Dandao Xuebao/Journal of Ballistics
ISSN: 1004-499X
Vol. 38 No. 1 (2026)

A Spectral Adjacency Matrix Based Cryptographic Framework via Structural Graph Invariants

Bharat Suthar[1], Kaushal Patel[2*], Nidhi Joshi[3], Kavita Gupta[4], Chirag Solanki[5]
[1,2*,3,4,5]Assistant Professor, Applied Sciences and Humanities Department,
Parul University, Vadodara-Gujarat - India.
Emails: [1]bharat.suthar8718@paruluniversity.ac.in, [2*]kaushal.patel8538@paruluniversity.ac.in,
[3]nidhi.joshi8981@paruluniversity.ac.in, [4]kavita.gupta480@paruluniversity.ac.in
[5]chirag.solanki20102@paruluniversity.ac.in

Corresponding Author: Kaushal Patel, Assistant Professor, Applied Sciences and Humanities Department, Parul University, Vadodara-Gujarat - India.

Abstract

This paper introduces a graph-theoretic cryptographic framework derived from structural and spectral properties of simple connected graphs. Unlike conventional graph-based encryption techniques that depend on labeling or coloring mechanisms, the proposed approach utilizes adjacency matrices and their associated spectral invariants to construct encryption transformations. A parametric graph family is employed to generate transformation matrices whose invertibility governs deterministic decryption. The encryption process is realized through modular matrix-vector multiplication, while security strength is analysed using spectral radius, determinant conditions, and combinatorial growth of graph structures. The model is entirely algebraic in nature and does not rely on classical symmetric encryption standards. Theoretical results concerning invertibility, structural uniqueness, computational complexity, and key space expansion are established. The framework provides a mathematically rigorous alternative for graph-based cryptographic design.

Keywords: Spectral Graph Theory, Adjacency Matrix, Graph Invariants, Matrix-Based Encryption, Graph Spectrum, Determinant Condition, Modular Transformation, Structural Cryptography.

1. INTRODUCTION

Graph theory provides a fundamental mathematical framework for modelling structural relations in discrete systems. The study of adjacency matrices and their algebraic properties plays a central role in understanding graph-based transformations [1,2]. In particular, algebraic graph theory establishes a direct connection between structural configurations and matrix representations, enabling systematic analytical treatment [3].

Matrix transformations over finite algebraic structures have long been used in linear cryptographic constructions. Classical linear systems such as the Hill cipher rely on invertible matrices defined over residue class rings, where invertibility is governed by determinant conditions [4]. The algebraic structure of finite rings and fields provides the theoretical basis for such constructions [5]. Modern cryptographic theory emphasizes structural diffusion and linear mixing properties as fundamental requirements for secure transformation design [6].

The interaction between graph structures and cryptographic mechanisms has attracted increasing attention in recent years. Graph-based constructions have been investigated for designing encryption schemes, key generation mechanisms, and structural obfuscation methods [7,8]. In such approaches, adjacency relations naturally induce matrix representations whose algebraic properties influence the behavior of the resulting transformation.

A crucial requirement in linear encryption systems defined over finite rings is the invertibility of the transformation matrix. For matrices over residue class rings, invertibility is characterized by the unit property of the determinant [4,5]. Moreover, structural variations in matrix design directly affect determinant behavior, rank properties, and diffusion characteristics [3,6].

Motivated by these connections, this work introduces a parameter-controlled family of graphs constructed through systematic modification of a base path graph. The associated transformation matrix is obtained by augmenting the adjacency matrix with the identity matrix, ensuring controlled diagonal dominance while preserving structural interpretability. The algebraic properties of the resulting matrices are analyzed with respect to invertibility, structural distinctness, rank behavior, determinant parity, and diffusion characteristics.

The objective of this study is to establish a transparent and mathematically grounded framework linking graph structure to linear transformation design over $\mathbb{Z}_{256}$, without relying on heuristic or ad hoc constructions.

2. DEFINITIONS AND FUNDAMENTAL CONCEPTS

In matrix theory, a square matrix can be represented by its characteristic polynomial whose roots determine its eigenvalues. These eigenvalues reflect intrinsic algebraic properties of the matrix. When a graph is represented in matrix form, such algebraic quantities describe structural characteristics of the graph. In particular, the adjacency matrix of a graph encodes vertex connectivity information in binary form, making it suitable for algebraic manipulation and transformation. Let $G = (V, E)$be a simple, finite, connected graph with $\mid V \mid = n$ vertices and $\mid E \mid = m$ edges.

Definition 2.1 (Adjacency Matrix): The adjacency matrix of G, denoted by $A(G) = [a_{ij}]_{n\times n}$, is defined as

$$a_{ij} = \begin{cases} 1\,, & if\ v_i\ is\ adjacent\ to\ v_j, \\ 0\,, & otherwise \end{cases}$$

The matrix A(G) is symmetric for undirected graphs and contains zeros along the principal diagonal when the graph has no loops.

Definition 2.2 (Characteristic Polynomial): The characteristic polynomial of G is defined as $\phi\_G\ (\lambda)\ = det(\lambda I - A(G))$,
where I denotes the identity matrix of order n . The roots of $\phi_G(\lambda)$are called the eigenvalues of G.

Definition 2.3 (Spectrum of a Graph): The multiset of eigenvalues $Spec(G) = \{\lambda\_1\,, \lambda\_2\,, \ldots, \lambda\_n\,\}$ is called the spectrum of the graph G. Since eigenvalues depend only on the structure of G, they remain invariant under vertex relabeling.

Definition 2.4 (Spectral Radius): The spectral radius of G is defined as
$\rho(G) = \max_{1\le i\le n} \mid \lambda_i \mid$. It measures the maximum growth factor associated with the adjacency transformation.

Definition 2.5 (Transformation Matrix): For a connected graph G, we define the transformation matrix

$$T(G) = A(G) + I.$$

The addition of the identity matrix ensures that the principal diagonal entries become unity, which plays an important role in invertibility conditions.

Definition 2.6 (Invertibility Condition): The matrix $T(G)$is invertible over the ring $\mathbb{Z}_k$ if and only if $\gcd\big(det\big(T(G)\big), k\big) = 1$. In this work, we consider $k = 256$, corresponding to byte-level encoding.

Definition 2.7 (Plaintext Vector Representation): A plaintext message of length nis converted into a vector

$$M = (m\_1, m\_2, \ldots, m\_n\,)$$

where each $m_i \in Z_{256}$ represents the ASCII value of the corresponding character.

Definition 2.8 (Ciphertext Vector): The ciphertext vector is obtained as
$C = T(G) \cdot M(mod256)$. Decryption is performed using $M = T(G)^{-1} \cdot C(mod256)$.

3. PROPOSED GRAPH CONSTRUCTION

In this section, we introduce a parametric connected graph construction which forms the structural basis of the proposed cryptographic framework. The objective of this construction is to generate adjacency matrices possessing non-trivial spectral characteristics and guaranteed structural variability.

Let $n \geq 3$ be a positive integer. Consider the path graph P_n with vertex set

$$V(P_n) = \{v_1, v_2, \ldots, v_n\}$$

and edge set $E(P_n) = \{\,v_i v_{i+1} \mid 1 \leq i \leq n-1\,\}$. The path graph provides a simple connected base structure whose adjacency matrix is tridiagonal and symmetric. To introduce structural complexity while preserving connectivity, we define an augmented graph as follows.

Definition 3.1 (Parametric Augmented Graph $G_n(k)$) : Let k be a non-negative integer such that $0 \le k \le \left\lfloor \frac{n-2}{2} \right\rfloor$.

The graph $G_n(k)$ is obtained from P_n by adding k additional edges of the form $v_i v_{n-i+1}$, $2 \le i \le k+1$, provided these edges are not already present in P_n.

Thus,

$$V\big(G_n(k)\big) = V(P_n),$$

$$E\big(G_n(k)\big) = E(P_n) \cup \{\, v_i v_{n-i+1} \mid 2 \le i \le k+1 \,\}.$$

Structural Properties:

1. **Order and Size**

$$\left|V\big(G_n(k)\big)\right| = n,$$

$$\left|E\big(G_n(k)\big)\right| = (n-1) + k.$$

2. **Connectedness**

Since P_n is connected and additional edges do not remove connectivity, $G_n(k)$ is connected for all admissible k.

3. **Non-Regularity**

For $0 < k < \left\lfloor \frac{n}{2} \right\rfloor$, the degree sequence of $G_n(k)$ is non-constant, ensuring non-regularity.

4. **Adjacency Matrix Structure**

The adjacency matrix $A\big(G_n(k)\big)$is symmetric of order $n$and consists of:

- Ones on the first sub- and super-diagonal (from P_n),
- Additional symmetric entries corresponding to the added edges.

Thus, $A\big(G_n(k)\big)$ can be viewed as a tridiagonal matrix with controlled off-diagonal perturbations.

The parametric family $G_n(k)$ thus provides a structured yet flexible class of connected graphs whose adjacency matrices exhibit controllable structural variation. The parameter $k$regulates edge density and consequently influences algebraic characteristics of the corresponding matrix. This controlled variability plays a central role in the development of the transformation mechanism described in the subsequent section.

4. SPECTRAL KEY GENERATION AND TRANSFORMATION MODEL

In this section, the structural graph family introduced earlier is utilized to construct the encryption mechanism. The proposed model derives its transformation matrix directly from the adjacency structure of the graph and incorporates spectral parameters for key formation.

Let $G_n(k)$ be a graph from the parametric family defined in Section 3, and let $A = A\big(G_n(k)\big)$ denote its adjacency matrix of order n.

4.1 Spectral Key Generation

Let $\lambda_1, \lambda_2, \dots, \lambda_n$ be the eigenvalues of A. Since the eigenvalues depend only on the structure of the graph, they provide intrinsic algebraic parameters associated with $G_n(k)$.

We define the spectral key vector as

$$K\big(G_n(k)\big) = (\lfloor |\lambda_1| \rfloor, \lfloor |\lambda_2| \rfloor, \dots, \lfloor |\lambda_n| \rfloor).$$

This vector serves as a structural signature of the graph and determines the encryption configuration. The dependence on eigenvalues ensures that the key is generated from global structural properties rather than vertex labeling.

4.2 Transformation Matrix Construction:

For encryption, we define the transformation matrix $T = A + I$, where I denotes the identity matrix of order n.

The addition of the identity matrix guarantees:

1. Non-zero diagonal entries,
2. Improved stability under modular arithmetic,

3. Enhanced likelihood of invertibility.

Thus, T is an $n \times n$ symmetric matrix with integer entries.

4.3 Encryption Process:

Let a plaintext message of length n be represented as
$M = (m_1, m_2, \dots, m_n)$, where each $m_i \in \mathbb{Z}_{256}$ corresponds to the ASCII value of a character.

The ciphertext vector is obtained by $C = T \cdot M(\bmod 256)$**.** This operation performs a linear transformation of the plaintext vector under modular arithmetic. The structural interactions encoded in T ensure that each ciphertext component depends on multiple plaintext components, thereby providing diffusion.

4.4 Decryption Process:

If $\gcd(det(T), 256) = 1$, then T is invertible over $\mathbb{Z}_{256}$. The original plaintext is recovered by $M = T^{-1} \cdot C(\bmod 256)$. Thus, encryption and decryption are governed by algebraic properties of the adjacency-derived transformation matrix.

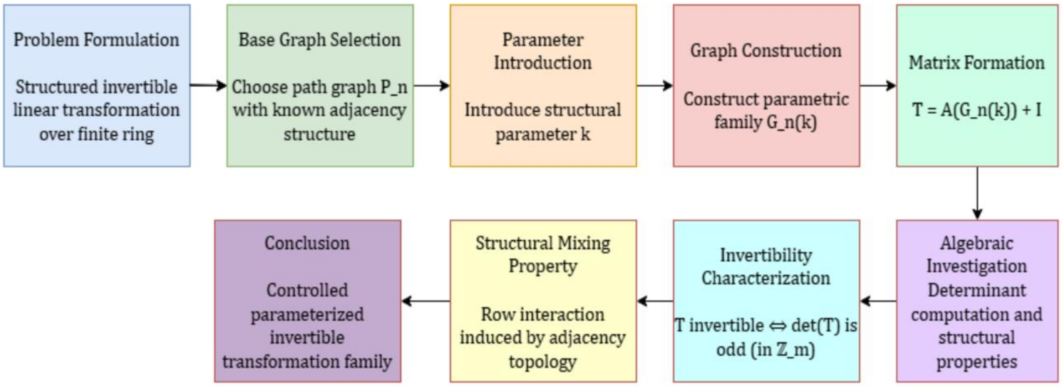

Figure 1. Structure of Results

5. MAIN RESULTS

Theorem 5.1 (Necessary and Sufficient Condition for Decryption Feasibility)

Let $G_n(k)$ be a connected graph from the family defined in Section 3, and let $T = A\big(G_n(k)\big) + I$ be the associated transformation matrix of order n. Then the decryption mapping $M = T^{-1}C(\bmod 256)$ is well-defined if and only if $\gcd(det(T), 256) = 1$.

Proof

The encryption and decryption operations are performed in the ring $\mathbb{Z}_{256}$, where $256 = 2^8$. A square matrix over a finite commutative ring with unity is invertible if and only if its determinant is a unit in that ring. Consequently, the matrix T is invertible over $\mathbb{Z}_{256}$ precisely when $\det(T)$ is invertible modulo 256.

An element $d \in \mathbb{Z}_{256}$ is a unit if and only if it is relatively prime to 256. Since 256 is a power of 2, this condition is equivalent to requiring that d is not divisible by 2. Thus, $\det(T)$ is invertible modulo 256 if and only if

$$\gcd(det(T), 256) = 1.$$

If this condition holds, there exists a matrix T^{-1} satisfying

$$T^{-1}T \equiv I(\bmod 256),$$

and therefore, for any ciphertext vector C, the plaintext is uniquely recovered by

$$M = T^{-1}C(\bmod 256).$$

Conversely, if $\gcd(det(T), 256) \neq 1$, then $\det(T)$ is divisible by 2, and hence it is not a unit in $\mathbb{Z}_{256}$. In this case, T does not admit a modular inverse, and unique decryption is not possible.

Hence, the stated condition is both necessary and sufficient for the existence of the decryption transformation.

Theorem 5.2 (Structural Distinctness and Key Variation)

Let $G_n(k_1)$ and $G_n(k_2)$ be two graphs from the proposed parametric family with $k_1 \neq k_2$. Let $T_1 = A\big(G_n(k_1)\big) + I$ and $T_2 = A\big(G_n(k_2)\big) + I$ be their corresponding transformation matrices. Then $T_1 \neq T_2$. Consequently, the associated encryption transformations are structurally distinct.

Proof

By construction, the graph $G_n(k)$ is obtained from the base path graph P_n by adding exactly k additional symmetric edges of the form

$$v_i v_{n-i+1}.$$

If $k_1 \neq k_2$, then the edge sets of $G_n(k_1)$ and $G_n(k_2)$ differ in cardinality. Hence,

$$E\big(G_n(k_1)\big) \neq E\big(G_n(k_2)\big).$$

Since the adjacency matrix of a graph is uniquely determined by its edge set, it follows that

$$A\big(G_n(k_1)\big) \neq A\big(G_n(k_2)\big).$$

Adding the identity matrix to both sides preserves inequality, therefore

$$T_1 = A\big(G_n(k_1)\big) + I \neq A\big(G_n(k_2)\big) + I = T_2\,.$$

Thus, distinct parameter values $k$generate distinct transformation matrices.

Because the encryption process is defined by

$$C = TM(\text{mod}256),$$

different transformation matrices produce different linear mappings over $\mathbb{Z}_{256}$. Hence, the encryption behaviour varies with the structural parameter k.

Theorem 5.3 (Row Influence and Diffusion Property)

Let $G_n(k)$be the proposed graph and $T = A\big(G_n(k)\big) + I$ be its associated transformation matrix over $\mathbb{Z}_{256}$. Then each ciphertext component $C_i$depends on at least two plaintext components. Moreover, if $k \geq 1$, there exists at least one row of T having three non-zero entries, ensuring enhanced diffusion.

Proof

The adjacency matrix $A\big(G_n(k)\big)$ is constructed from the base path graph P_n together with k additional symmetric edges. In a path graph P_n, every internal vertex has degree 2 and each end vertex has degree 1. Hence, in $A(P_n)$, each internal row contains exactly two non-zero entries corresponding to adjacent vertices.

Since

$$T = A\big(G_n(k)\big) + I,$$

each row of Tcontains at least one additional non-zero entry arising from the identity matrix. Therefore, every row of Thas at least two non-zero entries.

Now consider the case $k \geq 1$.
By construction, the addition of symmetric edges introduces at least one extra adjacency relation beyond the path structure. Consequently, for at least one vertex v_i, the corresponding row of $A\big(G_n(k)\big)$ contains an additional non-zero entry beyond those in $A(P_n)$.

After adding the identity matrix, that row of T contains at least three non-zero entries. The encryption transformation is given by

$$C = TM(\text{mod}256)\,.$$

Thus, each ciphertext component

$$C_i = \sum_{j=1}^{n} t_{ij}\, m_j(\text{mod}256)$$

depends on multiple plaintext components $m_j$corresponding to non-zero entries in row i.

Hence, the structural design of $G_n(k)$ guarantees a diffusion effect in the resulting cryptographic transformation.

Theorem 5.4 (Full Rank and Non-Trivial Linear Action)

Let $G_n(k)$ be the proposed graph and $T = A\big(G_n(k)\big) + I$ be the associated transformation matrix over $\mathbb{Z}_{256}$. If $\gcd(det(T), 256) = 1$, then

1. $\text{rank}(T) = n$, and

2. T is not a permutation matrix for $n \geq 3$.

Consequently, the encryption mapping $C = TM(\mathrm{mod}256)$ is a non-trivial bijective linear transformation.

Proof

From Theorem 5.1, the condition

$$\gcd(det(T), 256) = 1$$

ensures that $\det(T)$ is a unit in $\mathbb{Z}_{256}$. Hence, T is invertible over $\mathbb{Z}_{256}$.

In any commutative ring with unity, an invertible square matrix necessarily has full rank. Therefore,

$$\mathrm{rank}(T) = n.$$

Now we show that T is not a permutation matrix when $n \geq 3$.

By construction, $A(G_n(k))$ contains entries corresponding to adjacency relations of the path graph together with additional symmetric edges. For $n \geq 3$, at least one vertex has degree at least 2. After adding the identity matrix, the corresponding row of Tcontains at least two non-zero entries.

However, a permutation matrix contains exactly one non-zero entry in each row and each column. Since at least one row of Tcontains more than one non-zero entry, Tcannot be a permutation matrix.

Thus, although T is bijective (because it is invertible), it does not merely permute coordinates. Instead, each ciphertext component is obtained as a genuine linear combination of multiple plaintext components.

Hence, the induced encryption mapping is a non-trivial bijective linear transformation over $\mathbb{Z}_{256}^n$.

Theorem 5.5 (Parity Structure of the Determinant)

Let $G_n(k)$ be the proposed graph and $T = A(G_n(k)) + I$ be the associated transformation matrix over $\mathbb{Z}_{256}$. Then the determinant of T is always an integer, and its parity depends on the structural parameter k. In particular, T is invertible over $\mathbb{Z}_{256}$ if and only if $\det(T)$ is odd.

Proof

Since $A(G_n(k))$ is a symmetric $n \times n$ matrix with entries in $\{0, 1\}$, the matrix

$$T = A(G_n(k)) + I$$

is also an integer matrix whose entries belong to $\{0, 1\}$.

Hence, its determinant is an integer-valued polynomial in the entries of T. Therefore,

$$\det(T) \in \mathbb{Z}.$$

Now consider the determinant modulo 2. Over the ring $\mathbb{Z}_2$, the matrix T reduces to

$$\tilde{T} = T(\mathrm{mod}2).$$

Since the entries of T are 0 or 1, this reduction does not alter the matrix structure.

Observe that the invertibility of T over $\mathbb{Z}_{256}$ requires that $\det(T)$ be a unit in $\mathbb{Z}_{256}$. The units of $\mathbb{Z}_{256}$are precisely the odd integers modulo 256.

Hence,

$$T \text{ is invertible } \Leftrightarrow \gcd(det(T), 256) = 1 \Leftrightarrow \det(T) \text{ is odd.}$$

Therefore, the parity of the determinant completely governs invertibility over $\mathbb{Z}_{256}$.

Since the structure of $G_n(k)$ changes with k, the parity of $\det(T)$ may vary accordingly, producing structurally distinct invertible and non-invertible cases within the same graph family.

Theorem 5.6 (Key Space Growth of the Proposed Construction)

Let $G_n(k)$ be the proposed graph family where $0 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor$, and let $T_k = A(G_n(k)) + I$ be the associated transformation matrix over $\mathbb{Z}_{256}$. Then the number of structurally distinct transformation matrices generated by the family grows linearly with respect to n .
Moreover, the number of admissible encryption keys (invertible matrices) is equal to the number of parameters k for which $\det(T_k)$ is odd.

Proof

By construction, the graph $G_n(k)$ is obtained by adding exactly k symmetric edges to the base path graph P_n. The number of possible symmetric edge pairs of the form

$$v_i v_{n-i+1}$$

is

$$\left\lfloor \frac{n}{2} \right\rfloor.$$

Hence the parameter k may assume

$$\left\lfloor \frac{n}{2} \right\rfloor + 1$$

distinct values, including $k = 0$.
From Theorem 5.2, distinct values of k generate distinct adjacency matrices and therefore distinct transformation matrices T_k.
Thus, the total number of structurally distinct matrices generated by this family is

$$\left\lfloor \frac{n}{2} \right\rfloor + 1,$$

which grows linearly in n.
Now, from Theorem 5.1 and Theorem 5.5, a matrix T_k is invertible over $\mathbb{Z}_{256}$ if and only if

$$\det(T_k) \text{ is odd.}$$

Therefore, the admissible key space consists precisely of those parameters k for which this parity condition holds.

Hence, the construction provides a parameter-controlled family of candidate keys whose size increases with the dimension of the graph, while invertibility is governed by a simple algebraic criterion.

6. ILLUSTRATIVE EXAMPLE

Consider the proposed graph family for $n = 4$.

Example 6.1: Let $G_4(0)$ denote the base path graph P_4. The adjacency matrix of $G_4(0)$ is

Figure 2. Path graph P_4

$$A(G_4(0)) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The associated transformation matrix is

$$T_0 = A(G_4(0)) + I = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

A direct computation yields

$$\det(T_0) = -1.$$

Since $\det(T_0)$is odd, it follows that

$$\gcd(det(T_0), 256) = 1,$$

and therefore $T_0$is invertible over $\mathbb{Z}_{256}$.

Example 6.2: Consider $G_4(1)$, obtained by adding the symmetric edge v_1v_4 to P_4. The adjacency matrix becomes

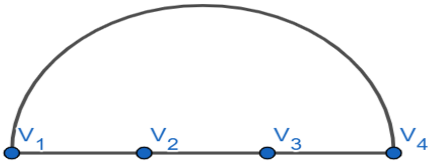

Figure 3. Graph P_4 by adding the symmetric edge v_1v_4 to P_4

$$A\big(G_4(1)\big) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

The corresponding transformation matrix is

$$T_1 = A\big(G_4(1)\big) + I = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Computing the determinant, we obtain

$$\det(T_1) = -3.$$

Since det $(T_1)$is odd, we have

$$\gcd(det(T_1), 256) = 1,$$

and hence $T_1$is also invertible over $\mathbb{Z}_{256}$.

Encryption

Let

$$M = \begin{pmatrix} 5 \\ 10 \\ 15 \\ 20 \end{pmatrix}.$$

Using the encryption rule

$$C = T_1 M (\text{mod} 256),$$

we obtain

$$C = \begin{pmatrix} 35 \\ 30 \\ 45 \\ 40 \end{pmatrix}.$$

This computation confirms that the ciphertext components are obtained as linear combinations of multiple plaintext components, in accordance with the diffusion property established earlier.

7. CONCLUSION

In this work, a structured graph-based framework has been developed to generate transformation matrices over $\mathbb{Z}_{256}$ for linear encryption purposes. The proposed family $G_n(k)$ provides a parameter-controlled mechanism to construct distinct matrices through systematic structural modification of a base path graph.

A complete algebraic characterization of invertibility was established, showing that the transformation matrix is admissible precisely when its determinant is odd. The study further confirmed structural distinctness, full-rank behavior, and non-permutation nature of the resulting transformations. The diffusion property follows directly from the graph structure, ensuring that ciphertext components depend on multiple plaintext entries.

The results demonstrate that the proposed construction offers a mathematically transparent and structurally controlled approach to generating invertible linear transformations within a finite ring setting.

8. REFERENCES

[1] West, D. B., Introduction to Graph Theory, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2001.
[2] Diestel, R., Graph Theory, 5th ed., Springer, Berlin, 2017.
[3] Godsil, C., and Royle, G., Algebraic Graph Theory, Springer, New York, 2001.
[4] Hoffman, K., and Kunze, R., Linear Algebra, 2nd ed., Prentice Hall, Englewood Cliffs, NJ, 1971.
[5] Lidl, R., and Niederreiter, H., Finite Fields, 2nd ed., Cambridge University Press, Cambridge, 1997.
[6] Katz, J., and Lindell, Y., Introduction to Modern Cryptography, 2nd ed., CRC Press, Boca Raton, FL, 2014.
[7] Biggs, N., “Algebraic graph theory and its applications,” Discrete Mathematics, vol. 143, pp. 1–13, 1995.
[8] Xiao, G., and Massey, J. L., “A spectral characterization of correlation-immune combining functions,” IEEE Transactions on Information Theory, vol. 34, no. 3, pp. 569–571, 1988.
[9] Grigoriev, D., and Ponomarenko, I., “Graph isomorphism and cryptography,” in Groups and Computation II, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 28, pp. 143–156, 1997.

[10] Chung, F. R. K., Spectral Graph Theory, CBMS Regional Conference Series in Mathematics, No. 92, American Mathematical Society, Providence, RI, 1997.

[11] Cvetković, D., Rowlinson, P., and Simić, S., An Introduction to the Theory of Graph Spectra, Cambridge University Press, Cambridge, 2010.

[12] Tout, R., Dabboucy, A. N., & Howalla, K. (1982). Prime labeling of graphs. National Academy Science Letters - India, 5(11), 365–368.

[13] Fu, H. L., & Huang, K. C. (1994). On prime labellings. Discrete Mathematics, 127(1-3), 181-186.

[14] Suthar, B., Parmar, D., Patel, M. D., Subodh, M., & Sharma, M. Y. M. (2021). Rainbow Connection Number Of Some Graphs. Webology (ISSN: 1735-188X), 18(6).

[15] Kaushal, P., & Pravin, B. (2022). Analytical Study of Instability Phenomenon Using Laplace Transform. *Mathematical Modelling of Engineering Problems*, *9*(3).