Binsalleeh H. Adversarial Attacks with Defense Mechanisms on Convolutional Neural Networks and Recurrent Neural Networks for Malware Classification[J]. Applied Sciences, 2024, 14(4): 1673.

[2] Li Z, Liu F, Yang W, et al. A survey of convolutional neural networks: analysis, applications, and prospects[J]. IEEE transactions on neural networks and learning systems, 2021, 33(12): 6999-7019.

[3] Nitaj A, Rachidi T. Applications of neural network-based AI in cryptography[J]. Cryptography, 2023, 7(3): 39.

[4] Wang A, He S, Wei C, et al. Using Convolutional Neural Network to Redress Outliers in Clustering Based Side-Channel Analysis on Cryptosystem[C]. International Conference on Smart Computing and Communication. Cham: Springer Nature Switzerland, 2022: 360-370.

[5] Lotfollahi M, Jafari Siavoshani M, Shirali Hossein Zade R, et al. Deep packet: A novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.

[6] Dong C, Loy C C, He K, et al. Image super-resolution using deep convolutional networks[J]. IEEE transactions on pattern analysis and machine intelligence, 2015, 38(2): 295-307.

[7] Simonyan K. Very deep convolutional networks for large-scale image recognition [J]. arxiv preprint arxiv:1409.1556, 2014.

[8] Pamidiparthi S, Velampalli S. Cryptographic algorithm identification using deep learning techniques[C]. Evolution in Computational Intelligence: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020), Volume 1. Springer Singapore, 2021: 785-793.

[9] Dablain D, Krawczyk B, Chawla N V. DeepSMOTE: Fusing deep learning and SMOTE for imbalanced data[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 34(9): 6390-6404.

[10] Manz O. Symmetric Ciphers[M]. Encrypt, Sign, Attack: A compact introduction to cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022: 19-51.

[11] Usmonov M. Asymmetric Cryptosystems[J]. INDEXING, 2024, 1(1): 76-80.

[12] Kuznetsov A A, Potii O V, Poluyanenko N A, et al. Comparison of Stream Modes in Block Symmetric Ciphers[J]. Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies, 2022: 99-110.

[13] Zhou Y, Shi H, Zhao Y, et al. Encrypted network traffic identification based on 2d-cnn model[C]. 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2021: 238-241.

[14] Wang X, Su Y. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform[J]. Scientific Reports, 2020, 10(1): 18556.

[15] Alphonse A S, Abinaya S, Arikumar K S. A novel monogenic Sobel directional pattern (MSDP) and enhanced bat algorithm-based optimization (BAO) with Pearson mutation (PM) for facial emotion recognition[J]. Electronics, 2023, 12(4): 836.

[16] Le V N T, Ahderom S, Alameh K. Performances of the lbp based algorithm over cnn models for detecting crops and weeds with similar morphologies[J]. Sensors, 2020, 20(8): 2193.

[17] Javid A M, Das S, Skoglund M, et al. A ReLU dense layer to improve the performance of neural networks[C]. ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021: 2810-2814.