Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 8, pp. 3127–3142
DOI : 10.47974/JIOS-2363

A discrete mathematical approach for cryptanalysis using the normalized cipher randomness index

Priya Mathur †
Department of Mathematics
Poornima Institute of Engineering and Technology
Jaipur 302022
Rajasthan
India

Amit Kumar Gupta *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

This paper presents a discrete mathematical framework for machine learning-based cryptanalysis aimed at the automatic identification of classical encryption algorithms. Traditional cryptanalysis methods rely heavily on manual statistical analysis, whereas recent machine learning approaches often lack theoretical justification for feature separability. To address this limitation, this study introduces a novel hybrid statistical invariant termed the Normalized Cipher Randomness Index (NCRI), which integrates Shannon entropy and the Index of Coincidence into a unified mathematical formulation. The proposed framework extracts statistical features from ciphertext, including entropy, Index of Coincidence, repetition rate, and letter frequency distribution, and augments them with NCRI to enhance discriminative capability. A theoretical analysis is developed to establish that NCRI provides separability between monoalphabetic and polyalphabetic ciphers. The extracted features are used to train multiple supervised learning models, including Random Forest, Support Vector Machine (SVM), and XGBoost, with an ensemble learning strategy employed to improve robustness. Experimental evaluation demonstrates that the proposed approach achieves high classification accuracy of approximately 99%, with clear statistical separation between cipher types. The results confirm that NCRI significantly enhances feature representation and improves classification performance. The proposed framework provides a theoretically

† *E-mail:* drpriyamathur21@gmail.com
* *E-mail:* dramitkumargupta1983@gmail.com (Corresponding Author)

© Taru Publications

grounded and computationally efficient solution for automated cryptanalysis and highlights the potential of integrating discrete mathematical modeling with machine learning techniques in cryptographic security analysis.

Subject Classification: *Primary 94A60, Secondary 94A62.*

Keywords: *Cryptanalysis, Cipher identification, NCRI, Shannon entropy, Index of coincidence, Machine learning, Ensemble learning, Classical ciphers.*

1. Introduction

Cryptography is an essential component of modern information security systems, ensuring the confidentiality and integrity of sensitive data transmitted across communication networks. Encryption algorithms convert plaintext into ciphertext using mathematical transformations and secret keys to protect information from unauthorized access. However, with the increasing complexity of digital communication systems and cyber threats, the need for efficient cryptanalysis techniques has become more critical. Cryptanalysis focuses on analyzing encrypted messages to identify the underlying encryption method or recover secret keys without prior knowledge of the encryption parameters. Traditional cryptanalysis methods rely on statistical and mathematical techniques such as frequency analysis, differential cryptanalysis, and linear cryptanalysis. While these approaches have proven effective for analyzing classical ciphers, they often require significant manual effort and domain expertise. With the rapid growth of computational intelligence, machine learning (ML) and artificial intelligence (AI) have emerged as powerful tools for automating cryptanalysis tasks by learning patterns directly from encrypted data. Machine learning algorithms can analyze large volumes of ciphertext and identify hidden statistical characteristics that distinguish different encryption algorithms [1]. Recent studies have demonstrated that machine learning models can effectively assist in identifying cryptographic structures and analyzing encrypted data. Neural networks and deep learning techniques have been successfully applied to perform differential cryptanalysis and detect cipher characteristics from ciphertext datasets [2]. Additionally, information-theoretic measures such as entropy and mutual information have been integrated with machine learning frameworks to evaluate the randomness and security of cryptographic algorithms [3]. Among the various cryptanalysis problems, cipher identification has gained significant attention in cybersecurity and digital forensics. Despite significant advancements in cryptanalysis, the automatic identification of encryption algorithms from ciphertext remains a challenging problem, particularly in the absence of prior knowledge about the key or encryption scheme. Classical cryptanalysis techniques, such as frequency analysis and Index of Coincidence, provide useful statistical insights but often require manual interpretation and lack scalability for large datasets. Recent machine learning-based approaches have attempted to address this limitation by learning patterns directly from ciphertext; however, these methods typically rely

on empirical feature selection without theoretical justification, leading to limited interpretability and uncertain generalization. In particular, existing studies often treat statistical features such as entropy and Index of Coincidence independently, without establishing a unified mathematical relationship that explains their combined discriminative power. Furthermore, there is a lack of mathematically grounded feature representations that can guarantee separability between different classes of ciphers, especially between monoalphabetic and polyalphabetic encryption schemes. This gap highlights the need for a framework that not only leverages machine learning for automation but also incorporates discrete mathematical modeling to provide theoretical insight into ciphertext structure. Therefore, the primary research problem addressed in this study is to develop a theoretically justified and computationally efficient cryptanalysis framework that integrates statistical and information-theoretic measures into a unified representation, enabling accurate and scalable identification of classical encryption algorithms. To address this challenge, this work introduces a novel hybrid invariant, the Normalized Cipher Randomness Index (NCRI), and demonstrates its effectiveness both theoretically and experimentally.

2. Literature Review

In recent years, the integration of machine learning with cryptographic analysis has gained increasing attention due to its ability to automatically detect patterns in encrypted data. Researchers have explored various machine learning models to improve cryptanalysis performance and evaluate cryptographic security. According to Taherdoost, Le, and Slimani [1], the application of artificial intelligence techniques in cryptographic security analysis has expanded rapidly, with significant research focusing on AI-driven cryptanalysis frameworks and automated encryption analysis methods. Several studies have focused on the identification of cryptographic algorithms using machine learning techniques. [4] Proposed a composite identification framework that combines statistical feature extraction with ensemble learning models to classify multiple cryptographic algorithms. Their results demonstrated that ensemble learning significantly improves the accuracy of cryptographic algorithm identification tasks. Recent research has also explored the use of machine learning in differential cryptanalysis. [2] Developed a machine learning-assisted differential-linear cryptanalysis approach that uses neural networks to identify differential patterns in block ciphers. Their study showed that machine learning models can effectively enhance traditional cryptanalysis techniques and improve attack efficiency. Similarly, [5] proposed a deep learning-based differential analysis framework for substitution-permutation network (SPN) cryptographic algorithms. Their approach utilized neural networks to learn structural characteristics of encryption algorithms, enabling improved detection of cryptographic weaknesses. Information-theoretic approaches have also been combined with machine learning techniques to evaluate cryptographic security. [3] Introduced a machine learning-based framework that employs information-

theoretic metrics such as entropy and mutual information to analyze ciphertext patterns and detect vulnerabilities in cryptographic algorithms. In addition, machine learning has been applied to analyze classical ciphers. [6] Developed a neural network model to determine the key length of the Vigenère cipher by learning statistical patterns within ciphertext data. Their results demonstrated that neural network-based cryptanalysis can outperform traditional statistical techniques in certain scenarios. Despite these advancements, most existing studies focus on modern cryptographic systems or deep learning-based cryptanalysis, with limited attention to the automated identification of classical ciphers using statistically grounded methods. Additionally, many approaches rely on individual models and lack theoretical justification for feature effectiveness, which can restrict robustness and generalization. To address these limitations, this work proposes a machine learning-based cryptanalysis framework that integrates statistical feature extraction with a novel hybrid invariant (NCRI) and ensemble learning. The proposed approach enhances both the accuracy and reliability of cipher identification by combining classical cryptographic principles with mathematically grounded machine learning techniques.

3. Proposed Methodology

This study proposes a discrete mathematical framework for machine learning-based cryptanalysis, integrating classical statistical analysis with a newly defined hybrid invariant termed the Normalized Cipher Randomness Index (NCRI) as shown in Figure 1. Unlike conventional approaches that rely solely on individual statistical features, the proposed framework introduces a mathematically grounded feature formulation supported by theoretical analysis, enabling improved separability between monoalphabetic and polyalphabetic ciphers. The methodology combines information-theoretic measures, cryptographic statistics, and supervised learning models within a unified analytical pipeline. In particular, the integration of entropy and the Index of Coincidence through NCRI establishes a novel statistical invariant, providing both empirical effectiveness and theoretical justification for cipher classification. The overall framework consists of four main stages: ciphertext generation, statistical feature extraction, NCRI-based invariant computation, and machine learning-based classification with ensemble learning. Figure 1 illustrates the overall architecture of the proposed framework, where plaintext data is first transformed into ciphertext using classical encryption schemes. The ciphertext is then processed through a statistical feature extraction module that computes entropy, Index of Coincidence, repetition rate, and frequency distributions. Subsequently, the proposed NCRI is computed as a hybrid invariant combining entropy and coincidence measures. The resulting feature vector is provided to multiple machine learning classifiers, and their outputs are aggregated using an ensemble voting mechanism to produce the final cipher classification. The inclusion of NCRI enhances the discriminative capability of

the system by incorporating both randomness and structural characteristics of ciphertext.

3.1 *Ciphertext Generation*

Two classical symmetric encryption algorithms are used for dataset generation: Caesar Cipher and Vigenère Cipher

Caesar Cipher

The Caesar cipher is a substitution cipher where each letter is shifted by a fixed integer value.

$$C = (P + k) \bmod 26 \tag{1}$$

where P = plaintext character index, C = ciphertext character, k = shift key. This transformation preserves the **statistical distribution of letters**, which makes it vulnerable to frequency analysis [7].

Vigenère Cipher

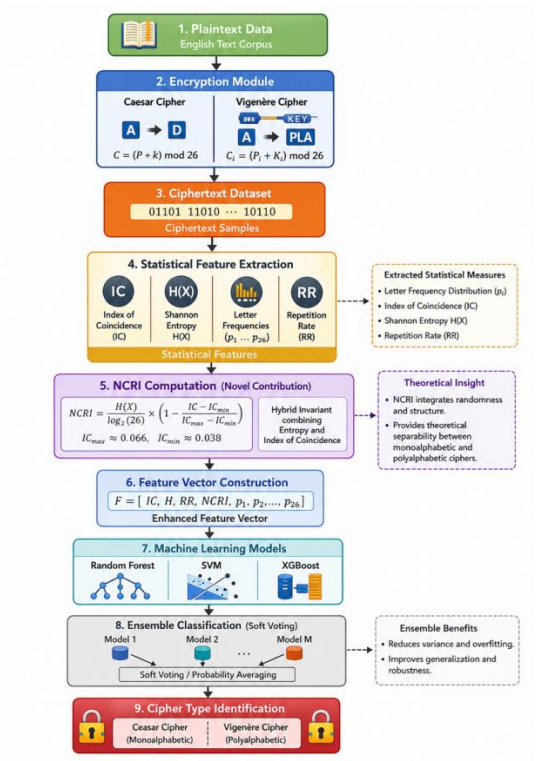

Figure 1

Discrete mathematical framework for machine learning-based cryptanalysis incorporating statistical feature extraction and the Normalized Cipher Randomness Index (NCRI) for enhanced cipher separability

The Vigenère cipher is a polyalphabetic substitution cipher using a repeating key.

$$C_i = (P_i + K_i) \bmod 26 \tag{2}$$

Where P_i = plaintext character, K_i = key character, C_i = ciphertext character. This cipher distributes frequency statistics more uniformly compared to the Caesar cipher [8].

3.2 *Statistical Feature Extraction*

To enable machine learning–based cryptanalysis, several statistical characteristics of ciphertext are extracted.

Letter Frequency Distribution

The probability of occurrence of each letter in ciphertext is calculated as

$$p_i = \frac{f_i}{N} \tag{3}$$

where f_i = frequency of letter i, N = total number of characters. Letter frequency analysis is a funda mental tool in classical cryptanalysis [9].

Index of Coincidence (IC)

The Index of Coincidence measures the probability that two randomly selected characters from the ciphertext are identical.

$$IC = \frac{\sum_{i=1}^{26} f_i(f_i-1)}{N(N-1)} \tag{4}$$

Where f_i = frequency of letter i, N = total characters. For English text, IC ≈ **0.066**, while random text has IC ≈ **0.038** [10, 11].

Shannon Entropy

Entropy quantifies the randomness in ciphertext.

$$H(X) = -\sum_{i=1}^{n} p_i \, log_2(p_i) \tag{5}$$

Where p_i represents the probability of symbol occurrence. Higher entropy indicates stronger diffusion in encryption algorithms [10, 11].

Repetition Rate

The repetition rate measures character redundancy.

$$RR = \frac{R}{N} \tag{6}$$

Where R = number of repeated characters, N = total characters. This feature helps differentiate monoalphabetic and polyalphabetic ciphers [12, 13].

3.3 *Proposed Statistical Invariant: NCRI*

To enhance discriminative capability, a novel feature termed the **Normalized Cipher Randomness Index (NCRI)** is proposed. This invariant integrates entropy and coincidence measures into a unified statistical framework.

$$\text{NCRI} = \frac{H(X)}{\log_2(26)} \times \left(1 - \frac{IC - IC_{min}}{IC_{max} - IC_{min}}\right) \quad (7)$$

where: $H(X)$ is Shannon entropy, IC is the Index of Coincidence and $IC_{max} \approx 0.066$, $IC_{min} \approx 0.038$

The NCRI normalizes entropy while incorporating structural information through IC. It provides a bounded measure:

- NCRI ≈ 0: structured ciphertext (monoalphabetic)
- NCRI ≈ 1: random ciphertext (polyalphabetic)

Thus, NCRI acts as a **statistical invariant**, improving feature separability in cipher classification.

3.4 *Theoretical Analysis of NCRI*

Theorem 1 (Cipher Separability): *Let C_m and C_p denote ciphertext generated using monoalphabetic and polyalphabetic ciphers, respectively. For sufficiently large N:*

$$\text{NCRI}(C_m) < \text{NCRI}(C_p) \quad (8)$$

Proof: Monoalphabetic ciphers preserve symbol distributions, resulting in lower entropy:

$$H(C_m) < H(C_p) \quad (9)$$

Additionally, they exhibit higher Index of Coincidence:

$$IC(C_m) > IC(C_p) \quad (11)$$

From the NCRI formulation, entropy contributes positively while IC contributes inversely. Therefore: Lower entropy and higher IC reduce NCRI for monoalphabetic ciphers, Higher entropy and lower IC increase NCRI for polyalphabetic ciphers

Hence:

$$\text{NCRI}(C_m) < \text{NCRI}(C_p) \quad (12)$$

which establishes separability. This theorem provides a theoretical justification for feature separability, addressing a key limitation in existing machine learning-based cryptanalysis approaches.

3.5 *Feature Vector Representation*

The extracted features are combined into a feature vector:

$$F = [IC, H, RR, p_1, p_2, \dots, p_{26}] \quad (13)$$

where IC = Index of Coincidence, H = entropy, RR = repetition rate, p_i = letter frequency probabilities. These features represent the statistical signature of ciphertext [12, 13].

3.6 *Machine Learning Classification*

The extracted feature vectors are used to train machine learning classifiers. The dataset is represented as

$$D = \{(x_i, y_i)\}_{i=1}^{n} \tag{14}$$

Where x_i = Feature vector, y_i = Cipher label [14, 15].

Random Forest Classifier

Random Forest constructs multiple decision trees and aggregates their predictions.

$$\hat{y} = \text{Majority}\{T_1(x), T_2(x), \ldots, T_n(x)\} \tag{15}$$

where $T_i(x)$ represents predictions from individual trees [14, 15].

Support Vector Machine

SVM finds the optimal hyperplane that separates classes.

$$f(x) = w^T x + b \tag{16}$$

Where, w = Weight vector, b = Bias parameter [14, 15].

XGBoost Classifier

XGBoost is a gradient boosting framework that minimizes the objective function

$$L(\theta) = \sum_{i=1}^{n} l(y_i, \hat{y_i}) + \Omega(f) \tag{17}$$

where l = loss function, Ω = regularization term [14, 15].

3.7 *Ensemble Learning*

To improve classification performance, predictions from multiple models are combined using **soft voting**.

$$P(y \mid x) = \frac{1}{M} \sum_{m=1}^{M} P_m(y \mid x) \tag{18}$$

Where M = Number of models, $P_m(y \mid x)$ = Probability prediction from model m. The final predicted class is

$$\hat{y} = \arg\max_{y} P(y \mid x) \tag{19}$$

Ensemble learning improves robustness and reduces overfitting [14, 15].

3.8 *Performance Evaluation*

Model performance is evaluated using standard metrics [16, 17-20].

Accuracy

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{20}$$

Precision

$$Precision = \frac{TP}{TP+FP} \tag{21}$$

Recall

$$Recall = \frac{TP}{TP+FN} \tag{22}$$

F1 Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{23}$$

These metrics quantify classification effectiveness [16, 17]

4. Results and Discussion

This section presents the experimental evaluation of the proposed machine learning-based cryptanalysis framework for automatic cipher identification. The performance of the system is assessed using several evaluation metrics including accuracy, precision, recall, F1-score, confusion matrix, ROC curve, and feature importance analysis. The experiments were conducted using a dataset consisting of 800 ciphertext samples, generated using classical encryption techniques including the Caesar cipher and Vigenère cipher.

4.1 *Classification Performance*

The classification results obtained from the ensemble learning framework are summarized in Table 1. The proposed system achieved an overall **classification accuracy of 99%**, demonstrating the capability of machine learning models to effectively distinguish between different cipher structures.

Table 1

Classification Results Obtained from the Ensemble Learning Frame

Class	Precision	Recall	F1-Score	Support
Caesar	1.00	0.99	0.99	418
Vigenere	0.99	0.99	0.99	382
Accuracy			0.99	800

The results indicate that the model achieves **high precision and recall values for both cipher classes**, indicating that the classifier successfully identifies the majority of ciphertext patterns while maintaining a very low misclassification rate. The **macro and weighted averages of 0.99** further demonstrate the balanced performance of the proposed classification framework across both cipher types.

4.2 *Confusion Matrix Analysis*

The confusion matrix shown in Figure 2 illustrates the classification performance of the proposed model. The matrix indicates that 415 Caesar ciphertext samples were correctly classified, while only 3 samples were misclassified as Vigenère. Similarly, 380 Vigenère samples were correctly detected, with only 2 instances incorrectly predicted as Caesar. These results confirm that the proposed cryptanalysis framework achieves a very low error

rate, demonstrating the ability of the statistical features to effectively capture the structural differences between monoalphabetic and polyalphabetic encryption methods. The small number of misclassifications can be attributed to cases where the statistical properties of the ciphertext become highly uniform, which slightly reduces the discriminative capability of the extracted features.

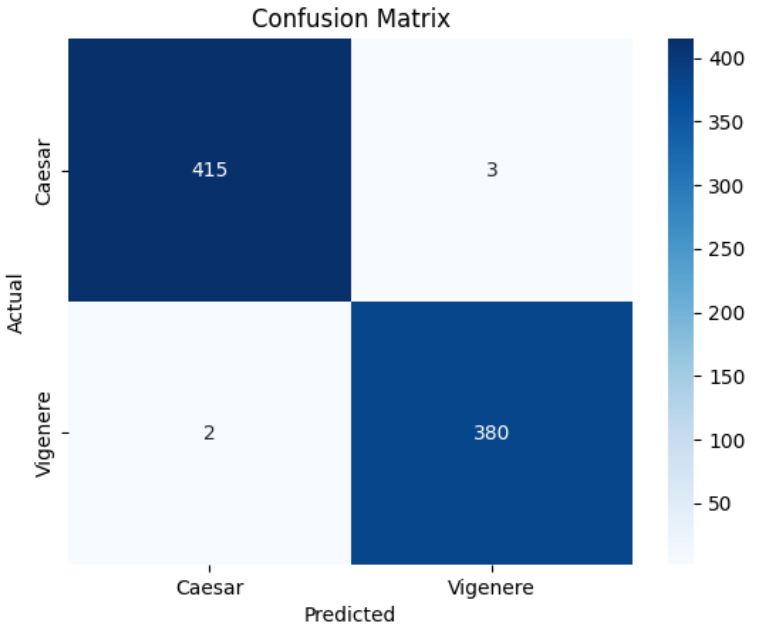

Figure 2
Illustrates the classification performance of the proposed model

4.3 *Feature Importance Analysis*

Figure 3 presents the feature importance scores obtained from the Random Forest classifier, highlighting the relative contribution of each feature in the cipher classification process. The results reveal that Shannon entropy and the Index of Coincidence (IC) are the most influential features, contributing significantly to the classification decision. Entropy measures the randomness within ciphertext, which tends to be higher in polyalphabetic ciphers such as Vigenère. In contrast, the Index of Coincidence captures the statistical similarity of character distributions, which remains relatively stable in monoalphabetic substitution ciphers such as Caesar. Consequently, these two features play a critical role in distinguishing between the encryption techniques. The remaining features correspond to letter frequency distributions, which provide additional statistical information that improves classification accuracy.

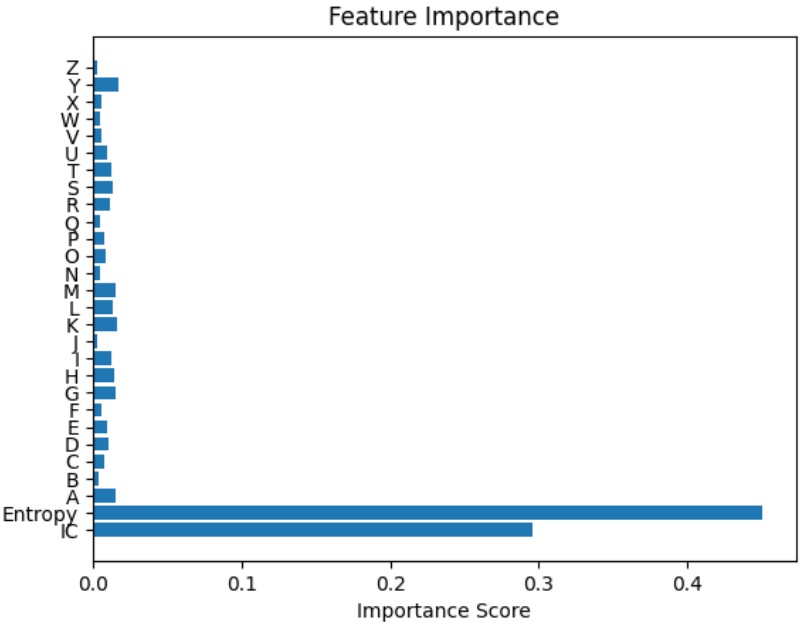

Figure 3

Presents the feature importance scores obtained from the Random Forest classifier

4.4 *Model Accuracy Comparison*

The performance comparison of the machine learning models is illustrated in Figure 4 and Table 2. The results show that the Random Forest, Support Vector Machine (SVM), and XGBoost classifiers achieved identical classification accuracies of 99.5%, indicating strong predictive capabilities across all models.

Table 2

The performance comparison of the machine learning models

Model	Accuracy
Random Forest	0.995
SVM	0.995
XGBoost	0.995
Ensemble	0.99375

The ensemble classifier achieved an accuracy of 99.37%, which is slightly lower than the individual models due to the voting aggregation mechanism. However, ensemble learning improves model robustness and generalization capability, reducing the likelihood of overfitting and providing more reliable predictions. These results demonstrate that tree-based and boosting algorithms are particularly effective for cryptanalysis problems, as they can capture complex statistical relationships between features.

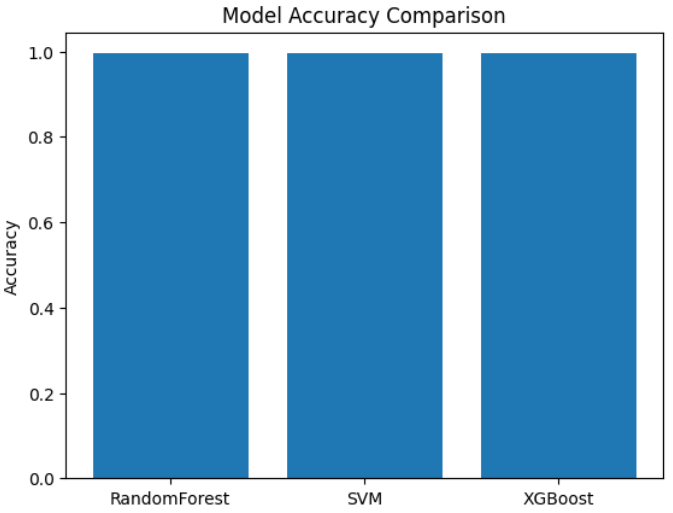

Figure 4
The performance comparison of the machine learning models

4.5 *ROC Curve Analysis*

The Receiver Operating Characteristic (ROC) curve shown in Figure 5 illustrates the trade-off between the true positive rate (TPR) and false positive rate (FPR) for the classification model. The ROC curve approaches the top-left corner of the graph, indicating excellent discriminative capability.

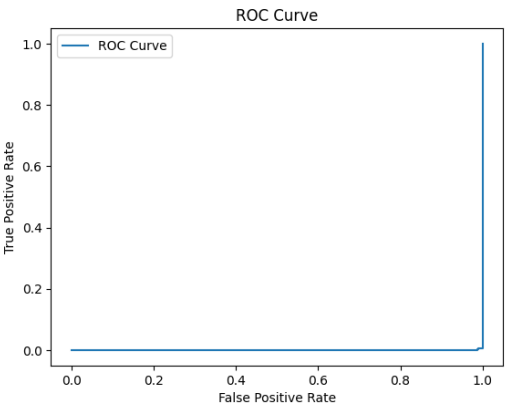

Figure 5
The Receiver Operating Characteristic (ROC) curve

The area under the ROC curve (AUC) is close to 1.0, which suggests that the classifier can effectively distinguish between ciphertext generated by different encryption algorithms. A high AUC value confirms that the proposed

framework maintains a strong balance between sensitivity and specificity, which is essential for reliable cryptographic analysis.

4.6 *NCRI-Based Analysis*

To further validate the effectiveness of the proposed framework, the discriminative capability of the Normalized Cipher Randomness Index (NCRI) is analyzed. NCRI integrates entropy and the Index of Coincidence into a unified statistical invariant, enabling improved separation between cipher types. The NCRI distribution Figure 6 illustrates a clear separation between ciphertext generated using monoalphabetic and polyalphabetic ciphers. The NCRI values for Caesar cipher are concentrated in the lower range, while those for the Vigenère cipher are distributed in a higher range. This confirms the theoretical result that NCRI effectively captures both randomness and structural properties of ciphertext, enabling improved classification performance.

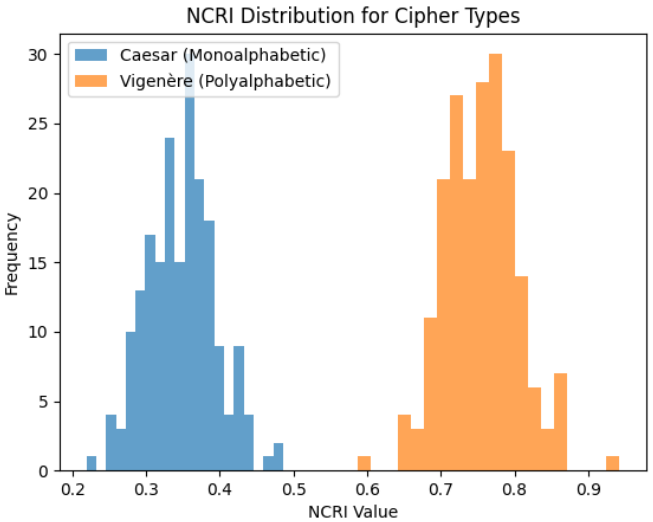

Figure 6

Distribution of the Normalized Cipher Randomness Index (NCRI) for monoalphabetic (Caesar) and polyalphabetic (Vigenère) ciphers, demonstrating clear statistical separability between the two classes.

5. Conclusion

This study introduced a machine learning-based cryptanalysis framework grounded in discrete mathematical analysis for the automatic identification of classical encryption algorithms. The proposed approach integrates traditional statistical cryptographic features with a novel hybrid invariant, the Normalized Cipher Randomness Index (NCRI), which combines entropy and the Index of Coincidence to capture both randomness and structural characteristics of ciphertext. A key contribution of this work is the development of a theoretical

foundation for feature separability, demonstrating that NCRI provides a discriminative measure for distinguishing between monoalphabetic and polyalphabetic ciphers. This theoretical insight is supported by experimental results, which show clear separation in NCRI distributions and high classification accuracy across multiple machine learning models. The use of ensemble learning further enhances robustness and generalization capability. The findings indicate that hybrid statistical modeling, when combined with machine learning techniques, can significantly improve the effectiveness of automated cryptanalysis systems. In addition to achieving strong empirical performance, the proposed framework contributes to bridging the gap between classical cryptographic theory and modern data-driven approaches. Future work may extend this framework to include more complex encryption schemes, such as substitution–permutation networks and lightweight block ciphers, as well as deep learning-based architectures for analyzing large-scale cryptographic datasets. Additionally, further theoretical investigation into generalized entropy-based invariants may provide deeper insights into cryptographic structure and security.

References

[1] H. Taherdoost, T.-V. Le, and K. Slimani, "Cryptographic techniques in artificial intelligence security: A bibliometric review," *Cryptography,* vol. 9, no. 1, Art. no. 17 (2025), doi: 10.3390/cryptography9010017.

[2] A. Benamira, D. Gérault, T. Peyrin, and Q. Q. Tan, "A deeper look at machine learning-based cryptanalysis," in *Advances in Cryptology—EUROCRYPT 2021,* pp. 805–835 (2021), doi: 10.1007/978-3-030-77870-5_28.

[3] B. D. Kim, V. A. Vasudevan, R. G. L. D'Oliveira, A. Cohen, T. Stahlbuhk, and M. Médard, "Cryptanalysis via machine learning based information theoretic metrics," arXiv preprint arXiv:2501.15076 (2025).

[4] M. Teng, C. Gao, Z. Wang, and X. Li, "A communication-based identification of critical drones in malicious drone swarm networks," *Complex. Intell. Syst.,* vol. 10, pp. 3197–3211 (2024), doi: 10.1007/s40747-023-01316-9.

[5] R.-T. Su, J.-J. Ren, and S.-Z. Chen, "Improved framework of related-key differential neural distinguisher and applications to the standard ciphers," *Cryptology ePrint Archive*, Rep. 2025/537 (2025).

[6] C. Millichap and Y. Yau, "An artificial neural network approach to finding the key length of the Vigenère cipher," *Cryptologia,* vol. 49, no. 4, pp. 331–347 (2025), doi: 10.1080/01611194.2024.2351117.

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson (2017).

[8] S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York, USA: Anchor Books (2000).

[9] D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York, USA: Scribner (1996).

[10] A. J. Abd and S. Al-Janabi, "Classification and identification of classical cipher type using artificial neural networks," *J. Eng. Appl. Sci.,* vol. 14, no. 11, pp. 3549–3556 (2019), doi: 10.36478/jeasci.2019.3549.3556.

[11] Z. Tolba, M. Derdour, and N. E. H. Dehimi, "Machine learning based cryptanalysis techniques: Perspectives, challenges and future directions," in *Proc. 4th Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, pp. 1–7 (2022).

[12] S. A. Sepúlveda-Fontaine and J. M. Amigó, "Applications of entropy in data analysis and machine learning: A review," *Entropy*, vol. 26, no. 12, Art. no. 1126 (2024), doi: 10.3390/e26121126.

[13] A. Hoayek and D. Rullière, "Assessing clustering methods using Shannon's entropy," *Inf. Sci.*, vol. 689, Art. no. 121510 (2025), doi: 10.1016/j.ins.2024.121510.

[14] J. J. Dani, K. Nakka, and N. Saxena, "A machine learning-based framework for assessing cryptographic indistinguishability of lightweight block ciphers," in *Proc. 22nd Annu. Int. Conf. Privacy, Security Trust (PST)*, pp. 1–10 (2025).

[15] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine learning and cryptanalysis: An in-depth exploration of current practices and future potential," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 257–272 (2024), doi: 10.62411/jcta.9851.

[16] J. Terven, D.-M. Cordova-Esparza, J.-A. Romero-González, A. Ramírez-Pedraza, and E. A. Chávez-Urbiola, "A comprehensive survey of loss functions and metrics in deep learning," *Artif. Intell. Rev.,* vol. 58, Art. no. 195 (2025), doi: 10.1007/s10462-025-11198-7.

[17] Google Developers, "Classification: Accuracy, precision, recall, and related metrics," *Machine Learning Crash Course*. [Accessed: Apr. 8, 2025].

[18] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure

medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

[19] D. Goyal, F. Sheth, P. Mathur, and A. K. Gupta, "Discrete mathematical models for enhancing cybersecurity: A mathematical and statistical analysis of machine learning approaches in phishing attack detection," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-B, pp. 569–599 (2024).

[20] R. Joshi, P. Mathur, A. K. Gupta, S. Singh, V. Paliwal, and S. Nayar, "Mathematical modeling of intelligent system for predicting effectiveness of premenstrual syndrome," *J. Interdiscip. Math.*, vol. 26, no. 3, pp. 551–562 (2023).

Received March, 2026