Security Assessment of Commercial Password Applications: A Framework that Integrates Randomness Visualization and Spatiotemporal Deep Learning

Jiang Luo[1], Fuxin Hong[1], Shuai Liu[1], Yang Yang[1] and Hailong Chi[2,*]

[1]*China Yangtze Power Co., Ltd., Yichang, 443000, China*
[2]*Beijing IWHR Technology Co, Ltd., Beijing, 100038, China*
E-mail: chihailong5@outlook.com
[*]*Corresponding Author*

Received 25 November 2025; Accepted 13 January 2026

Abstract

To solve the compliance risks caused by "weak passwords", "clear text transmission", and algorithm misuse, and to help commercial passwords achieve automated and high-precision security assessment, this study proposes a "randomness-space-time" dual-axis fusion framework. This framework contains two core innovations: firstly, on the static ciphertext side, a "randomness visualization" strategy is proposed, which concatenates the NIST nine-term global randomness test values with local non-overlapping template matching results into a vector. After dimensionality reduction by an autoencoder, it is stacked with the original hexadecimal word throttling and bit accumulation graph to form a three-channel grayscale image, which is then input into the ResNet50 for fine-grained recognition of the encryption algorithm. Secondly,

Journal of Cyber Security and Mobility, Vol. 15_2, 273–302.
doi: 10.13052/jcsm2245-1439.1521

on the dynamic traffic side, a spatio-temporal parallel fusion network is designed, the session is fragmented into packet sequences, and "Attention-ResNet50" is run in parallel to extract the "spatial" texture features inside the packets. It uses the Transformer encoder to capture the "time" remote dependencies between data packets to achieve accurate identification of encryption protocols. The results showed that in ciphertext traffic detection, the recognition accuracy of ciphertext and traffic protocols reached 98.83% and 98.25%, both 3%–8% ahead of the control model. The single-sample inference delay was $<$5 ms, and the throughput was $>$240 sessions/s. This study couples randomness test statistics with deep vision-sequence models to achieve "ciphertext-traffic" dual-modal collaborative assessment, which can effectively provide compliance detection and defense technical guidance for commercial cryptography applications.

Keywords: Commercial cryptography, randomness test, spatiotemporal fusion, ResNet, transformer, deep learning.

1 Overview

In the context of the digital wave sweeping the world, cryptography technology, as the cornerstone of ensuring network and information security, has become increasingly prominent in its strategic position. Among them, commercial encryption, as the core technology and basic support to ensure cyberspace security, has fully penetrated into key information infrastructure fields, such as government affairs, finance, communications, and energy [1]. However, since the formal implementation of the cryptographic law, its actual application still faces multiple challenges such as irregular application, insufficient coverage, and abuse of insecure cryptographic algorithms [2]. Many systems are still vulnerable to "weak passwords" or even clear-text transmission, or fail to deploy cryptographic services correctly according to specifications, exposing information assets to severe security risks [3]. To address these challenges, automated password application compliance audits and security assessments of information systems have become crucial. Regarding the issue of information encryption, many scholars have conducted research. Among them, Patel AK et al. proposed a biometric password system to solve the problems of traditional passwords being easily broken and biometric recognition being easily forged. The system utilized directed gradient histogram technology to extract unique 32-bit encryption keys from facial features, and combined advanced encryption standards to

encrypt and decrypt multimedia data. The evaluation showed that the key generated by this method had high entropy and resistance to attacks. By integrating the uniqueness of biometric recognition with the security of AES, it provided a reliable approach for data protection [4]. Shi W et al. proposed a classification region location privacy protection model to address the risks of reverse inference attacks in location data management. The model divided regions through personalized clustering and dynamically allocated differential privacy budgets using sensitivity first algorithms. Finally, Laplacian noise was introduced to achieve region fuzzification. The results indicated that the model could effectively resist specific attacks and had good privacy protection effects [5]. To address the issues of low efficiency and insufficient sensitivity in traditional network security analysis, Zhou L et al. proposed a fusion of a Gaussian operator and a fuzzy neural network, combined with an optimized fireworks algorithm to achieve multi-objective feature selection. The results showed that this method improved the detection sensitivity to over 70%, providing a reference for dynamic network security frameworks [6]. To improve the accuracy of network intrusion detection systems, Wanjiu SK et al. proposed a discriminative spatiotemporal feature learning model. This hybrid method innovatively combined a 2D Convolutional Neural Network (CNN) to extract spatial features of network traffic and utilized bidirectional Long Short-Term Memory (LSTM) networks to capture its temporal features. The test results showed that the accuracy and precision were significantly better than existing models [7].

Past research on cryptographic algorithm identification has mainly focused on two major technical paths. The first is to conduct an intrusive analysis of software and hardware through static disassembly or dynamic debugging, but this requires extremely high professional skills and has limited applicable scenarios. The second is the current mainstream ciphertext-only analysis method, which is to identify the encryption algorithm while only mastering the ciphertext data [8]. Current research focuses mostly on application type identification or malicious traffic detection, and less on the refined identification of encryption protocols (especially cipher suites). Most models only use single-dimensional features or simple feature splicing to achieve traffic detection, failing to effectively integrate spatiotemporal information and deeply characterize the intrinsic communication patterns of complex network protocols [9]. Commercial privacy passwords are difficult to obtain due to the random nature of their ciphertext, making identification difficult and complex. The ciphertext features of domestic commercial cryptographic algorithms lack unified rules, and problems such as traffic compliance

detection and high-dimensional feature data are more prominent. Therefore, in response to the above issues and technical bottlenecks, the core goal of the research is to provide an automated, high-precision non-invasive detection scheme for the security assessment of commercial password applications. The importance of research lies in its ability to assist regulatory agencies and businesses in effectively identifying security risks such as password misuse and abuse. With the deepening implementation of the Password Law, how to quickly and accurately audit the compliance of password applications in existing information systems (whether weak passwords are used, whether protocols are deployed correctly) has become an urgent practical issue. The research method can efficiently identify ciphertext algorithms and encryption protocols in a non-invasive manner, which is in compliance with the requirements of the Cryptography Law and provides powerful technical tools for regulatory agencies and enterprises. It helps to proactively identify security risks and enhance the overall security of critical information infrastructure. This study designs a security assessment scheme for commercial cryptography applications that integrates randomness characteristics and spatiotemporal relationships. Therefore, this study analyzes the National Institute of Standards and Technology (NIST) standards and combines NIST randomness test features with byte stream features. In addition, it is proposed to use the improved Residual Convolutional Neural Network (ResNet50) to realize the identification of commercial cryptographic algorithms to improve the accuracy of algorithms and data analysis.

Although the biometric key in reference [4] has uniqueness, its focus is on key generation rather than algorithm recognition of unknown ciphertext. The methods in references [5] and [6] focus on privacy protection and feature selection, and their analysis dimensions are relatively single, making it difficult to cope with the inherent pseudo-random characteristics of encryption algorithms. Although reference [7] integrates spatiotemporal features, its "space" is limited to the statistical level of network traffic and fails to delve into the byte-level "texture" of data packet payloads. Moreover, its "time" model is inferior to Transformer in capturing ultra-long-distance protocol interactions. The innovation of the research lies in proposing a "randomness spatiotemporal" dual-axis fusion framework. The key innovation of this framework lies in two aspects, one of which is the ciphertext recognition with "randomness visualization". The study proposes to consider the statistics of the NIST randomness test itself as a learnable feature and visualize it as an image. By fusing this random feature map with the original byte structure map and bit accumulation map into a multi-channel

input, and utilizing the powerful visual feature extraction ability of ResNet50, high-precision recognition of encryption algorithms can be achieved. This solves the problem of traditional methods relying only on shallow statistical features and being difficult to distinguish highly pseudo-random ciphertexts. The second is the identification of traffic protocols for "spatiotemporal parallel fusion". For encrypted traffic, a parallel dual-branch network is designed from the dimensions of "space" and "time". The Attention-ResNet50 is used to analyze the byte distribution texture of packet payload in the "spatial" dimension, and the Transformer encoder is used to capture the interaction patterns and long-range dependencies of data packet sequences in the "time" dimension. This kind of spatiotemporal parallel processing and fusion can accurately depict the subtle differences between different encryption protocols (including State Secrets SSL, TLS 1.3, post quantum cryptographic protocols, etc.). The deep quantization of the encryption algorithm "pseudo-random quality" and the simultaneous modeling of byte "spatial texture" within data packets and "global temporal dependence" between data packets make the research method have stronger recognition accuracy and generalization ability than single or simple feature concatenation methods. This study aims to better provide automated and high-precision technical support for security assessment of commercial cryptography applications and provide decision-making support for active defense.

2 Literature Review

Commercial privacy data security is an important part of the development of individuals, enterprises, and countries, and data leakage can easily lead to data property and social security issues. To ensure the security of commercial privacy data, Kumbhakar D et al. combined the Elgamal cryptosystem and LSB image steganography technology to generate encrypted data into steganographic images. This method could ensure the safety of transaction data during the decryption process, and the image quality it generated was high [10]. To take into account e-commerce security and system performance, Chen independently completed purchase and encryption operations through software agents deployed on the client. Experiments have shown that this method improved system performance by 10%, shortened response time by 30.5%, and effectively prevented deadlock and request loss problems [11]. To improve the usability and security of graphic passwords, Rasheed A F et al. proposed an Arabic numeral recognition system based on deep learning, while using the "selected pixel" method to optimize network transmission

performance. Evaluations showed that the system outperformed traditional graphical password schemes in terms of login time, data storage, and password entropy [12]. Singamaneni K K et al. put forth a model that fuses multi-qubit quantum key distribution and attribute encryption to ensure cloud data security, distribute keys through quantum channels, and achieve attribute-based data access control. This model could effectively utilize the principles of quantum mechanics to ensure cloud data security [13]. HariKrishna A et al. proposed a Pipelined Advanced Encryption-Based Communication Protocol (PAEBCP). This protocol optimized encryption and decryption efficiency by decomposing the encryption process into multiple parallel stages. This architecture significantly improved the security of mobile communication systems while effectively responding to evolving threats [14]. Jean A et al. developed an independent encryption application that integrates Diffie-Hellman, Mersenne Twister, and Advanced Encryption Standard. This tool supported fast encryption and decryption of emails, codes, and form data, and successfully resisted key cracking attempts in tests [15].

In response to possible security risks in the implementation of FIDO2/WebAuthn passwordless authentication, Grammatopoulos A V et al. developed an automated testing tool to evaluate its consistency and security by analyzing requests and simulated responses. Actual tests showed that it effectively found common security issues in multiple services [16]. Considering the challenges of secure communication in the post-quantum era, Seyhan K et al. put forward a Lattice-based Password Authenticated Key Exchange Protocol (Saber.PAKE). The protocol was designed based on the modular learning rounding puzzle and adopted a three-channel explicit authentication method. This protocol could effectively resist common threats such as dictionary attacks and was superior to similar protocols in message size and running time [17]. Given the inefficiency of traditional password recovery systems, Luo Y et al. designed a heterogeneous parallel password recovery system built on the MT-3000 processor, using multi-level parallelism and a unified task allocation strategy. This system was superior to other traditional solutions in recovery speed and scalability [18]. To protect the privacy of healthcare patients, Adeniyi A E et al proposed to scramble the input data of the AES algorithm. This method could effectively save encryption and decryption time and show less complexity in small file processing [19]. To address the problem of phishing detection in encrypted traffic, Kondaiah C et al. proposed a model based on ensemble learning, which extracts features from Transport Layer Security protocol traffic and integrates multiple deep learning algorithms. This model achieved a classification precision of 99.61%

under undecrypted conditions and was suitable for real-time protection of the transport layer [20].

Previous research mostly approaches it from a single perspective, or relies on reverse engineering for intrusive analysis, or only uses shallow statistics such as byte frequency and entropy value to identify the ciphertext only. Traffic-side work has paid insufficient attention to fine-grained identification of cipher suites and generally ignores the timing context of protocol interactions. Therefore, based on the difference between the texture stability and pseudo-random statistics of encrypted images, this study proposes to transform the "randomness test statistic" into learnable visual features to better provide support for feature recognition of encryption algorithms. The purpose is to further provide technical methods and tools for automated detection of commercial password compliance.

3 Security Technology Design of Commercial Cryptography Applications

3.1 Ciphertext Feature Extraction and Recognition Based on Random Distribution

Ciphertext has great difficulty in byte stream feature extraction due to its complex structure and characteristics. Traditional methods ignore the local differences in random distribution within the ciphertext and find it difficult to capture their essential differences. Therefore, based on the ciphertext attributes, combined with the statistical randomness characteristics of the ciphertext and the byte stream structure information, this study proposes to construct a multi-channel feature representation of the ciphertext and use ResNet to achieve feature recognition. This study uses the NIST randomness test to extract features from the ciphertext data, selects nine methods to capture the global statistical distribution characteristics of the ciphertext data, and uses the non-overlapping module matching test to capture its local randomness characteristics. Nine methods: frequency test, intra-block frequency test, run test, longest 1 run test, binary matrix rank test, discrete Fourier transform test, sequence test, approximate entropy test, and cumulative sum test [21]. Figure 1 is the NIST randomness test chart.

The ciphertext sequence is often unified with a hexadecimal sequence and then converted into a ciphertext grayscale image, or the ciphertext 2 prohibits accumulation and is converted into a matrix vector and a grayscale image result. Considering that NIST randomness tests are relatively sensitive

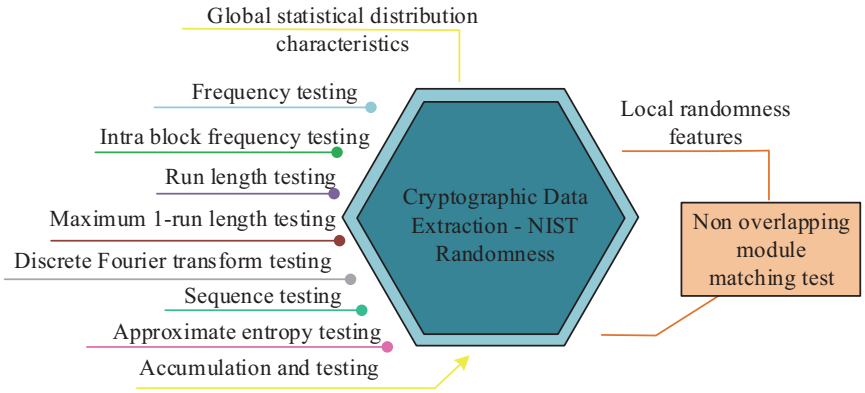


Figure 1 Schematic diagram of NIST randomness test.

to the input sequence length, a fixed-length chunking strategy is adopted to ensure the stability and comparability of statistical results. Specifically, all ciphertext files to be analyzed are uniformly divided into equally sized 1024-byte ciphertext blocks. The NIST randomness tests are conducted on these standardized non-overlapping blocks. If the end of a file did not contain a full block, zero-padding is applied to meet the standard length and achieve alignment. This study uses the ciphertext throttling information and NIST randomness features to extract grayscale images and uses them together as the ciphertext feature channel. Specifically, in the feature extraction process, the ciphertext file C to be analyzed of a uniform size is first divided into t ciphertext blocks C_j ($j = 1, 2, \ldots, t$) of equal length. Each ciphertext block C_j performs the above global and local randomness tests, and obtains a global feature vector $G_j(g_{j,1}, g_{j,2}, \ldots, g_{j,p})$ of dimension p and a local feature vector $L_j(l_{j,1}, l_{j,2}, \ldots, l_{j,r})$ of dimension r. This study introduces an autoencoder to perform nonlinear dimensionality reduction on L_j, inputs L_j into the autoencoder, and extracts the low-dimensional code $L'_j = Encoder(L_j)$ generated by it in the hidden layer. Subsequently, the dimensionally reduced L'_j is spliced with the original global feature vector $G_j(g_{j,1}, g_{j,2}, \ldots, g_{j,p})$ to form the final random feature vector F_j of the ciphertext block. The feature vectors F_t of t ciphertext blocks contained in a ciphertext file are stacked to form a feature matrix of $t \times d$ (d is the dimension of the feature vector after fusion), and this matrix is normalized and mapped into a grayscale image. At the same time, this study extracts byte stream features and constructs the Hexadecimal Byte Stream Grayscale Image (HBSGI) and Binary Cumulative Sum Grayscale Image (BCSGI). That is, the ciphertext block is treated

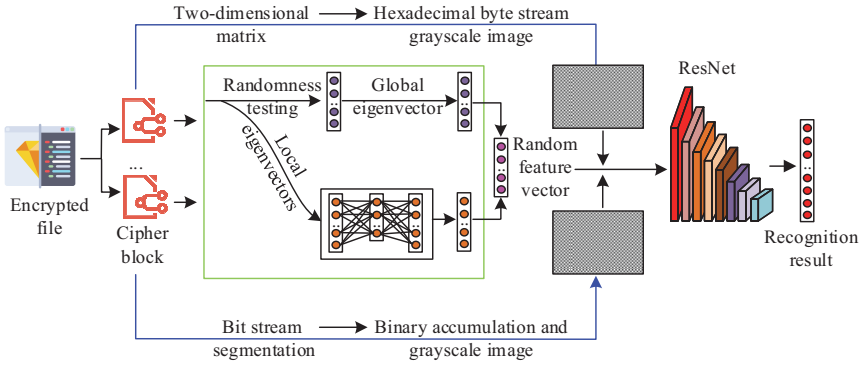


Figure 2 Overall architecture of the feature recognition model.

directly as a sequence of bytes and read. Its byte sequence is reshaped into a 2D matrix to generate an HBSGI. The ciphertext block is converted into a binary bit stream. The bit stream is then segmented by a fixed window size, and the cumulative sum of all bits within each window is calculated. After the cumulative sum results of all windows are normalized, they are also organized into a 2D matrix to generate BCSGI. After encoding, the grayscale image, HBSGI, and BCSGI are obtained, unified in size, and stacked into a three-channel feature map. It is input into ResNet. Figure 2 shows the overall framework of the feature recognition model.

In Figure 2, ResNet50 is the benchmark model. Its input layer receives the ciphertext three-channel feature map, and then the data flows through a series of convolutional layers, batch normalization layers, and residual blocks to gradually extract and abstract features. Finally, through the global average pooling layer and the fully connected layer, the extracted high-level features are mapped to the category probabilities of each cryptographic algorithm, and the recognition results are output. The theoretical motivation for transforming randomness statistics into images lies in the research hypothesis that distinct statistical metrics exhibit higher-order correlations unique to cryptographic algorithms. Reshaping these metrics into a 2D matrix converts this abstract statistical relationship into a spatial pattern. Powerful CNNs can effectively capture such local spatial patterns (like image textures) through their convolution kernels, thereby learning more discriminative combinatorial features than 1D vectors. Furthermore, by stacking randomness plots, byte stream plots, and cumulative sum plots into a three-channel image, CNNs can integrate structural, distributional, and pseudo-randomness dimensions at the same spatial location, achieving deep insights into the ciphertext's

intrinsic characteristics. This enables a better understanding of the ciphertext and enhances recognition accuracy.

3.2 Encrypted Traffic Protocol Identification Integrating Spatiotemporal Correlation

Encrypted traffic is not a completely random, chaotic data flow. It still retains structural characteristics that can be analyzed at the level of protocol interaction and data encapsulation. Therefore, after designing ResNet, this study took into account the spatiotemporal characteristics of traffic and proposed an encryption protocol identification scheme based on the idea of integrating them, correlating the intrinsic nature of encrypted traffic in the protocol interaction sequence (time dimension) and payload byte distribution (space dimension) [22]. The status sequence of Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Internet Protocol Security (IPSec) has obvious traffic timing characteristics, and the details vary greatly. Parsing the key field sequences in the interaction process of these protocols can effectively distinguish different features [23, 24]. Therefore, to make full use of the above two heterogeneous features, this study proposes an encrypted traffic protocol scheme that integrates spatiotemporal features. That is, two parallel subnetworks are designed to process time series data and spatial data, and the extracted deep features are fused. Figure 3 shows the parallel model architecture.

In Figure 3, a residual network (Attention-ResNet50) based on the Attention Mechanism (AM) is used for the spatial features represented by the traffic grayscale image. The traffic image is input into the multi-layer Attention-ResNet50 structure. After multiple rounds of convolution and pooling to extract high-level feature maps, the AM enables the model to adaptively learn the importance of different areas in the feature map. In view of the

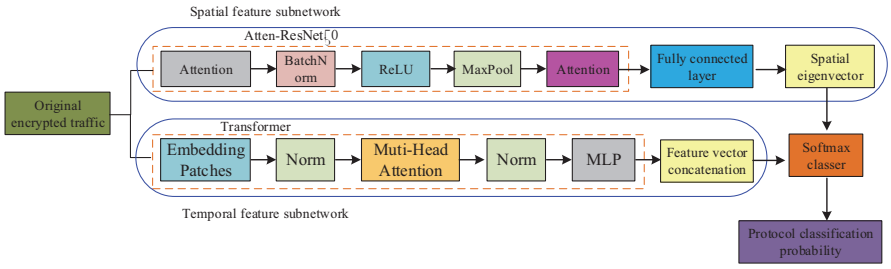


Figure 3 Schematic diagram of parallel model architecture.

timing characteristics represented by the traffic byte stream, the encoder part of the Transformer model is used to effectively capture long-distance dependencies in the sequence and process the associated data of complex contexts in protocol interactions [25]. The convolution operation extracts the local pattern of the image through a learnable filter, and the process can be expressed as Equation (1) [26].

$$O_k = g\left(c_k + \sum_i V_{i,k} \otimes I_i\right) \tag{1}$$

In Equation (1), I_i and O_k are the i-th input and k-th output feature map. $V_{i,k}$ is the convolution kernel weight connecting the input and output, $\otimes$ is the convolution operation, and c_k is the bias term. ReLU is selected as the activation function $g()$ to enhance the nonlinear expression ability and alleviate the vanishing gradient problem. The AM focuses computing resources on the "salient" areas that contribute the most to the classification task, thereby suppressing interference from noise and irrelevant background. The calculation of attention weight is shown in Equation (2) [27].

$$Attention(Q', K', V') = softmax\left(\frac{Q'K'^T}{\sqrt{d_k}}\right)V' \tag{2}$$

Q' and K' are the keys and values of the feature map extracted by CNN, V' is the learnable query vector, T is the transpose symbol, and $\sqrt{d_k}$ denotes the dimension of the query and key. In the process of temporal feature extraction, first, each data packet in a network session $Session = \{p_1, p_2, p_3, \ldots, p_m\}$ is mapped into a vector representation through the embedding layer, and an embedding vector sequence is obtained. Afterwards, the sequence is input into a stacked Transformer encoder. Each encoder layer uses a multi-head self-AM to enable the representation of each packet to aggregate information from all other packets in the sequence. Finally, all updated packet representations are spliced and passed through a linear layer to obtain the timing feature vector Z_t of the entire network session, as shown in Equation (3) [28].

$$\begin{cases} u_j = TransformerEnc(s_j), \quad 1 \le j \le m \\ Z_t = W_{out}[u_1, u_2, \ldots u_m] \end{cases} \tag{3}$$

In Equation (3), u_m is the sequence information of data packet s_j after being processed by the AM, and m is the number of data packets. The spliced

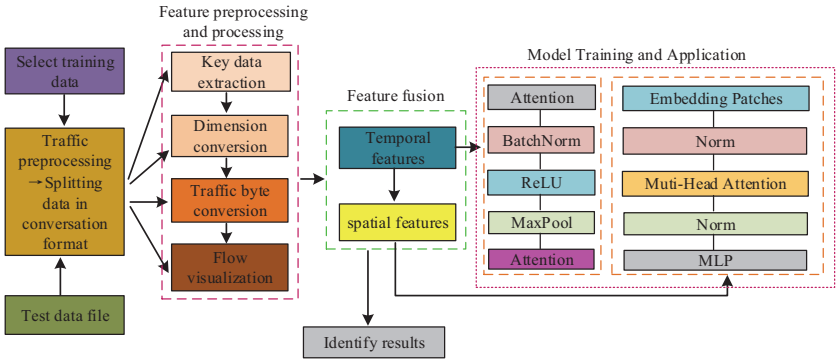


Figure 4 Encrypted traffic protocol identification process.

fusion feature vector h_{fused} is input into a Softmax classifier and outputs the probability distribution of various protocols. Equation (4) is the output result of the agreement probability [29].

$$\hat{y} = softmax(W_{final} \cdot h_{fused} + b_{final}) \tag{4}$$

In Equation (4), W_{final} and b_{final} are the weight and bias terms of the final classification layer. Figure 4 shows the encrypted traffic protocol identification process.

In Figure 4, protocol traffic identification needs to first segment independent communication sessions from unprocessed data packets, perform data cleaning and preprocessing, and simultaneously construct its characteristics in the form of timing byte streams and spatial grayscale images. Afterwards, these paired features are input into a parallel spatiotemporal fusion model for training, and the same preprocessing and feature construction steps are performed on new, unknown traffic. Then, it is input into the trained model, and its predicted protocol category label is directly output to realize protocol recognition.

4 Security and Performance Evaluation of Integrated Commercial Ciphertext Recognition Algorithms

4.1 Environmental and Related Parameters

To comprehensively verify the effectiveness of the research algorithm, the performance test of the ciphertext identification algorithm and the encrypted traffic protocol identification algorithm is performed. The hardware platform

is a graphics workstation equipped with Intel(R) Core (TM) i7-12700H CPU, 32GB DDR5 memory, and NVIDIA GeForce RTX 3070 Ti GPU (8GB video memory). The software environment is built on the Ubuntu 20.04.5 LTS operating system, the deep learning framework uses PyTorch 1.12.1, the programming language is Python 3.9, and CUDA 11.6 is used for GPU acceleration. The system back-end service is deployed in a Docker container, and the database utilizes MySQL 8.0. For the Multi-dimensional Randomness Feature with ResNet (MRF-ResNet), pre-trained ResNet50 is used as the backbone network. For the Transformer branch in STF-Net, the key hyperparameters are set as follows: sequence length of 64, embedding dimension of 128, number of multi-head attention heads of 8, and encoder layers of 6. To prevent overfitting, various regularization strategies are employed in the study, including applying Dropout ($p = 0.5$) after all fully connected layers, using the AdamW optimizer and setting weight decay (L2 regularization) to 1e-4, and stopping training if the validation set loss does not improve for 10 consecutive epochs. This study constructs a ciphertext dataset containing multiple standard cryptographic algorithms, covering commercial cryptographic algorithms, internationally accepted algorithms, and unencrypted plaintext data. Files of varying lengths are encrypted. Each algorithm and parameter combination (such as different key lengths, different working modes) generates 10,000 samples, totaling approximately 150,000 sample files. The dataset is segmented into sets of training and test at a ratio of 6:4, and the ISCX-VPN-NonVPN dataset is used to obtain regular encrypted traffic. More than 50,000 session flows per protocol class are collected. After data preprocessing, to enhance the statistical reliability of the results, 5-fold cross-validation is used in the study: for each experiment, the training set and validation set are merged and evenly divided into 5 parts, with 1 part used as the validation set and the remaining 4 parts used for training. Finally, the average of the 5 validation results is taken as a stable estimate of the model performance. To conduct a comprehensive evaluation, this study selects indicators covering classification performance, operational efficiency, resource overhead, and security for evaluation. To ensure the information protection of ciphertext blocks during training/testing, the study considers the entire ciphertext file or network session as an indivisible unit when partitioning the dataset. The list of all raw files/sessions is randomly shuffled and distributed according to a set ratio. A file (and all the blocks it generates) or a session (and all the data packets it contains) either belongs entirely to the training set or the testing set, and there will never be a situation where one part is in the training set and the other part is in the testing set.

4.2 Performance Test of Ciphertext Characteristics Under Random Distribution

To verify the performance of the proposed MRF-ResNet, this study selects Support Vector Machine-Histogram of Oriented Gradients (SVM-HOG), TextTextCNN, and C4.5 Decision Tree Algorithm-Byte Frequency (C4.5-ByteFreq) for comparison. Among them, SVM-HOG represents the idea of "traditional machine learning+manual image features", C4.5-ByteFreq represents the classic method based on "shallow statistical features (such as byte frequency)", and TextCNN is a widely used "basic deep learning model" for sequence data. By comparing with these models, the advantages of "randomness visualization" and "spatiotemporal fusion" strategies can be clearly demonstrated. Figure 5 shows the classification results and ablation experiment of the ciphertext recognition algorithm.

In Figure 5(a), MRF-ResNet is better than other algorithms in various classification indicators, with an average accuracy of 98.83%. The average accuracy of SVM-HOG, C4.5-ByteFreq, and TextCNN does not exceed 95%, and their average F1 scores are only 86.13%, 88.89%, and 94.46%. In Figure 5(b), the feature channel of the baseline model is the Random Feature Grayscale Image (RFGI). The feature channel of Variant A is RFGI+HBSGI, and the feature channel of Variant B is RFGI+BCSGI. The research model is a combination of three grayscale image features. The average recognition accuracy of the research algorithm exceeds 95%, verifying the innovative value of the multi-dimensional feature fusion strategy. Better than C4.5-ByteFreq, it proves the value of deep learning and multidimensional features. Better than TextCNN, it proves the effectiveness of converting ciphertext into 2D images and fusing multi-channel information. The superiority of SVM-HOG proves that end-to-end deep learning feature extraction is superior to manual feature extraction. Afterwards, a random security analysis is conducted on these algorithms, as listed in Table 1.

Among the test items in Table 1, 1–8 respectively represent frequency check, intra-block frequency test, running test, overlapping module matching test, linear complexity test, sequence test, approximate entropy test, and random walk test. MRF-ResNet has passed the key stream sequence test project. TextCNN fails the test on items 2 and 6. SVM-HOG fails many test items. Table 2 displays the computational performance results of various ciphertext recognition algorithms.

In Table 2, although MRF-ResNet has a large model volume and parameter count due to the use of ResNet18 structure, its single-sample inference

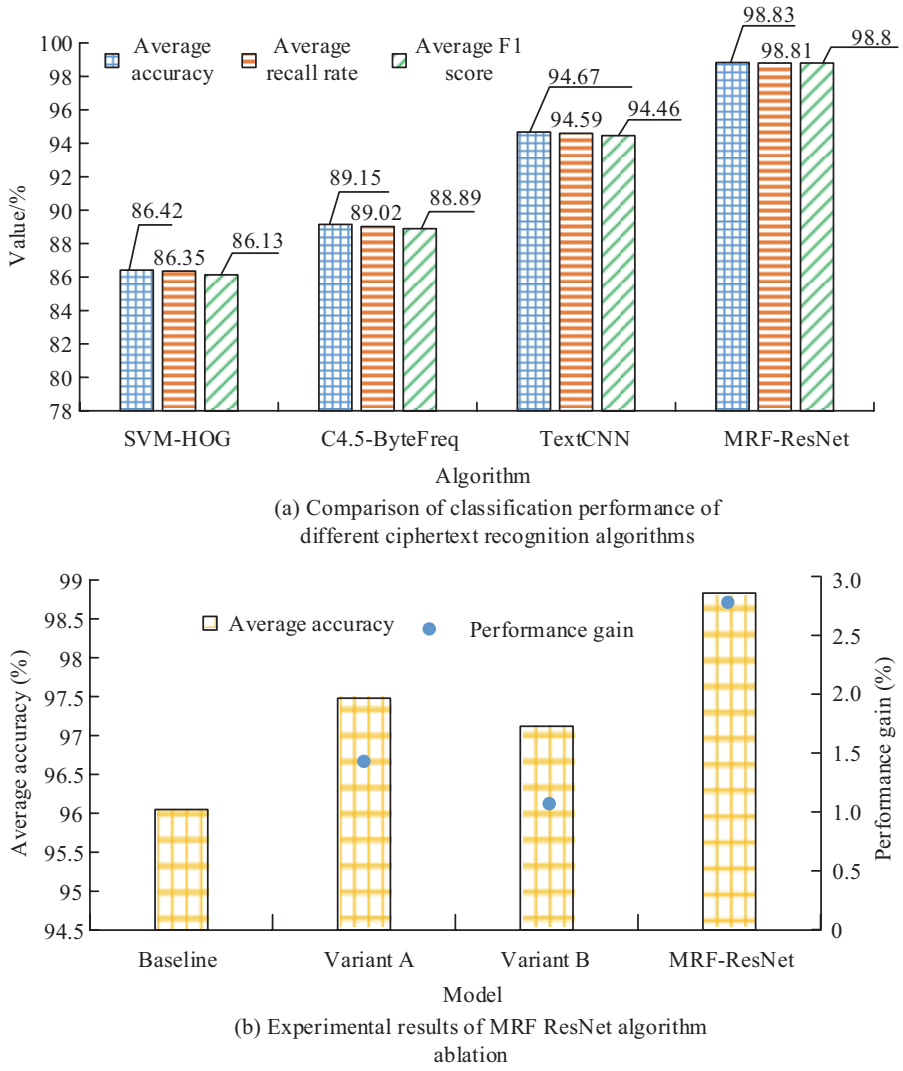


Figure 5 Classification and ablation results of ciphertext recognition algorithm.

delay in 5-fold cross-validation is 4.6 ± 0.4 ms, slightly higher than TextCNN (3.1 ± 0.3 ms). However, its throughput (217 ± 18 samples/s) can still meet the needs of the vast majority of offline analysis scenarios. The standard deviation of all efficiency indicators is less than 10% of the mean, indicating that the model has stable operational efficiency in multiple experiments.

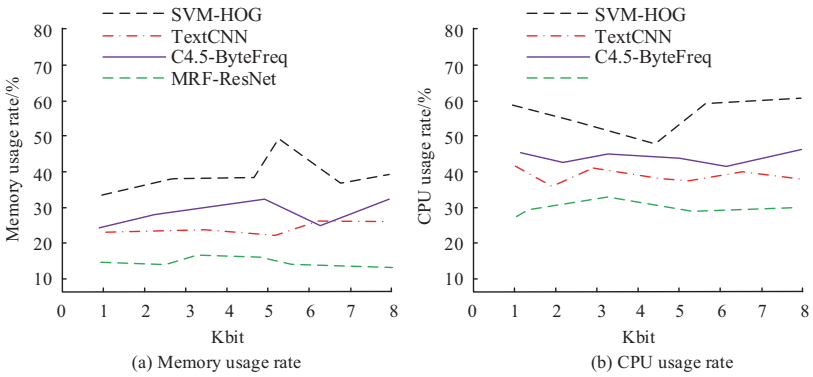
Table 1 Randomness test results

	MRF-ResNet		TextCNN		C4.5-ByteFreq		SVM-HOG	
Model	p	Result	p	Result	p	Result	p	Result
1	0.31056	√	0.50446	√	0.51895	√	0.56393	√
2	0.33031	√	0.52421	×	0.53893	√	0.58391	√
3	0.40284	√	0.59674	√	0.60324	√	0.64822	√
4	0.27194	√	0.46584	√	0.38139	×	0.42637	×
5	0.31313	√	0.50703	√	0.56028	√	0.60526	√
6	0.28415	√	0.47805	×	0.33211	×	0.37709	√
7	0.34168	√	0.53558	√	0.26024	√	0.30522	×
8	0.39885	√	0.59275	√	0.52191	√	0.56689	×

Note: "√" indicates pass; "×" means fail.

Table 2 Efficiency and resource cost comparison of different cryptography recognition algorithms

Algorithm Model	Model Parameter Quantity (M)	Model Volume (MB)	Single Sample Inference Latency (ms)	Throughput (Samples/ Second)
SVM-HOG	–	58.7 ± 0.2	15.2 ± 0.5	65 ± 12.5
C4.5-ByteFreq	–	21.3 ± 0.4	8.5 ± 0.1	117 ± 13.6
TextCNN	4.8 ± 5.31	18.3 ± 0.1	3.1 ± 0.3	322 ± 11.7
MRF-ResNet	11.2 ± 2.16	42.8 ± 0.6	4.6 ± 0.4	217 ± 18.1



(a) Memory usage rate (b) CPU usage rate

Figure 6 Performance of three algorithms in handling sensitive privacy data.

In Figure 6(a), the mean memory usage of MRF-ResNet is 18.24%, while that of SVM-HOG, C4.5-ByteFreq, and TextCNN is 33.68%, 27.35%, and 24.33%. In Figure 6(b), the CPU usage of MRF-ResNet exceeds 75%, which is significantly higher than the comparison algorithm, indicating that it can

Table 3 Encryption traffic classification performance of different models

Algorithm	Accuracy (%)	Recall Rate (%)	F1 Score (%)	Model Parameter Quantity (M)	Single Batch Inference Delay (ms)	Robustness to Unknown Traffic (%)	Resilience Against Attacks (%)	Model Interpretability (%)
Research model	99.48	99.50	99.49	7.8	4.5	92.5	95.2	65.8
EAPT	99.05	99.12	99.10	6.5	5.2	90.8	85.5	42.0
TFE-GNN-Light	99.35	99.41	99.38	5.2	3.8	89.5	87.3	62.5
ESDBO-MSCNN	87.10	86.50	86.80	10.5	4.0	75.0	82.3	45.3
XPSF	98.55	98.45	98.50	<1.0	4.2	85.0	79.6	92.5
TransECA-Net	98.30	98.20	98.25	8.5	5.5	88.5	87.4	43.8
NetST	99.20	99.28	99.24	7.2	4.8	91.5	88.5	40.5

ensure performance while ensuring data security. At the same time, further research methods will be applied to the Adversarial Pre-Trained Transformer Encrypted traffic classification model (EAPT) [30], the lightweight graph encrypted traffic classification encoder (TFE-GNN-Light) [31], the Elite Strategy Dung Beetle Optimization algorithm optimized Multi-Scale CNN (ESDBO-MSCNN) [32], and the interpretable path signature feature based encrypted traffic classification (XPSF) [33]. Comparison is conducted between the Transformer-A-based model with Efficient Channel Attention for Encrypted Traffic Classification (TransECA-Net) [34] and the Swin Transformer Network Encrypted Traffic Classification Based on Swin Transformer (NetST) [35] to better analyze the model performance of encrypted traffic. The results are shown in Table 3.

The results in Table 3 indicate that in terms of core classification performance, the research model outperforms all comparison models with an accuracy of 99.52% and an F1 score of 99.49%, including equally strong TFE-GNN-Light (F1 score 99.38%) and NetST (F1 score 99.24%). This indicates that the strategy of integrating random features with spatiotemporal relationships can more accurately capture the essential differences of encrypted traffic than models that rely solely on temporal or structural features, thereby achieving better classification performance. In terms of robustness to unknown traffic, the generalization accuracy of the study (92.5%) is significantly higher than that of NetST (91.5%) and EAPT (90.8%), demonstrating its stronger generalization ability to emerging and unseen traffic types. This is mainly attributed to the introduction of randomness features, which provide a universal discriminative criterion that does not depend on specific application behavior patterns. The "adversarial attack resilience" value of the research model (95.2%) is nearly 7% higher

than the suboptimal NetST (88.5%). The reason is that adversarial attacks often deceive models by tampering with temporal features such as packet length and latency. The cryptographic randomness statistics relied upon by research models are difficult to effectively forge, thus constructing a natural defense barrier. In terms of model efficiency, the research model achieves an excellent balance between 7.8M parameter count and 4.5 ms inference delay. Although it is not as lightweight as the TFE-GNN-Light (5.2 M, 3.8 ms), its efficiency is sufficient to meet real-time detection requirements. The research model balances operational efficiency and interpretability, and has good performance in classifying encrypted traffic.

4.3 Encrypted Traffic Protocol Identification Performance Analysis

To verify the performance of the Spatio-Temporal Fusion Network (STF-Net-MRF-ResNet), this study selects 1D-CNN, LSTM, and Flow Sequence-Residual Graph Convolutional Networks (FS-RGCN) for comparison. Figure 7 shows the classification performance of different encrypted traffic protocol identification algorithms.

In Figure 7(a), under different traffic sample protocol numbers, the four algorithms show differences in the fluctuations of the recognition classification curves. Among them, the average recognition classification accuracy of 1D-CNN, LSTM, FS-RGCN, and STF-Net-MRF-ResNet is 88.64%, 85.12%, 82.14%, and 93.26%. In Figure 7(b), the average recognition and classification accuracy of 1D-CNN, LSTM, and FS-RGCN does not exceed 90%, which is less than 92.18% of the research algorithm. In Figure 7(c), the recognition and classification accuracy of each comparison algorithm differs greatly. Except for STF-Net-MRF-ResNet, the values of the other algorithms do not exceed 85%. The research algorithm shows excellent performance on all protocol categories, especially when distinguishing national secret SSL and TLS 1.3, which have similar structures but different cipher suites, and identifying post-quantum cryptographic traffic (Saber.PAKE). Table 4 shows the ablation experimental data of the research algorithm.

In Table 4, the branches that process spatial and temporal features in parallel are indispensable for the final performance, and the average accuracy of the fused model ($98.25 \pm 0.28\%$) far exceeds any spatial ($95.17 \pm 0.52\%$) and temporal feature ($94.39 \pm 0.61\%$) branches. Table 5 shows the real-time performance of different encrypted traffic protocol identification algorithms.

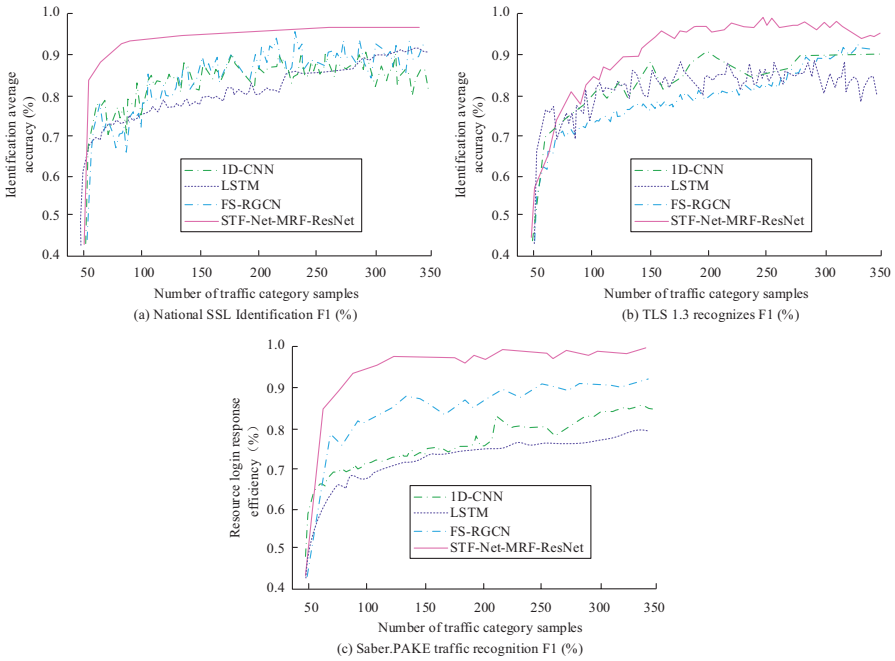


Figure 7 Comparison of classification performance of different encryption traffic protocol identification algorithms.

Table 4 Experimental results of STF-Net-MRF-ResNet

Model Variant	Feature Processing Branch	Average Accuracy (%)	Performance Gain (%)
ResNet50-Branch	Only spatial features (Attention-ResNet50)	95.17 ± 0.52^{b}	–
Transformer-Branch	Only temporal features (Transformer Encoder)	94.39 ± 0.61^{b}	–
STF-Net-MRF-ResNet	Parallel fusion of spatiotemporal features	98.25 ± 0.28^{a}	+3.08 (vs CNN)

Note: Values with different superscript letters (a, b) within the same column are significantly different ($p < 0.01$). The gain is calculated compared to the best-performing single-branch variant (ResNet50-Branch, denoted as "b").

In Table 5, STF-Net-MRF-ResNet has the highest training time (9.5 h) and resource usage (4.5 GB) due to its dual-branch parallelism and complex Transformer structure, and the inference delay (4.1 ms) is also relatively long. However, its throughput of over 240 sessions/s is sufficient to handle

Table 5 Real-time performance analysis

Algorithm Model	Training Time (h)	Single Session Inference Latency (ms)	Throughput (Sessions/ Second)	Memory Usage (GB)
1D-CNN	5.2	1.8	555	2.1
LSTM	7.8	3.5	285	3.4
FS-RGCN	6.1	2.4	416	2.8
STF-Net-MRF-ResNet	9.5	4.1	243	4.5

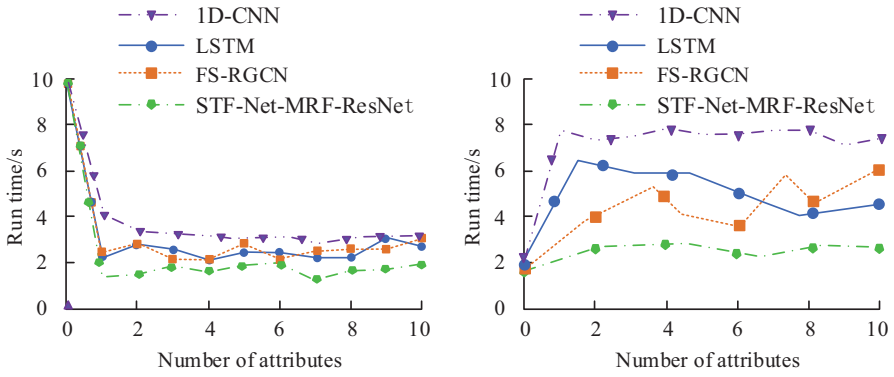


Figure 8 Computational efficiency of different algorithms.

the real-time monitoring needs of medium-sized networks. Afterwards, the operational efficiency of the protocol identification algorithms is compared, as shown in Figure 8.

In Figure 8(a), the protocol encryption operation efficiency under STF-Net-MRF-ResNet is higher, and its runtime under different number of attributes is shorter than other methods. The second-performing FS-RGCN and LSTM have a runtime of no more than 4 s in the later stage. In Figure 8(b), the encryption time spent by the research algorithm is always smaller than that of the comparison algorithms. The results of analyzing the data processing speed, throughput, and data query efficiency of the above algorithms are exhibited in Table 6.

In Table 6, 1D-CNN, LSTM, and FS-RGCN all take more than 5 seconds, and their average speeds are 14.33 MB/s, 22.39 MB/s, and 34.12 MB/s, indicating low operating efficiency. For system throughput and access control cost, STF-Net-MRF-ResNet has better values, the communication cost does not exceed 3 KB, and the control effect is obvious.

Table 6 The application effect of commercial encryption recognition algorithm

					Access Control Cost	
Model	Data Size (MB)	Time (s)	Average Speed (MB/s)	Throughput (tps/s)	Index Re Encryption Communication Cost (kb)	Key Generation Communication Cost (kb)
1D-CNN	256	9.34	14.33	1536	2.43	3.36
LSTM	256	11.33	22.39	1127	3.26	4.21
FS-RGCN	256	6.25	34.12	1928	3.24	3.77
STF-Net-MRF-ResNet	256	4.27	63.25	2415	0.85	2.12

5 Summary

In this study, the ciphertext feature recognition algorithm and protocol traffic recognition algorithm of commercial cryptography are designed by innovatively combining the randomness characteristics and spatio-temporal relationship. MRF-ResNet achieved 98.83% ciphertext algorithm recognition accuracy, while the average accuracy of SVM-HOG, C4.5-ByteFreq, and TextCNN did not exceed 95%. STF-Net achieved 98.25%. The integration of randomness features, byte stream structure features, and bit accumulation features could significantly improve recognition accuracy performance. Its ciphertext recognition algorithm had an average recognition accuracy of over 95%. Under different traffic sample protocol numbers, the average recognition and classification accuracy of STF-Net-MRF-ResNet was 93.26%, which was better than other algorithms. Its identification accuracy under different protocol suites exceeded 95%, and it could effectively distinguish between SSL and TLS 1.3, which had similar structures but different cipher suites, and identify post-quantum cryptographic traffic. STF-Net-MRF-ResNet supported real-time detection of 240 sessions/s, and its protocol encryption operation efficiency was high. The reason why research methods can achieve better classification advantages and feature recognition accuracy compared to other comparative methods is due to their innovative multidimensional feature representation and powerful feature extraction network. Unlike baseline models that rely solely on single-dimensional features, MRF-ResNet integrates three complementary feature dimensions: raw byte structure (hexadecimal graph), bit cumulative distribution (cumulative sum graph), and global and local pseudo-random statistics (NIST randomness graph). This “three-way” input provides the model with much richer and more comprehensive information than single-byte sequences or frequency statistics. As a feature extractor, ResNet50’s deep residual structure can

effectively learn complex feature levels from low-level textures to high-level semantics. This can automatically discover subtle but discriminative combination patterns of different cryptographic algorithms in terms of randomness distribution, byte structure, and statistical patterns. The research method can effectively ensure the security of commercial password applications, ensure data security, and reduce misjudgments caused by weak randomness and suite confusion. However, this study still has certain shortcomings, such as the lack of long-period drift testing in the context of extremely large traffic and the lack of full coverage of post-quantum cipher suites. The proposed model belongs to a multi-class supervised learning framework, whose main goal is to perform high-precision compliance detection on a set of known and predefined commercial cryptographic algorithms and protocol suites. Therefore, for encryption algorithms or protocols that have not yet appeared in the training set, the model cannot directly identify its specific category and may misjudge it as a known category with the most similar characteristics. Future work can explore combining this framework with open-set recognition or anomaly detection techniques to achieve alerting for unknown encryption types. This study does not specifically focus on multi-channel sessions such as HTTP/2 and QUIC. Handling complex traffic such as mixed or multi-path sessions requires more sophisticated application-layer protocol parsing and flow reassembly logic. Therefore, to overcome this limitation, future attempts can be made to introduce an application-layer protocol parsing module to achieve data stream reassembly and consider embedding additional flow vectors in the encoder to enhance the awareness and attention of the flow. Multi-task learning frameworks can be used to provide richer semantic information for network traffic management. Future work will further consider introducing self-supervised pre-training to alleviate labeling dependence, design lightweight dynamic convolution to reduce the model, and try to embed an online incremental learning framework to achieve continuous evaluation.

Funding

The research is supported by China Yangtze Power Co., Ltd., Research on the Application of Chip-Level Self-developed and Controllable Hardware in Cascade Dispatching Automation Systems, Project Z242302028.

References

[1] Wiefling S, Jørgensen P R, Thunem S, Iacono L L. Pump up password security! Evaluating and enhancing risk-based authentication on a real-world large-scale online service. ACM Transactions on Privacy and Security, 2022, 26(1): 1–36. DOI: 10.1145/3546069.

[2] Oladoyinbo T O, Oladoyinbo O B, Akinkunmi A I. The Importance Of Data Encryption Algorithm In Data Security. Current Journal of International Organization of Scientific Research Journal of Mobile Computing & Application (IOSRJMCA), 2024, 11(2): 10–16. DOI: 10.9790/0050-11021016.

[3] Kumar M, Kondaiah C, Pais A R, Rao R S. Machine learning models for phishing detection from TLS traffic. Cluster Computing, 2023, 26(5), 3263–3277. DOI: 10.1007/s10586-023-04042-6.

[4] Patel A K, Paul D, Giri S, Chaudhary S, Gautam B. Gradient-based facial encoding for key generation to encrypt and decrypt multimedia data. arXiv preprint arXiv:2412.06927, 2024. DOI: 10.48550/arXiv.2412.06927.

[5] Shi W, Zhang J, Chen X, Ye X. PCDP-CRLPPM: a classified regional location privacy-protection model based on personalized clustering with differential privacy in data management. The Computer Journal, 2025, 68(4): 372–396. DOI: 10.1093/comjnl/bxae118.

[6] Zhou L, Liu C, Tian L, Wang J, Liu C, Yu X. Network security analysis based on feature selection and optimized fireworks algorithm. Scientific Reports, 2025, 15(1): 44188. DOI: 10.1038/s41598-025-27855-4.

[7] Wanjau S K, Wambugu G M, Oirere A M, Muketha G M. Discriminative spatial-temporal feature learning for modeling network intrusion detection systems. Journal of computer security, 2024, 32(1): 1–30. DOI: 10.3233/JCS-220031.

[8] Baskar K, Muthumanickam K, Vijayalakshmi P, Kumarganesh S. A Strong Password Manager Using Multiple Encryption Techniques. Journal of The Institution of Engineers (India): Series B, 2025, 106(4): 1207–1214. DOI: 10.1007/s40031-024-01144-6.

[9] Hughes J P, Diffie W. The Challenges of IoT, TLS, and Random Number Generators in the Real World: Bad random numbers are still with us and are proliferating in modern systems. Queue, 2022, 20(3): 18–40. DOI: 10.1145/3546933.

[10] Kumbhakar D, Sanyal K, Karforma S. An optimal and efficient data security technique through crypto-stegano for E-commerce. Multimedia Tools and Applications, 2023, 82(14): 21005–21018. DOI: 10.1007/s11042-023-14526-7.

[11] Chen, E. "Analysis of E-Commerce Security Protection Technology Based on YOLO Algorithm Optimized by Lightweight Neural Network". Journal of Cyber Security and Mobility, 2025, 14 (04): 849–876, DOI: 10.13052/jcsm2245-1439.1444.

[12] Rasheed A F, Zarkoosh M, Elia F R. Enhancing graphical password authentication system with deep learning-based arabic digit recognition. International journal of information technology, 2024, 16(3): 1419–1427. DOI: 10.1007/s41870-023-01561-8.

[13] Singamaneni K K, Muhammad G, Ali Z. A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers. IEEE Transactions on Consumer Electronics, 2023, 70(1): 1092–1101. DOI: 10.1109/TCE.2023.3331306.

[14] HariKrishna A, Bindu D, Sowmya C, Varshitha G, Tharunasree C. Enhanced Secure Communication Protocol with Pipelined Advanced Encryption for Mobile Networks. Turkish Journal of Computer and Mathematics Education, 2024, 15(1): 205–211. DOI: 10.61841/turcomat.v15i1.14613.

[15] Jean A, Alherbe T. Gid Crypto: Application for End-to-End Encrypt and Decrypt E-mail and Data. ASEAN Journal of Scientific and Technological Reports, 2024, 27(2): 90–102. DOI: 10.55164/ajstr.v27i2.251127.

[16] Grammatopoulos A V, Politis I, Xenakis C. Blind software-assisted conformance and security assessment of FIDO2/WebAuthn implementations. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2022, 13(2): 96–127. DOI: 10.22667/JOWUA.2022.06.30.096.

[17] Seyhan K, Akleylek S. A new password-authenticated module learning with rounding-based key exchange protocol: Saber. PAKE. Journal of Supercomputing, 2023, 79(16): 17859–17896. DOI: 10.1007/s11227-023-05251-x.

[18] Luo Y, Liu J, Gong C, Li T. An efficient heterogeneous parallel password recovery system on MT-3000. The Journal of Supercomputing, 2025, 81(1): 38. DOI: 10.1007/s11227-024-06532-9.

[19] Adeniyi A E, Abiodun K M, Awotunde J B, Olagunju M, Ojo O S, Edet N P. Implementation of a block cipher algorithm for medical information

security on cloud environment: using modified advanced encryption standard approach. Multimedia Tools and Applications, 2023, 82(13): 20537–20551. DOI: 10.1007/s11042-023-14338-9.

[20] Kondaiah C, Pais A R, Rao R S. An ensemble learning approach for detecting phishing URLs in encrypted TLS traffic. Telecommunication Systems, 2024, 87(4): 1015–1031. DOI: 10.1007/s11235-024-01229-z.

[21] Rajesh Kanna P, Santhi P. Exploring the landscape of network security: a comparative analysis of attack detection strategies. Journal of Ambient Intelligence and Humanized Computing, 2024, 15(8): 3211–3228. DOI: 10.1007/s12652-024-04794-y.

[22] Abudalou M. Enhancing Data Security through Advanced Cryptographic Techniques. Int. J. Comput. Sci. Mob. Comput., 2024, 13(1): 88–92. DOI: 10.47760/ijcsmc.2024.v13i01.007.

[23] Jangam S K. Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices. International Journal of AI, BigData, Computational and Management Studies, 2023, 4(3): 82–91. DOI: 10.63282/3050-9416.IJAIBDCMS-V4I3P109.

[24] Salem R B, Aimeur E, Hage H. A Multi-Party Agent for Privacy Preference Elicitation. Artificial Intelligence and Applications, 2023, 1(2): 98–105. DOI: 10.47852/bonviewAIA2202514.

[25] Ibrahım S, Zengin A, Hızal S, Akhter A S, Altunkaya C. A novel data encryption algorithm to ensure database security. Acta Infologica, 2023, 7(1): 1–16. DOI: 10.26650/acin.1134979.

[26] Akshaya S. ResNet50-based deep convolutional neural network for zero-day attack prediction and detection. International Journal of Advanced Technology and Engineering Exploration, 2025, 12(124): 507. DOI: 10.19101/IJATEE.2024.111100055.

[27] Yu W, Liu C, Ni L, et al. Password region attribute classification based on multi-granularity cascade fusion. Connection Science, 2025, 37(1): 2461092. DOI: 10.1080/09540091.2025.2461092.

[28] Yılmaz A G, Turhal U, Nabiyev V. Multi-input hybrid face presentation attack detection method based on simplified Xception and channel attention mechanism. Expert Systems with Applications, 2025, 283: 127610. DOI: 10.1016/j.eswa.2025.127610.

[29] Pan J, Chen Y, Zhao C, et al. Long Text Classification Model Based on Transformer Sliding Window and Threshold Optimization. Journal of Internet Technology, 2025, 26(2): 231–240. DOI: 10.70003/160792642025032602008.

[30] Zhan M, Yang J, Jia D, Fu G. EAPT: An encrypted traffic classification model via adversarial pre-trained transformers. Computer Networks, 2025, 257: 110973. DOI: 10.1016/j.comnet.2024.110973.
[31] Chen Z W, Wei X X, Wang Y S. Encrypted traffic classification encoder based on lightweight graph representation. Scientific Reports, 2025, 15(1): 28564. DOI: 10.1038/s41598-025-05225-4.
[32] Peng Q, Fu X, Lin F, Zhu X, Ning J, Li F. Multi-Scale Convolutional Neural Networks optimized by elite strategy dung beetle optimization algorithm for encrypted traffic classification. Expert Systems with Applications, 2025, 264: 125729. DOI: 10.1016/j.eswa.2024.125729.
[33] Xu S J, Kong K C, Jin X B, Geng G G. Unveiling traffic paths: Explainable path signature feature-based encrypted traffic classification. Computers & Security, 2025, 150: 104283. DOI: 10.1016/j.cose.2024.104283.
[34] Liu Z, Xie Y, Luo Y, Wang Y, Ji X. TransECA-Net: A transformer-based model for encrypted traffic classification. Applied Sciences, 2025, 15(6): 2977. DOI: 10.3390/app15062977.
[35] Zhang J, Zhao H, Feng Y, Cai Z, Zhu L. NetST: Network Encrypted Traffic Classification Based on Swin Transformer. Computers, Materials & Continua, 2025, 84(3). DOI: 10.32604/cmc.2025.066367.

Biographies

Jiang Luo, male, born in January 1989, from Wuhan, Hubei Province, of Han ethnicity. He graduated from Wuhan University of Technology with a bachelor's degree in Computer Science and Technology in 2012, and obtained a master's degree in Computer Application from Wuhan University of Technology in 2015. His research field is the operation and maintenance of hydropower automation systems.

Work Experience: From 2015 to present, he has been working at the Three Gorges Cascade Dispatching& Communication Center of China Yangtze Power Co., Ltd. Position: Business Supervisor.

Fuxin Hong, male, born in January 1984, from Yichang, Hubei Province, of the Tujia ethnicity. He graduated from Nanjing University of Posts and Telecommunications with a bachelor's degree in Computer Science and Technology in 2007, and obtained a master's degree in the same field from Nanjing University of Posts and Telecommunications in 2010. His research field is the operation and maintenance of hydropower automation systems.

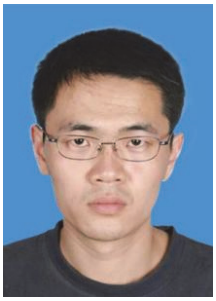
Work Experience: From 2010 to present, he has been working at the Three Gorges Cascade Dispatching& Communication Center of China Yangtze Power Co., Ltd. Currently, he serves as the Deputy Director of the Automation Department.
Academic Background: 5 patents, 3 academic awards.

Shuai Liu, male, born in March 1985, from Chengdu, Sichuan Province, of Han ethnicity. He graduated from Chongqing University with a bachelor's degree in Electrical Engineering and Automation in 2007, and

obtained an engineering master's degree from Chongqing University in 2021. His research field is: Automation of River Basin Hydropower Station Group Dispatching. Work Experience: From 2007 to present, he has been working at the Three Gorges Cascade Dispatching& Communication Center of China Yangtze Power Co., Ltd. as the Automation Director. Academic Background: 2 academic papers have been published, and 5 patents have been obtained.

Yang Yang, born in October 1987, female, from Zigong, Sichuan Province, of Han ethnicity. She graduated from Sichuan University with a bachelor's degree in Electrical Engineering and Automation in 2010. Research field: Operation and maintenance of hydropower automation systems.

Work experience: From 2010 to 2026, she worked at China Yangtze Power Co., Ltd. Currently, she serves as the director of the Kunming Branch of the Automation Department.



Hailong Chi, born in August 1975, male, from Yantai City, Shandong Province. Han ethnicity. He graduated from Harbin Institute of Technology

in 2004 with a master's degree in Electrical Engineering and Automation. Research field: Power Dispatch Automation System.

Work Experience: Since 2004, he has been working at Beijing IWHR Technology Co., Ltd. Position: Senior Development Manager. Academic Background: Obtained 2 patents and 3 academic papers.