Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3305–3313
DOI : 10.47974/JDMSC-2817

A discrete graph-theoretic spectral framework for analyzing classical cipher security

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

Abstract

This paper proposes a spectral graph-theoretic framework for cryptanalysis using Cipher Transition Graphs (CTGs) and metrics such as eigenvalues, spectral gap, entropy, clustering, and path length. Results show that plaintext and Caesar cipher share identical properties (spectral gap 1.2056, entropy 12.6732), indicating weak transformation; Vigenère shows slight variation (gap 1.2652, clustering 0.1545); while Playfair exhibits higher clustering (0.1824) but lower entropy (11.4216). Overall, all ciphers retain structural patterns, confirming their moderate security and limitations.

Subject Classification: *Primary 05C50, Secondary 94A60.*

Keywords: *Spectral graph theory, Cryptanalysis, Classical ciphers, Cipher transition graph, Eigenvalue analysis, Graph entropy, Network metrics, Discrete mathematics.*

1. Introduction

Cryptography ensures secure communication by transforming plaintext into ciphertext to maintain confidentiality and integrity. Despite their historical importance, classical ciphers such as Caesar, Vigenère, and Playfair exhibit structural weaknesses that can be exploited by modern techniques. Graph-theoretic methods provide an effective way to model ciphertext as networks, while spectral graph theory reveals hidden structural patterns using eigenvalues and matrix representations [1], [2]. These approaches have been successfully applied in areas like network science and data analysis, and are increasingly used in cryptography [3]–[5]. Entropy-based measures further help quantify randomness in encryption schemes [6], [7]. However, most existing research focuses on modern cryptographic systems, with limited spectral analysis of classical ciphers. Traditional cryptanalysis methods rely mainly on frequency

E-mail: drpriyamathur21@gmail.com

and statistical analysis, which may not capture deeper structural dependencies. To address this gap, this paper proposes a spectral graph-theoretic framework that models ciphertext as a Cipher Transition Graph (CTG) and evaluates it using eigenvalues, spectral gap, entropy, and network metrics, providing a unified approach to assess cipher strength and identify vulnerabilities.

2. Literature Review

Recent studies highlight the growing use of graph theory and spectral analysis in cryptography to model data relationships and evaluate security [3], [5]. Graph-based encryption frameworks improve structural understanding and algorithmic performance [3], [4], while spectral graph theory uses eigenvalues and Laplacian matrices to reveal connectivity and hidden patterns in networks [1], [8]. Entropy-based measures are also widely used to assess randomness, with higher entropy indicating stronger resistance to attacks [6], [7]. Further advancements include chaos-based and hybrid cryptographic models [9], post-quantum approaches using mathematical and graph structures [10], and graph neural networks for complex system analysis [2]. However, spectral graph-theoretic analysis of classical ciphers remains limited [11], [12], [13], as most work focuses on modern encryption or specialized domains. This gap motivates the need for a unified framework integrating graph theory, spectral analysis, and entropy to better evaluate classical ciphers, which is addressed in this work.

4. Methodology

The study proposes a unified spectral graph-theoretic framework for analyzing classical ciphers by modeling ciphertext as a Cipher Transition Graph (CTG). After preprocessing plaintext and applying Caesar, Vigenère, and Playfair encryption, ciphertext is represented as a directed graph of character transitions. From this, adjacency and Laplacian matrices are derived to compute spectral properties such as eigenvalues and spectral gap [1], [2]. Entropy is calculated using probabilistic transitions to measure randomness [3], while structural metrics like density, clustering coefficient, and average path length assess network complexity [2], [4]. Together, these measures provide a comprehensive evaluation of cipher security, as outlined in Figure 1.

Plaintext T is preprocessed by retaining only uppercase alphabetic characters [14], [15], [16], [17], [18], [19]:

$$T' = \{ c \in T \mid c \in A \}, A = \{A, B, \dots, Z\} \tag{1}$$

The processed text is encrypted using classical ciphers:

$$C_i = (P_i + k) mod 26 \tag{2}$$

$$C_i = (P_i + K_i) mod 26 \tag{3}$$

$$(C_1, C_2) = f(P_1, P_2, M) \tag{4}$$

where M is a 5×5 key matrix.

Ciphertext is modeled as a directed Cipher Transition Graph (CTG) [14–19]:

$$G = (V, E) \tag{5}$$

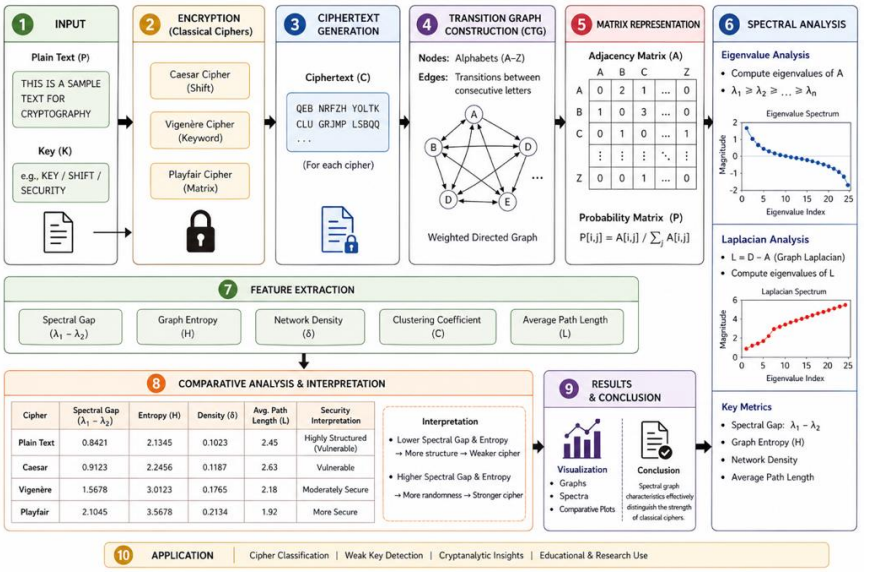

Figure 1
Spectral graph-based cryptanalysis framework for classical ciphers

$$E = \{(c_i, c_{i+1}) \mid i = 1, \ldots, n-1\} \tag{6}$$

with edge weights $w(u, v)$ representing transition frequency. The weighted adjacency matrix is:

$$A_{ij} = \begin{cases} w(v_i, v_j), & \text{if edge exists} \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

Spectral properties are obtained from eigenvalues [14–19]:

$$\lambda_i \in \text{eig}(A) \tag{8}$$

$$\Delta\lambda = \lambda_1 - \lambda_2 \tag{9}$$

A smaller $\Delta\lambda$ indicates higher structural regularity. The Laplacian matrix is:

$$L = D - A \tag{10}$$

$$D_{ii} = \sum_j A_{ij} \tag{11}$$

Structural metrics include density, clustering, and path length [14–19]:

$$\text{Density} = \frac{2|E|}{|V|(|V|-1)} \tag{12}$$

$$C = \frac{1}{|V|} \sum_{i \in V} \frac{2e_i}{k_i(k_i-1)} \tag{13}$$

$$L = \frac{1}{|V|(|V|-1)} \sum_{i \neq j} d(v_i, v_j) \tag{14}$$

Finally, entropy is computed from transition probabilities [14–19]:

$$P_{ij} = \frac{w(i,j)}{\sum_k w(i,k)} \tag{15}$$

$$H = -\sum_{i,j} P_{ij} \log_2 P_{ij} \tag{16}$$

These combined spectral and structural measures enable comprehensive cryptanalysis.

5. Results and Discussion

The effectiveness of the proposed spectral graph-theoretic cryptanalysis framework is validated through a combination of spectral plots, graph visualizations, and quantitative metrics, as summarized in Table 1 and illustrated in Figures 2 to 6. The spectral and Laplacian analyses of Cipher Transition Graphs (CTGs) for Plain text, Caesar, Vigenère, and Playfair ciphers (Figure 2–5) reveal consistent structural patterns, where dominant eigenvalues indicate non-random behavior and preserved transition dependencies. Plain text and Caesar show nearly identical spectra and Laplacian characteristics, confirming identical spectral gap (1.2056) and weak security due to unchanged topology, while Vigenère and Playfair exhibit slightly more distributed eigenvalues and Laplacian spreads, indicating moderate variability and improved diffusion. Graph structures (Figure 6) further support this, with Plain and Caesar showing similar connectivity, Vigenère displaying more distributed transitions, and Playfair exhibiting localized clustering consistent with its higher clustering coefficient. Comparative metrics (Figure 7) show all ciphers have similar spectral gaps (1.20–1.26), with Vigenère highest, entropy highest for Plain and Caesar (12.6732) but lower for Playfair (11.4216), sparse density (~0.10–0.12), highest clustering for Playfair (0.1824), and longest path length for Playfair (2.6324). Overall, as summarized in Table 1, all ciphers remain moderately secure: Caesar offers negligible improvement, Vigenère introduces slight randomness, and Playfair increases local complexity without significant spectral enhancement. These results validate that classical ciphers retain exploitable structural patterns, and the proposed framework effectively captures both global and local properties for cryptanalysis

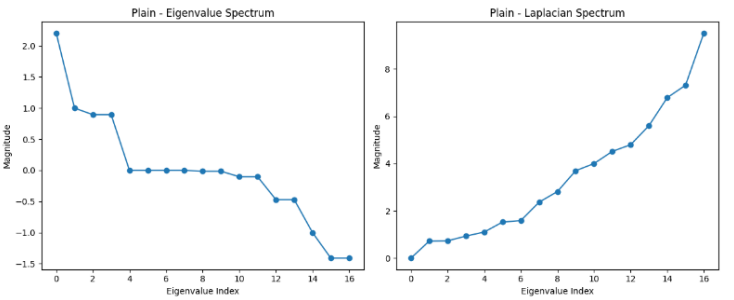

Figure 2
Eigenvalue and Laplacian spectra of the Plain text transition graph.

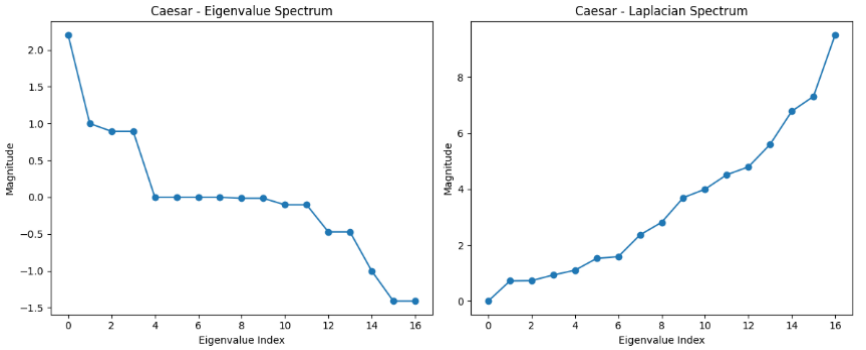

Figure 3

Eigenvalue and Laplacian spectra of the Caesar cipher transition graph.

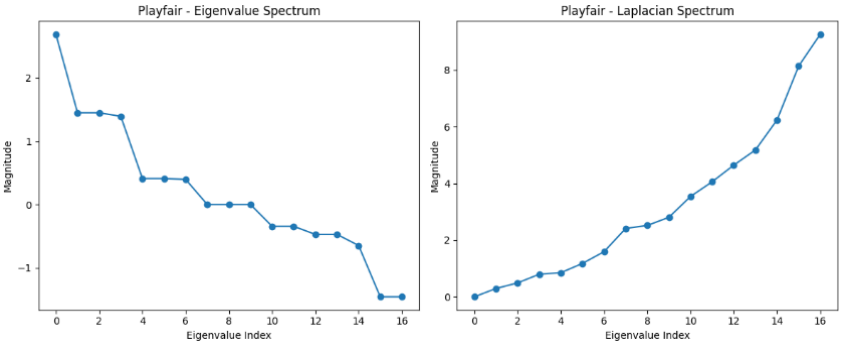

Figure 4

Eigenvalue and Laplacian spectra of the Playfair cipher transition graph.

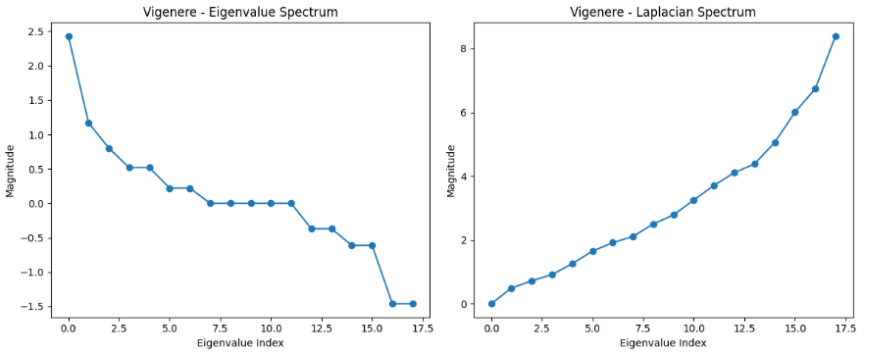

Figure 5

Eigenvalue and Laplacian spectra of the Vigenère cipher transition graph.

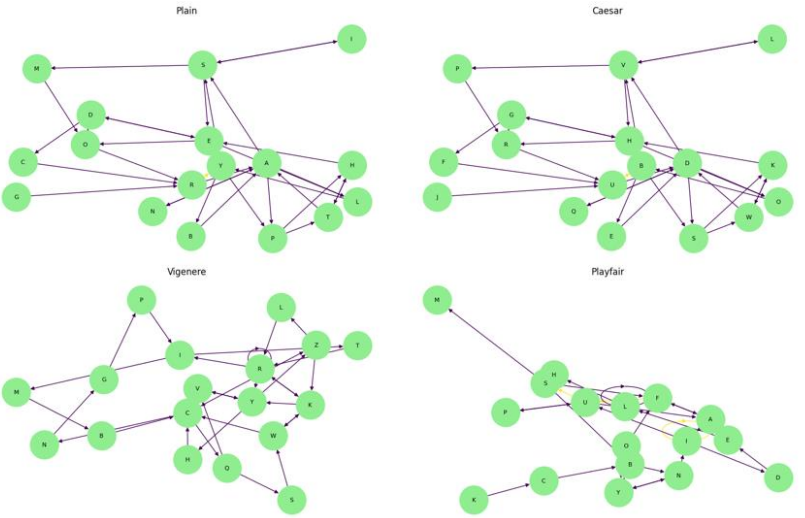

Figure 6
Cipher Transition Graphs (CTGs) for Plain, Caesar, Vigenère, and Playfair ciphers.

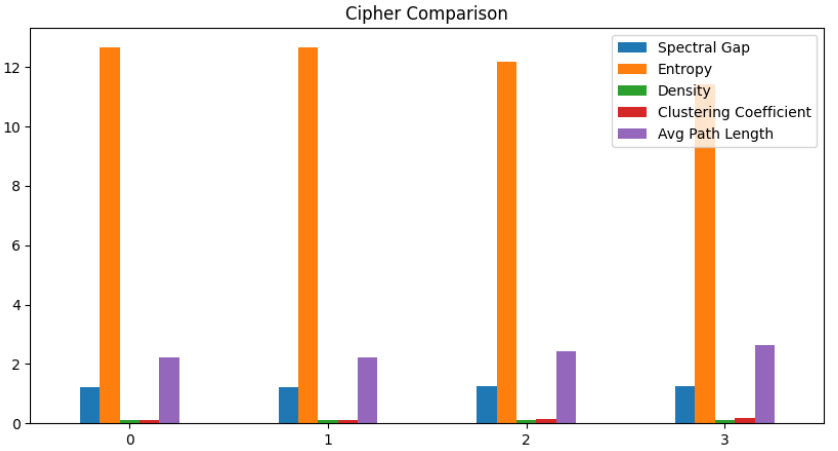

Figure 7
Comparative analysis of spectral and structural metrics across classical ciphers.

Table 1
Spectral and Structural Analysis of Classical Ciphers

CIPHER	SPECTRAL GAP $(\lambda_1 - \lambda_2)$	ENTROPY (H)	DENSITY	CLUSTERING COEFFICIENT	AVG. PATH LENGTH	SECURITY LEVEL
PLAIN	1.2056	12.6732	0.1176	0.1165	2.2059	Moderately Secure

CAESAR	1.2056	12.6732	0.1176	0.1165	2.2059	Moderately Secure
VIGENÈRE	1.2652	12.1699	0.1078	0.1545	2.4248	Moderately Secure
PLAYFAIR	1.2415	11.4216	0.1066	0.1824	2.6324	Moderately Secure

6. Conclusion

This study presents a spectral graph-theoretic framework for analyzing classical ciphers using Cipher Transition Graphs and combined spectral and network metrics. Results show that the Caesar cipher preserves plaintext structure (spectral gap 1.2056, entropy 12.6732), indicating high vulnerability, while Vigenère and Playfair introduce only moderate improvements in variability and local complexity. Despite these differences, all ciphers remain moderately secure and retain exploitable structural patterns. The framework effectively captures both global and local properties, validating its usefulness for cryptanalysis and providing a foundation for extending graph-based methods to modern encryption systems.

References

[1] F. R. K. Chung, *Spectral Graph Theory.* Providence, RI, USA: American Mathematical Society (1997).

[2] S. Ji, S. Pan, E. Cambria, P. Marttinen, and P. S. Yu, "A Survey on Knowledge Graphs: Representation, Acquisition, and Applications," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 2, pp. 494–514 (Feb. 2022), doi: 10.1109/TNNLS.2021.3070843.

[3] Y. Banu, B. K. Rath, and D. Gountia, "Analyzing cryptographic algorithm efficiency within graph-based encryption models," *Frontiers in Computer Science,* vol. 7, Art. no. 1630222 (2025), doi: 10.3389/fcomp.2025.1630222.

[4] K. Song, N. Imran, J. Y. Chen, and A. C. Dobbins, "A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications," *CoRR*, arXiv: abs/2504.08618 (2025).

[5] N. Ali, A. Sadiqa, M. A. Shahzad, M. I. Qureshi, H. M. A. Siddiqui, S. A. O. Abdallah, and N. S. Abd El-Gawaad, "Secure communication in the digital age: A new paradigm with graph-based encryption algorithms," *Frontiers in Computer Science,* vol. 6, Art. no. 1454094 (2024), doi: 10.3389/fcomp.2024.1454094.

[6] W. Alexan, K. M. Hosny, and M. Gabr, "A new fast multiple color image encryption algorithm," *Cluster Computing*, vol. 28, Art. no. 325 (2025), doi: 10.1007/s10586-024-04919-0.

[7] M. Gabr, D. El-Damak, W. Alexan, M. B. M. Mansour, A. M. Elsayed, M. M. Darwish, and K. M. Hosny, "Fibonacci Q-Matrix, Hyperchaos, and Galois Field (2^8) for Augmented Medical Image Encryption," *IEEE Access*, vol. 12, pp. 102718–102744 (2024), doi: 10.1109/ACCESS.2024.3433499.

[8] M. Martín-Nieto, D. Castaño, S. Horta Muñoz, and D. Ruiz, "Solving Mazes: A New Approach Based on Spectral Graph Theory," *Mathematics*, vol. 12, no. 15, Art. no. 2305 (2024), doi: 10.3390/math12152305.

[9] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings," *Groups, Complexity, Cryptology,* vol. 5, pp. 217–225 (2013).

[10] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization," *Computer Security Resource Center (CSRC)*. [Online]. Available: https://csrc.nist.gov/pqc-standardization. [Accessed: Jul. 18, 2026].

[11] 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," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1473–1486 (2025).

[12] 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," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 569–599 (2024).

[13] 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," *Journal of Interdisciplinary Mathematics*, vol. 26, no. 3, pp. 551–562 (2023).

[14] L. Hogben, "Spectral graph theory and the inverse eigenvalue problem of a graph," *The Electronic Journal of Linear Algebra*, vol. 14, pp. 12-31 (2005).

[15] M. E. J. Newman, *Networks: An Introduction*. Oxford, U.K.: Oxford University Press (2010).

[16] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423 (1948).

[17] R. Diestel, *Graph Theory*, 5th ed. Berlin, Germany: Springer (2017).

[18] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press (2014).

[19] U. von Luxburg, "A tutorial on spectral clustering," *Statistics and Computing*, vol. 17, no. 4, pp. 395–416 (2007).

Received March, 2026