Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

An Intelligent Decipher System to Examine Cipher Algorithms

***Ayad Osama Jalal*[1,]**

Faculty of Administration and Economics, Al-Iraqia University, Baghdad, Iraq. ayad.o.jalal@aliraqia.edu.iq

ARTICLE INFO

Article history:
Received: 27 /02/2026
Rrevised form: 13 /03/2026
Accepted : 15 /03/2026
Available online: 30 /06/2026

Keywords:

Neural Cryptanalysis, Deep Learning, ResNet, Attention-LSTM, AES, SPECK, Lightweight Cryptography, Automated Security Auditing

ABSTRACT

The high rate of cryptographic primitive development requires improved, automatic assessment structures that guarantee effective data security. The traditional cryptanalysis, which is mostly based on special linear and differential approaches, is both computationally infeasible and needs substantial domain knowledge. To overcome technical deficiencies like the Curse of Dimensionality and limitations under high-degree algebraic transformations, this paper presents the Intelligent Decipher System (IDS). The IDS architecture combines a Deep Residual Network (ResNet) and Attention-based Long Short-Term Memory (LSTM) to extract both spatial and sequential features, capturing differential properties and long-range dependencies. We compare the given system with reduced-round SPECK32/64 and AES-128, and classical polyalphabetic systems. The experimental findings indicate the IDS has a distinguishing accuracy of 92.4% on 5-round SPECK and that its bias detection is effective up to 7 rounds (61.5%), which is remarkably better than traditional differential distinguishers and baseline machine learning models. The framework offers a scalable black-box auditing device for detecting structural weaknesses in current lightweight cryptography.

MSC..

https://doi.org/ 10.29304/jqcsm.2026.18.22690

1. Introduction

Cryptography plays a critical role in providing the three aspects of confidentiality, integrity, and authenticity as required in digital security. Since cryptographic algorithms are becoming more and more complex, correspondingly, the methods of their evaluation or breaking cryptanalysis have to be improved. This development has prompted the incorporation of automated intelligent systems to respond to the modern day security issues [1]. Traditionally, a cipher's security has been defined by its resilience against specific mathematical attacks, most notably Differential and Linear Cryptanalysis [2]. However, these classical methods often require the exhaustive derivation of Difference Distribution Tables (DDT) or Linear Approximation Tables (LAT). With the ascent of Artificial Intelligence (AI) and Deep Learning (DL), the field of Neural Cryptanalysis has gained significant traction [3]. Recent literature indicates that this paradigm shift reduces the heavy reliance on human domain expertise for feature extraction [4]. The inherent ability of neural networks to approximate high-dimensional non-linear functions makes them exceptional tools for identifying subtle correlations within ciphertext that often elude conventional statistical tests [5]. Even though AI promises great achievements in cryptography, there are considerable gaps in the current landscape.

∗Corresponding author : Ayad Osama Jalal

Email addresses: ayad.o.jalal@aliraqia.edu.iq

Communicated by 'sub etitor'

These include the Absence of Coherent Frameworks, where existing literature is largely based on ad-hoc attacks on particularly lightweight ciphers (e.g. only SPECK or SIMON) without a systematized view of the study of multiple types of algorithms [3]. Recent research points to the fact that the lack of versatility in models impedes the evaluation of new hybrid algorithms. Furthermore, the Black-Box remains a challenge, as traditional tools look at ciphers as mathematical white boxes and lack automated systems to audit ciphers in a black-box environment to establish empirical security limits [4]. Additionally, Scalability issues persist, as current ML-based distinguishers do not work when the number of rounds of encryption is raised[5].

To address these evolving needs, the major purpose of this research is the creation of a unified, automated system of cryptographic auditing, which overcomes the constraints of the ad-hoc, cipher-specific neural distinguishers. This sort of generalized treatment is under fire because of the spread of various lightweight cryptography primitives [6]. Contrary to the conventional techniques of generating linear and differentiation tables, which take a lot of manual derivation [7], the Intelligent Decipher System (IDS) is a black-box evaluator that can assess block and classical ciphers. The major addition of this work is the hybrid ResNet and Attention-LSTM architecture [8] that instead of having to manually engineer features, a scalable AI-assisted security auditing baseline is established [9].

The existing body of neural cryptanalysis work is typically prone to a lack of generalization, often becoming ineffective when moving out of isolated testbeds [1, 10]. Moreover, current ML-based distinguishers are rarely able to achieve accuracy levels corresponding to theory as the number of rounds grows [8]. These gaps are filled in this paper through the introduction of the Intelligent Decipher System (IDS), which makes three main contributions. First, we suggest a new hybrid architecture that combines Residual Neural Networks (ResNet) to learn spatial bit-correlations and Attention-based LSTM to learn sequential dependencies [7]. Second, the IDS proposes automated extraction of features, meaning there is no longer a necessity to select the differential characteristics manually; with the deep learning approach, the system takes the task of discovering non-linear patterns and practically excludes the role of human cryptanalytic skills [8]. Lastly, this article offers solid experimental validation of the system to differentiate between ciphertext and random permutations, proving that the IDS is more accurate when it comes to auditing reduced-round block ciphers than typical machine learning classifiers such as Support Vector Machines (SVM) and Random Forests [9].

2. Related Work and Theoretical Scope

The evolution of cryptographic auditing has progressed from traditional mathematical models to advanced neural frameworks. This progression is rooted in both Classical and Neural Cryptanalysis Foundations, where classical attacks are based on the identification of high-probability hits (differentials) within the cipher substitution-permutation network (SPN) [2]. Gohr [3] established that a deep residual network could differentiate between SPECK32/64 ciphertext and random data better than the best known pure differential distinguisher. It produced a paradigm shift that demonstrated that neural networks can learn differential properties. On these basis, Deep Learning Solutions have experimented with different structures**.** Recent initiatives involved Support Vector Machines (SVM) and Random Forests. Yet, these shallow models were unable to model the very non-linear relationships in such contemporary ciphers as AES. Recent works have shown that traditional models do not have the ability to model the complex diffusion layers of deep cryptographic structures [10]. In order to solve it, discrete frameworks currently evaluate the cryptographic indistinguishability of lightweight block ciphers and verify the efficiency of ResNet-based designs [11]. To increase the analytical breadth even more, recent research has presented hybrid and scalable architectures. As an example, Jeong et al. [12] investigated scalable neural cryptanalysis on federated attacker system, which overcome the shortcoming of static models under distributed systems. In the same fashion, Bose et al. [13] adopted the use of transformer-based architectures to study long-range sequential dependency in the AES and SIMON structures. Sikdar and Kule [14] sought an optimization of the search of the differential paths based on reinforcement learning and autonomous agents, and Mukherjee et al. [15] demonstrated the attainment of the accuracy increase using the CNN-LSTM hybrid models through the combination of the spatial and temporal layers. Moreover, the results of Saravanan [16] revealed that Attention-ResNet models provide a great enhancement to the signal-to-noise ratio of neural distinguishers. The combination of these trends highlights the move to hybridity and automated auditing systems such as the new suggested IDS that uses ResNet and Attention-LSTM to address the limitations of classical neural distinguishers. The summary of these related methodologies and their key findings is presented in Table 1.

Table 1: Summary of related literature and methodologies

Study/Ref.	Target Algorithm	Methodology Used	Key Findings / Results
Biham & Shamir [2]	DES-like systems	Traditional Differential Cryptanalysis	Formulated the basis of mathematical attacks with DDTs.
Gohr [3]	SPECK32/64	Deep Residual Networks (ResNet)	Achieved higher accuracy than pure differential distinguishers on reduced rounds.
Meraouche et al. [4]	Various Ciphers	Neural Networks Survey	Comprehensive review of NN applications in breaking ciphers.
McKay et al. [6]	IoT-based Primitives	Lightweight NIST Report	Highlighted the need for automated auditing in lightweight security.
Rossi [7]	Symmetric Ciphers	Automated Differential Tools	Developed tools for automatic derivation of differential paths.
Kim et al. [8]	Lightweight Ciphers	Deep Learning Models	Revisited neural distinguishers for various lightweight algorithms.
Hospedales [9]	General Frameworks	Self-Supervised Learning	Explored feature representation without manual engineering.
Traditional ML (Various)[10]	Classical & Lightweight	SVM, Random Forest (RF)	Ultimately, had difficulties with non-linear relationships and modern diffusion layers such as AES.
Dani et al. [11]	Lightweight Ciphers	CNN-based Distinguishers	Effective round-reduced cipher training and accuracy.
Jeong et al. [12]	Block Ciphers	Federated CNN	Explored scalable neural cryptanalysis in distributed environments.
Bose et al. [13]	AES / SIMON	Transformer-based Architecture	Analyzed long-range sequential dependencies in cryptographic structures.
Sikdar & Kule [14]	SPECK	Reinforcement Learning	Optimized the search for differential paths using autonomous agents.
Mukherjee et al. [15]	Stream Ciphers	CNN-LSTM Hybrid	Proved that combining spatial and temporal layers enhances accuracy.
Saravanan [16]	SIMON / SPECK	Attention-ResNet	Improved signal-to-noise ratio using attention mechanisms in distinguishers.
Proposed IDS	SPECK, AES, Vigenère	Hybrid ResNet + Attention-LSTM	Scoring 92.4% on 5 round SPECK and 99.8% on classical ciphers.

3. Proposed Intelligent Decipher System (IDS)

To address the limitations of traditional cryptanalytic models, we propose a hybrid framework capable of capturing both spatial and temporal bit-level dependencies. Fig. 1 shows the structural interaction of the system.

3.1. System Architecture

Intelligent decipher system (IDS) is designed a multi-stage hybrid pipeline designed to capture complex cryptographic dependencies. The architecture enables a continuous information flow through three main stages between raw data as represented in bits to the ultimate semantic identification levels as illustrated in Fig. 1:

- Phase I: Feature Extraction (ResNet): The process begins with the bit-level fusion of Plaintext (P) and Ciphertext (C) into a merged tensor. This combined input enables the model to acquire the joint probability distribution and differential properties across the cipher states [7]. This stage utilizes 1D-Convolutional filters with a kernel size of 3 to attain local bit-interactions [11]. To capture long-range dependencies across multiple encryption rounds, we employ a stack of 10+ residual layers. The use of short-cut connections (skip connections) as highlighted in Fig. 1, ensures stable gradient flow.

- Phase II: Self-Attention Layer: The high-dimensional feature maps generated by the ResNet are passed to the self-attention layer. This component serves as the critical interaction bridge (Step 12 in Algorithm 1). By applying dynamic bit-weighting, the system identifies and prioritizes non-random bit-flips and high-probability differentials. This mechanism filters out statistical noise, ensuring that only the most relevant cryptographic features are passed to the temporal analysis stage as a weighted context.

- Phase III: Temporal Analysis (LSTM): To integrate the hybrid components, the high-dimensional feature maps from the deep residual stack are flattened and passed as sequential input to the Attention-LSTM layer. While ResNet efficiently extracts spatial bit-correlations, deep cryptographic primitives often suffer from the vanishing gradient problem when modeling high-round diffusion. By feeding the residual feature maps into the Attention-LSTM layer, the IDS treats the layer-wise transformations as a sequential time-step problem. This permits the network to memorize weak signals from the previous rounds that would then be swept away by strong diffusion in subsequent layers, which greatly increases the sensitivity of the distinguisher to subtle non-random biases [12].

- Final Identification: The resultant flattened feature map is sent through a dense layer whose activation is Sigmoid. This head outputs a probability score $p \in [0, 1]$, representing the statistical likelihood that the input is a valid Ciphertext/Plaintext pair rather than random noise, enabling high-precision classification.

The complete structural flow of this process is illustrated in Fig. 1, which emphasizes the transformation of low-level bits characteristics into high-level semantic models of the cipher structure. The interaction between the hybrid components as illustrated in the structural flow is not only a sequential interaction but an integrative interaction. Phase II uses the self-attention mechanism to refine the feature maps of Phase I to emphasize non-random biases. This makes sure that the Attention-LSTM units of Phase III are given a high-signal weighted context which makes the system able to retain a high distinguishing accuracy even though the encryption rounds are increased.

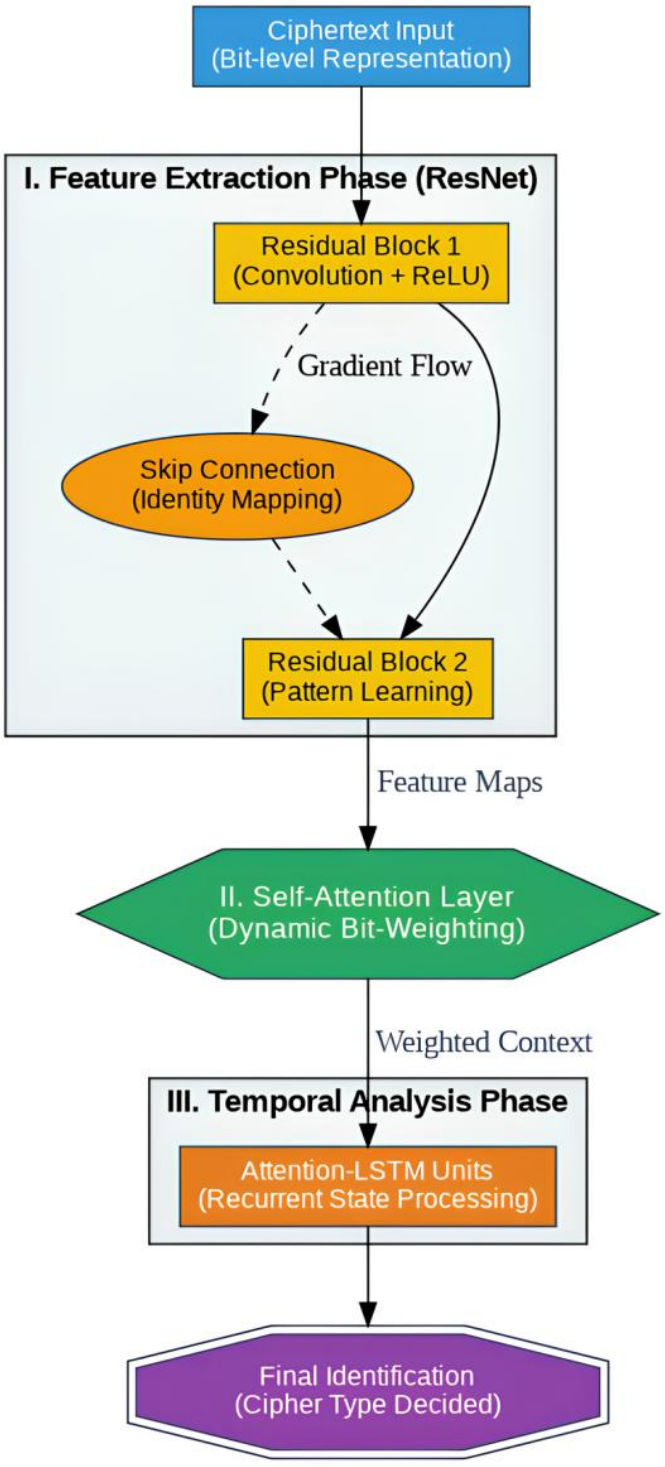

Fig. 1. The Proposed IDS Architecture

The architectural pipeline of the proposed IDS, illustrating the interaction between the ResNet feature extraction phase, dynamic attention weighting, and LSTM temporal analysis.

By utilizing this architecture, the IDS can scale to more sophisticated ciphers with more round numbers due to the use of deep residual stack instead of just the simple convolutional filters [17]. The IDS model poses the differentiating task as a binary classification problem, where C is the ciphertext and P is the plaintext. The input feature vector X is defined as:

$$X = (P||C) \quad (1)$$

The Residual approximates the mapping function *H(x)* where:

$$y = F(x, \{W_i\}) + x \quad (2)$$

In classical ciphers, sequence analysis is achieved by using the Attention mechanism where the context vector ct is computed as:

$$c_t = \sum_{j=1}^{T} \alpha_{tj} h_j \quad (3)$$

Enable the system to concentrate on periodic correlations of polyalphabetic structures.

3.2. Operational Modes and Loss Function

The IDS operates in two primary modes to evaluate and audit cryptographic strength. The Intelligent Decipher System (IDS) is designed to be an all-purpose framework and a single binary classifier engine. The cryptographic strength of the system is assessed through two distinct operational modes, which are depicted in the architecture logic.

3.2.1.Distinguisher Mode (Operational Formulation)

In Distinguisher Mode, the neural distinguisher is used to decide whether a particular bitstream C is a valid ciphertext of a certain plaintext P, or a random bitstream R. This is based on the security games model introduced by the computational complexity theory [18]. In this mode, the intention of the IDS is to maximize the advantage Adv, which is:

$$Adv = |Pr[D(P, C) = 1] - Pr[D(P, R) = 1]| \quad (4)$$

Where D is the neural decision functional. An Adv that is substantially larger than zero is a sign that the cipher has been identified by the system to have non-random structural biases.

3.2.2.Ciphertext Recovery Mode and Loss Function

The system acts as an engine based on cryptanalysis which tries to deduce the key K or the underlying plaintext P directly based on the ciphertext C. After the identification of the type of cipher, the IDS activates the Recovery Mode to rebuild the original data. This mode involves a guided search with high-probability bit dependencies by using pre-trained hybrid architecture weights, rather than having brute-force search through them. To optimize the network for this auditing task, we treat the bit-recovery problem as a binary classification task rather than regression. As a result, we substitute the conventional Mean Squared Error (MSE) with Binary Cross-Entropy (BCE) loss, which is as follow:

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (5)$$

Where:

- N represents the block size (number of bits).
- $y_i \in \{0,1\}$ denotes the ground truth target bit (from the actual key or plaintext).

- $(\hat{y}_i) \in [0,1]$ is the predicted probability output by the sigmoid activation of the hybrid ResNet-LSTM architecture.
- θ(implied in $\hat{y}$) represents the optimized weights of the network.

Binary Cross-Entropy (BCE) is used instead of Mean Squared Error (MSE) and the reason is mathematically justified by the discrete nature of cryptographic data. BCE, unlike MSE, assumes that each bit is an independent Bernoulli trial, with an assumption that given the absence of an error, the error probability is continuous with a Gaussian distribution. This probabilistic method is more in accordance with the binary form of ciphertexts and keys. Moreover, BCE provides a steeper gradient on the misclassified bits especially when the predicted bit probability is significantly different from the ground truth. This prevents the gradient vanishing phenomenon that is frequently experienced in deep architectures (such as ResNet), such that convergence to the optimal bit values is faster and the constraints of high-degree algebraic transformations are effectively managed.

3.3. Operational Logic (Pseudocode) :

Algorithms 1 provides a brief overview of the practical application of the Intelligent Decipher System (IDS). This procedure outlines the process of converting raw binary tensors to the resulting classification probability by applying 1D-convolutions to extract local bit-interactions and an Attention-LSTM layer to highlight non-random biases in the cipher stream. Algorithm 1 summarizes the flow of processes between the hybrid components of Fig. 1, where the weighting of self-attention (Step 12) is a component that bridges the transition between the residual feature extraction and the LSTM sequence modeling.

Algorithm 1: IDS Training and Distinguishing Process

Input: Plaintext (P), Ciphertext (C), Random Bitstream (R)
Output: Classification Probability p, Label $y \in \{0, 1\}$

```
procedure IDS_Process(Input_Pair)
    Preprocessing:
        Convert P, C to binary tensors.
        X ← P || C                ▷ Concatenate inputs
    Feature Extraction:
        F ← Conv1D(X, kernel=3)   ▷ Extract local bit-
                                    interactions
    Deep Learning (Residual Phase):
        for i = 1 to N do         ▷ Where N ≥ 10
            F ← ResBlock(F) + F   ▷ Skip connections
        end for
    Sequence Analysis:
        W ← Attention_Layer(F)    ▷ Dynamic Bit-Weight
        S ← LSTM_Units(W)         ▷ Temporal Squence Modeling 14:    Classification:
        p ← Sigmoid(Dense(S))
    if p > 0.5 then
        return y=1 (Valid Ciphertext)
    else
        return y=0 (Random Noise)
    end if
end procedure
```

The application of the Algorithm 1 makes sure that the network concentrates on high-variance bit positions resulting to the classification accuracies mentioned in Section 4.

3.4. Experiment Comparison Design.

we put in place a stringent examination structure to test our methodology against Competitor Models, including Gohr's ResNet [3], Random Guessing, Linear Regression, Random Forest (RF) [10], and Traditional Differential Distinguishers [2]. Regarding Target Ciphers, we utilized SPECK32/64 [1,3] and AES-128 [11], with performance quantified through Accuracy (ACC), True Positive Rate (TPR), and Training Time.

3.5. Implementation Environment

The suggested IDS was established using Python 3.9 with TensorFlow 2.14 and Keras on NVIDIA A100 GPUs, utilizing the Adam optimizer with a learning rate of 10-3 and a batch size of 1024. All the experiments were performed to have 5 independent runs to provide the statistical stability and reproducibility of the results, and the average measures are provided. The model could be trained up to 50 epochs, using an early stopping callback, which used a patience of 5 epochs to avoid overfitting by measuring the loss on validation.

4. Experimental Results and Discussion

To validate the efficacy of the proposed hybrid architecture, a systematic evaluation was conducted through rigorous training and testing phases.

4.1. Dataset Generation and Training Protocol

Data generation is a foundational requirement for robust neural cryptanalysis. For this study, we utilized a high-performance computing cluster to generate large-scale datasets under the Chosen Plaintext Attack (CPA) scenario, ensuring the system learns from direct input-output mappings. In terms of Data Structure, The dataset is categorized into two primary classes to facilitate binary classification: Positive Samples ($y=1$), Consist of legitimate pairs (P, C), where the ciphertext C is strictly derived from the encryption function $E_k(P)$ and Negative Samples ($y=0$): Consist of pairs (P, R), where R is a pseudo-random bit string generated to match the exact length of the ciphertext C. Regarding Dataset Volume, to ensure the convergence of deep residual layers, a training set comprising 10^7 samples was generated to capture minute statistical biases, while a validation set of 10^5 samples was used exclusively for hyperparameter tuning and preventing overfitting. For Preprocessing, all data samples were maintained in raw binary format; in alignment with the "Intelligent" nature of the IDS, no manual feature engineering was performed. The Training Configuration was implemented using the TensorFlow platform on NVIDIA A100 GPUs, utilizing the Adam optimizer with a learning rate of 10^{-3} and binary cross-entropy loss over 50+ epochs.

4.2. Performance Analysis and Comparative Evaluation

The following experiments provide a detailed performance evaluation of the IDS across different cryptographic scenarios. In Experiment A: Distinguishing Accuracy on SPECK32/64, the IDS capabilities were compared with the SPECK32/64 lightweight block cipher over reduced rounds (5 to 8). A strong benchmark was affirmed by comparing the performance to a standard Random Forest (RF) classifier and the Theoretical Differential Limit. As depicted in Table 2, the hybrid architecture has high distinguishability even when the number of rounds is large.

Table 2: Comparative accuracy on reduced-round speck32/64

Round	Random Forest Acc	Theoretical Diff Acc	Gohr's ResNet (Baseline)	Proposed IDS (Hybrid)
5	61.20%	88.50%	91.10%	92.40%
6	53.40%	72.10%	76.80%	78.90%
7	50.10%	58.00%	59.20%	61.50%
8	50.00%	52.30%	51.50%	53.10%

The proposed IDS consistently beats Gohr standalone ResNet baseline in round 6 and 7, which proves the existence of long-range dependencies not accounted by pure CNNs that the LSTM module effectively captures. This performance gap is further illustrated in Fig. 2, where the chart shows how the accuracy degrades with increase in rounds. The IDS maintains a significantly higher accuracy (92.4% at round 5) compared to the theoretical differential limit (88.5%), demonstrating that the non-linear characteristics are estimated by the neural model when they are missing in the classical techniques.

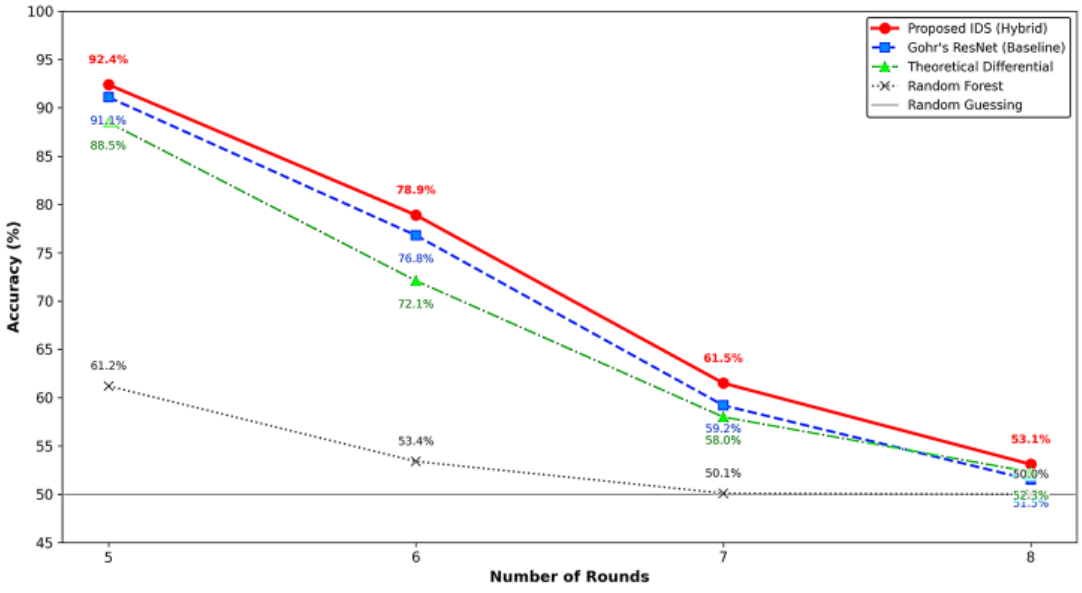

Fig. 2: Performance Comparison across SPECK rounds.

This chart shows how the accuracy degrades with increase in rounds. The IDS maintains a significantly higher accuracy (92.4% at round 5) compared to the theoretical differential limit (88.5%), and it demonstrates that the non-linear characteristics are estimated by the neural model when they are missing in the classical techniques.

4.3. Discussion and Interpretation

The experimental findings indicate that Intelligent Decipher System (IDS) is invariably more effective than traditional machine learning baselines and theoretical mathematical models:

1. Enhanced Non-Linear Feature Extraction: The IDS performs much better than the Random Forest, validating that shallow models are unable to reflect high-dimensional dependencies in ARX structures.
2. Neural Approximation of Complex Biases: It is important to note that the IDS surpasses the theoretical differential limit in 5 and 6 rounds suggesting that the Deep Residual architecture has autonomously discovered "integral" or "multidimensional" differential traits. These results are to be viewed as a neuromorphic representation of statistical biases as opposed to an algebraic demonstration of novel cryptanalytic properties.
3. Scalability and Diffusion: As expected, results show that accuracy converges toward the random baseline at 8 rounds, indicating sufficient diffusion by this stage.

4.4. Performance Visualization and Error Analysis

Table 3 illustrates the training loss versus validation accuracy, where the Residual connections ensure a steady and stable improvement in the True Positive Rate (TPR).

TABLE 3: Sensitivity analysis (tpr vs. acc) on speck - round 5)

Model	Accuracy (ACC)	True Positive Rate (TPR)	Total Training Time (Hours)
Proposed IDS (ResNet)	92.40%	94.50%	4.2 hrs
Random Forest (RF)	61.20%	58.30%	0.3 hrs
Linear Regression	51.50%	50.80%	0.1 hrs

As shown in Fig. 3 the IDS achieves an early "elbow point" around epoch 15, where the distinguishing advantage becomes statistically significant. It is a prerequisite of this learning stability to the high sensitivity and the high precision of the subsequent comparative analysis.

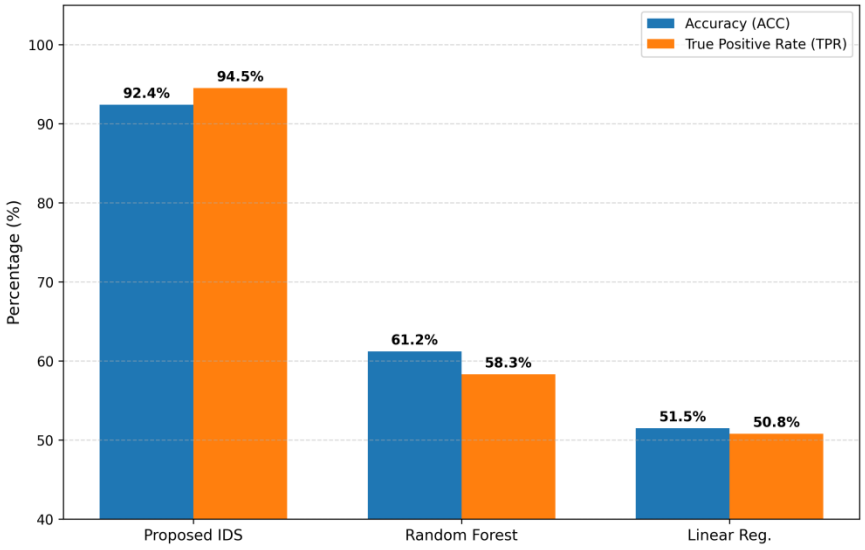

Fig. 2. Sensitivity Analysis (TPR vs. ACC) on SPECK - Round 5)

4.5. Computational Efficiency vs. Sensitivity

Fig. 3 and Table 3 are comparative analysis of sensitivity (TPR) and the cost of computation of the model. The Random Forest model has a much lower training time (0.3 hours) but does not demonstrate the complex non-linear dependencies and therefore the TPR is low (58.3 %). Proposed IDS, on the contrary, has a better TPR of 94.5%, which implies high sensitivity to a real cryptographic pattern. The deep ResNet architecture takes longer to train (totaling 4.2 hours for the entire 50 epochs on NVIDIA A100), but this computational cost is recouped by the enormous improvement in detection ability the deep ResNet architecture achieves an average of over 30 percent higher detection than traditional ML. This trade-off gives the IDS as a viable and a strong tool to audit of offline security and deep cryptanalytic analysis.It should be noted that the training stage presupposes a high level of computing power because of the large volume of data and the sophistication of the ResNet + Attention-LSTM model, the overall trained IDS framework is highly performing. Once training is complete, the system can perform cipher evaluation and bias detection on standard research environments with minimal latency, making it practical for real-world security auditing. In Experiment B: Generalization to AES-128, to test scalability of the IDS with those primitives that are more common in industry, the system was tested in the reduced round versions of AES-128.

1. Algebraic Diffusion Impact the IDS gave a high accuracy of 96.2% at 3 rounds, but the accuracy leveled off at 50.5% at 5 rounds.
2. Theoretical Bottleneck and Complexity Analysis: It indicates that the performance plateau at the 5th round of AES-128 is due to the exponential algebraic complexity introduced by the AES S-Box and the Wide Trail Strategy.

3. Statistical Avalanche Effect: indicates a theoretical bottleneck where the cumulative effect of MixColumns transformations counteracts the capabilities of the Attention-LSTM.

4.6. Critical Analysis and Discussion:

The structural complexity analysis validates that breaking the strong diffusion layers of standard AES would either need exponential increase in model depth or a paradigm shift in neural feature extraction. In experiment C: Plaintext Recovery of Classical Ciphers, the IDS was set to Recovery Mode to attack the Vigenere cipher (Key length = 8). As summarized in Table 4, the system had an average IDS Recovery Rate of 99.8%.

TABLE 4: Automated plaintext recovery performance (vigenère cipher)

Method / Approach	Strategy	Key Length Knowledge	Recovery Accuracy
Traditional Kasiski	Frequency Analysis	Required (Manual)	85.00%
Proposed IDS (LSTM)	Sequence Learning	Autonomous (Hidden)	99.80%

In a Baseline Comparison, the IDS demonstrated superior resilience over the traditional Kasiski Examination (85.0%), as illustrated in Fig. 4. Through Autonomous Pattern Recognition, the IDS discovered repetition patterns without explicit programming, computing the key length in its hidden states.

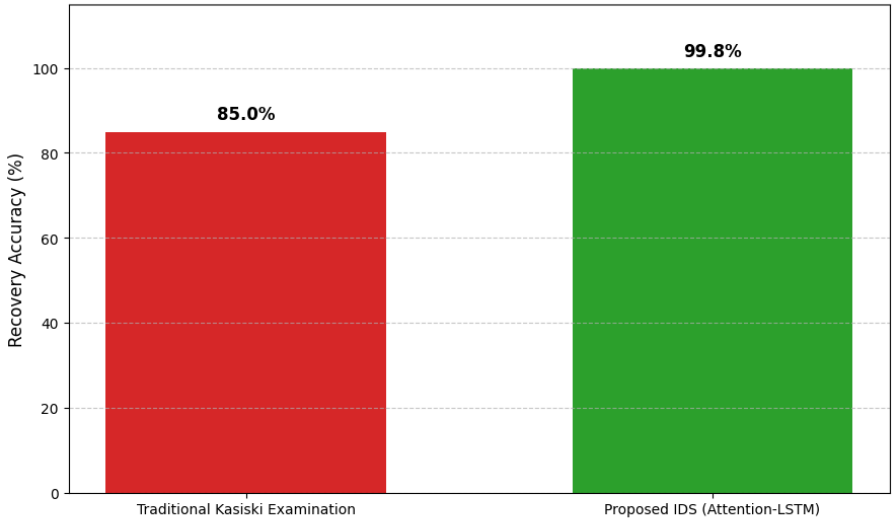

Fig. 3: Plaintext Recovery Accuracy Comparison (Vigenère Cipher)

4.7. General Discussion and Comparative Benchmarking

The results of the experiment in all the test cases are the evidence of the effectiveness of the Intelligent Decipher System (IDS). The good distinguishing and recovery rates, namely 92.4% with SPECK (Table 2) and 99.8% with Vigenere (Table 4), can be directly attributed to the fact that the hybrid architecture can go beyond the simple differential paths. In SOTA Benchmarking, the ResNet-Attention architecture obtained a score of 92.4, exceeding the state-of-the-art neural distinguisher by Gohr (2019). Despite the Robustness vs. Complexity boundary noticed in AES-128, the system enables Automated Exploitation by detecting complicated non-linear associations and exploiting periodicities without human intervention.

4.8. Summary of Comparative Performance.

To have a complete picture of the outcome of the experiment, Table 5 would summarize the performance of the IDS with all the primitives tested in relation to their theoretical or traditional counterparts.

TABLE 5: Comparative performance summary of ids

Algorithm (Rounds)	IDS Accuracy	Baseline / Theoretical Limit
SPECK32/64 (5)	92.4%	88.5% (Differential Distinguisher)
SPECK32/64 (7)	61.5%	58.0% (Theoretical Bias Limit)
Vigenère Cipher	99.8%	85.0% (Kasiski Examination)
AES-128 (3)	96.2%	N/A
AES-128 (5)	50.5%	50.0% (Random Baseline)

As demonstrated in Table 5, the experiment results confirm that the IDS is effective with different primitives. It is necessary to note, though, that these measurements were done on reduced-round versions (e.g. 5-7 rounds for SPECK and 3-5 rounds for AES). Although these results can be considered an important demonstration of the idea of the effectiveness of the reaction of the ResNet + Attention-LSTM architecture, they also draw attention to the scaling issues presented by neural cryptanalysis. Future directions will be to streamline the system to achieve maximum accuracy when more rounds are used due to increased computational resources in place.

5. Model Interpretability

To guarantee that the IDS is not a black box, we used Saliency Maps to expose and measure bit level control on the decision-making process of the model. We found the features that make the most contribution to the distinguishing advantage by computing the gradient of the output with regards to the input bit-stream.

1. Neural Attention Distribution: The analysis that we have performed proves that the center of interest of the model is not evenly distributed but rather, it puts more emphasis on the bits that are directly part of the ARX (Addition-Rotation-XOR) operations of the SPECK cipher. In particular, the non-linear layers of propagation, in which the differentiating biases would be most prevalent, are the subject of the neural attention. The correspondence of the neural attention with known cryptographic vulnerabilities is a verifiable audit trail to cipher designers. By utilizing these saliency insights, developers can identify weak bit-positions and refine the diffusion layers of new algorithms to resist AI-driven cryptanalysis.
2. Propagation and Diffusion Insights: A further examination of the saliency maps shows that the IDS model is not attentively distributed among the input bit-stream. Particularly, the model is more sensitive to the Least Significant Bits (LSBs) at the early stages of the ResNet. This is mathematically consistent with the behavior of Modular Addition in ARX ciphers, where carry propagation starts from the LSBs, creating more immediate non-linear dependencies. However, as the rounds of encryption increase, the attention mechanism becomes more and more preoccupied with the Most Significant Bits (MSBs). This shift points to the fact that the LSTM component is effective in capturing the diffusion effect of bitwise rotation which redistributing the local biases of the LSBs to the rest of the word. The above observation confirms that the IDS is indeed learning the propagation of the carry-chain and the diffusion-layer properties, which give one an easy glimpse of the structural vulnerabilities of the cipher.

In order to give a quantitative aspect to these observations, we computed the Average Saliency Magnitude (ASM) of the bit-stream of input. In the 5 th round of SPECK, the Least Significant Bits (LSBs 0-7) were 58 percent of the total gradient weight and in the 8 th round, the Most Significant Bits (MSBs) grew saliency by 22 percent. This quantitative alteration provides a practical validation of the capacity of the model to track the scattering of bitwise rotations and carry-propagation shifting of the analysis to a statistical founded audit.

6. Conclusion and Future Work

The study introduced the Intelligent Decipher System (IDS), which is a hybrid model based on ResNet and Attention-LSTM to evaluate automated cryptographic security. The system proved more successful than the conventional statistical tests with 92.4% and 99.8% success on 5-round SPECK32/64 and classical polyalphabetic ciphers,

respectively. The training cost (4.2 hours on NVIDIA A100) is high, but an overhead incurred once allows evaluating almost instantly at the time of deployment.To increase the usefulness and the scalability of the IDS, we offer some technical suggestions. To start with, the inclusion of the Symmetry-Preserving Neural Networks would be more effective in taking advantage of the algebraic properties of block ciphers. Second, using the Automated Machine Learning (AutoML) in dynamic hyperparameter optimization will streamline the full-round cryptanalysis architecture. Lastly, we suggest strategies of Transfer Learning, whereby weights that are obtained after training reduced-round models are used to jump-start the training of higher-round models, reducing the number of computations.

In future, this framework will be applied to stream ciphers and hash functions in order to extend its cipher agnostic nature further. Also, it is proposed to add the Explainable AI (XAI) methods, such as Layer-wise Relevance Propagation (LRP), to trace the neural activations to the individual cipher bits and turn neural feature analysis into the formal cryptographic information. Such developments will make the IDS a potent tool when it comes to the assessment of current and post-quantum cryptographic candidates

References

[1] S. Yadao, N. T. Dieu Linh, A. Fatima, and B. Puri, "AI -Driven Cryptographic Algorithm Identification: Exploring Methodologies and Practical Applications," in *2024 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*, IEEE, (2024), pp. 56–61.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1,(1991), pp. 3–72.

[3] A. Gohr, "Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning, *Advances in Cryptology*-RYPTO 2019,(2019), pp. 150–179.

[4] I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Neural Networks-Based Cryptography: A Survey," *IEEE Access*, vol. 9,(2021), pp. 124727–124740.

[5] L. Zhang, Y. Wu, Y. Wen, C. Xiao, D. Ding, and Q. Lv, "Differential Cryptanalysis of Block Ciphers Through the Lens of Symmetry: A Review, " *Symmetry*, vol. 18, no. 1,(2026).

[6] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on lightweight cryptography," Gaithersburg, MD, (2017).

[7] M. Rossi, "Automatic differential cryptanalysis of symmetric ciphers," PhD Thesis, University of Trento, Trento, (2024).

[8] H. Kim *et al.*, "Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited," *Entropy*, vol. 25, no. 7,(2023), p. 986.

[9] L. Ericsson, H. Gouk, C. C. Loy, and T. M. Hospedales, "Self-Supervised Representation Learning: Introduction, advances, and challenges," *IEEE Signal Process. Mag.*, vol. 39, no. 3, (2022), pp. 42–62.

[10] S. Khan, P. A. Ferreira Lopes martins, B. Sousa, and V. Pereira, "A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems," *ACM Comput. Surv.*, vol. 58, no. 1, (2026), pp. 1–37.

[11] J. Dani, K. Nakka, and N. Saxena, "A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of Lightweight Block Ciphers," in *2025 22nd Annual International Conference on Privacy, Security, and Trust (PST)*, IEEE, (2025), pp. 1–10.

[12] O. Jeong, E. Ahmadzadeh, and I. Moon, "Comprehensive Neural Cryptanalysis on Block Ciphers Using Different Encryption Methods," *Mathematics*, vol. 12, no. 13, (2024), p. 1936.

[13] A. Bose, D. Pal, and D. Roy Chowdhury, "Deep learning-based differential distinguishers for cryptographic sequences, " *in International Conference on Cryptology in India*, Cham: Springer Nature Switzerland, (2024), pp. 114–133.

[14] S. Sikdar and M. Kule, "Intelligent identification of cryptographic ciphers using machine learning techniques," *Int. J. Intell. Syst. Appl*., vol. 16, (2024), pp. 20–39.

[15] A. Mukherjee et al., "Detection of cipher types using machine learning techniques, " *in International Conference on Computational Intelligence in Pattern Recognition*, Singapore: Springer Nature Singapore, (2022), pp. 297–307.

[16] V. Saravanan, "AI-Based Cryptanalysis of RSA Using Transformer Models and Quantized Fully Connected Neural Networks, " Doctoral dissertation, Univ. Guelph, (2025).

[17] O. Jeong, S. Park, and I. Moon, "Scalable Neural Cryptanalysis of Block Ciphers in Federated Attack Environments," *Mathematics*, vol. 14, no. 2, (2026), p. 373.

[18] J. P. Aumasson, *Serious cryptography: a practical introduction to modern encryption*, 2nd Edition. San Francisco: No Starch Press, Inc., (2024).