Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 7s (2025)

Bidirectional Matrix-Graph Transformations for Secure Image Scrambling and Descrambling

Binoy Joseph[1], Bindhu K Thomas [2]

[1,2] Mathematics Research Center, Mary Matha Arts and Science College, Mananthavady, Kerala, India.

[1] binoy.sib@gmail.com, [2]bindhukthomas@gmail.com

Article History:

Received: 21-12-2024

Revised: 29-1-2025

Accepted:9-2-2025

Abstract:

The secrecy of data in encryption and decryption process is very important in this multimedia era. This paper introduces a novel scanning method to securely encrypt and decrypt data using a newly defined graph structure. Two key theorems are presented, illustrating the properties of scrambled and descrambled matrices, denoted by $[E_{\mathcal{C}_n}]$and $[EC'_n]$ corresponding to the graph. The proposed method is applied to digital images to demonstrate its effectiveness, providing a foundational understanding of this innovative approach.

Keywords: Graph theory, Elementary Standard Path,SCAN Pattern, Permutation Matrix, Pixel permutation.

1. Introduction

In this era, the role of multimedia information has become an essential part of everyone's life. There are many ways by which it may misused. So the protection of multimedia information has become very important especially from unauthorized access. Cryptography deals with protection of information from unauthorized access.Cryptography is the science of converting secret data into encoded information to ensure it can be transmitted securely without unauthorized access. While classical cryptography has roots stretching back over two thousand years, modern cryptography was formally established by Shannon in 1949 [1]. Graph theory, a branch of mathematics, has seen significant growth not only as a subject of mathematical research but also due to its applications in various fields. Graphs are frequently employed as ciphers to ensure secure communication, even in the presence of adversaries or unauthorized parties.

In [2,3], the authors presents a combinatorial encryption method where graph vertices represent messages, and specific-length walks serve as encryption tools. The concept of Expander Graphs was used in [4]-[7] for solving different problems in Cryptography.

An expander graph is a graph in which every subset of the vertices has many neighbors. In [8] Wael Mahmoud Al E proposed a new encryption algorithm to encrypt and decrypt data securely with the benefits of graph theory properties. In [9] Priyadarsini P. L. K. proposed algorithms for encoding based on strongly regular graphs that have a specific property. In [10]

M. Yamuna proposed a method of encryption using planar graphs. In [11], Gideon Samid patented an encryption method where a graph itself serves as the encryption key.In [12]-[16], pixel scrambling permutation done by using different scan patters.In our proposed image encryption technique we introduces a novel method using graph theory for pixel level permutation . The some of the existing various scan patterns are given in Figure 1.

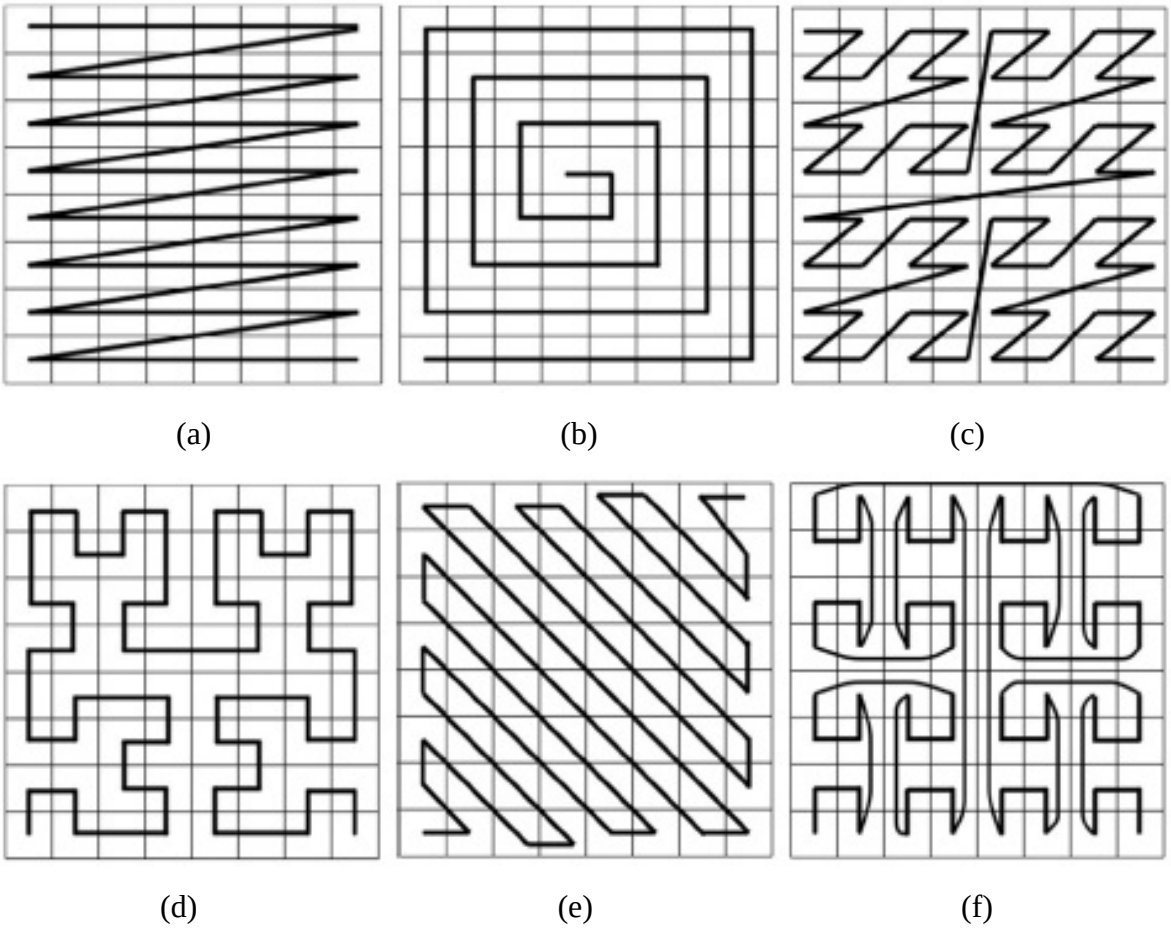


Figure 1: (a) Raster pattern (b) Spiral pattern (c) Z-Order pattern (d) Hilbert Curve pattern (e) Diagonal pattern (f) Gray Pattern

In this paper we propose a novel scanning pattern for pixel scrambling to scan the two dimensional $n \times n$ array of points based on newly defined graph

Let n be a positive integer greater than 1, C be an invertible (0, 1) matrix of order n, such that $C^n = I_n$ (I_n is the identity matrix of order n) and $C^i \neq I_n$, for any i, $(1 < i < n)$ then C will be called a cycle matrix of order n. A cycle matrix of order n in following form called cyclic permutation matrix [17] of order n and denoted by $\mathcal{C}_n$.

$$\mathcal{C}_n = \begin{bmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

This matrix cyclically shifts the elements of any vector **v** = $\left(v_{1,}v_{2,}\dots,v_{n-1},v_n\right)^{\boldsymbol{T}}$ one position to the right, such that:

$$\mathcal{C}_n\mathbf{v} = \left(v_{n,}v_{1,}v_{2,}\dots v_{n-1}\right)^{\boldsymbol{T}}$$

Properties of $\mathcal{C}_n$:

- The matrix $\mathcal{C}_n$ is orthogonal, i.e., $\mathcal{C}_n{\mathcal{C}_n}^T = {\mathcal{C}_n}^T\mathcal{C}_n = I_n$ where I_n is the identity matrix.
- The determinant of $\mathcal{C}_n$ is given by $\det(\mathcal{C}_n) = (-1)^{n-1}$
- The matrix satisfies ${\mathcal{C}_n}^n = I_n$, meaning that after n applications of $\mathcal{C}_n$, we recover the identity matrix.
- If n is any positive integer greater than 1, $\mathcal{C}_n$ is a cyclic permutation matrix, then $(\mathcal{C}_n)^1 + (\mathcal{C}_n)^2 + (\mathcal{C}_n)^3 + \cdots + (\mathcal{C}_n)^n = J_n$ where J_n is an n × n unit matrix.
- Let $A_{n\times n}$ be any matrix of order n, using Hadamard product

$$(\mathcal{C}_n)\odot A + (\mathcal{C}_n)^2\odot A + (\mathcal{C}_n)^3\odot A + \cdots + (\mathcal{C}_n)^n\odot A = A$$

- $(\mathcal{C}_n)^{-1} = (\mathcal{C}_n)^T = (\mathcal{C}_n)^{n-1}$

2. Formation of Graph

Let n be a positive integer and $n \neq 1$. Let $[G_n]$ be an $n \times n$ matrix with entries $\{v_1, v_2, \dots, v_n, \dots, v_n^2\}$ in the following form

$$[G_n] = \begin{bmatrix} v_1 & v_2 & v_3 & \dots & v_n \\ v_{n+1} & v_{n+2} & v_{n+3} & \dots & v_{2n} \\ v_{2n+1} & v_{2n+2} & v_{2n+3} & \dots & v_{3n} \\ \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot\cdot \\ v_{(n-1)n+1} & v_{(n-1)n+2} & v_{(n-1)n+3} & \dots & v_{n^2} \end{bmatrix}$$

We define a graph G_n with vertex set $V = \{v_1, v_2, \dots, v_n, \dots, v_{n^2}\}$ as follows

- The vertex in the j^{th} row of $\left[(\mathcal{C}_n)\odot[G_n]\right]$ is adjacent to the vertex in the $(j+1)^{th}$ row of $\left[(\mathcal{C}_n)\odot[G_n]\right], j = 1,2,3,\dots,n$
- The last vertex in $\left[(\mathcal{C}_n)\odot[G_n]\right]$ is adjacent to the vertex in the last row of $\left[(\mathcal{C}_n)^2\odot[G_n]\right]$
- The vertex in the j^{th} row of $\left[(\mathcal{C}_n)^2\odot[G_n]\right]$ is adjacent to the vertex in the $(j-1)^{th}$ row of $\left[(\mathcal{C}_n)^2\odot[G_n]\right], j = n, n-1, \dots,1$
- The vertex in the first row of $\left[(\mathcal{C}_n)^2\odot[G_n]\right]$ is adjacent to the vertex in the first row of $\left[(\mathcal{C}_n)^3\odot[G_n]\right]$, and so on
  Where $\odot$ denotes the Hadamard product (element-wise multiplication)

Remark 1. The graph thus generated is a path with initial vertex v_n. We called this path as *elementary standard path* and denoted by $E_{\mathcal{C}_n}$ and the corresponding $n \times n$ matrix representation is denoted by $\left[E_{\mathcal{C}_n}\right]$.

The vertices in the graph $E_{\mathcal{C}_n}$ will be denoted using the letter e instead of v to reflect this standard path.The elementary standard path. $E_{\mathcal{C}_4}$ given in the Fig.2.

Illustration. For $n = 4$

$$[G_4] = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ v_5 & v_6 & v_7 & v_8 \\ v_9 & v_{10} & v_{11} & v_{12} \\ v_{13} & v_{14} & v_{15} & v_{16} \end{bmatrix}$$

$$\left[(\mathcal{C}_4) \odot [G_4]\right] = \begin{bmatrix} 0 & 0 & 0 & v_4 \\ v_5 & 0 & 0 & 0 \\ 0 & v_{10} & 0 & 0 \\ 0 & 0 & v_{15} & 0 \end{bmatrix}, \quad \left[(\mathcal{C}_4)^2 \odot [G_4]\right] = \begin{bmatrix} 0 & 0 & v_3 & 0 \\ 0 & 0 & 0 & v_8 \\ v_9 & 0 & 0 & 0 \\ 0 & v_{14} & 0 & 0 \end{bmatrix}$$

$$\left[(\mathcal{C}_4)^3 \odot [G_4]\right] = \begin{bmatrix} 0 & v_2 & 0 & 0 \\ 0 & 0 & v_7 & 0 \\ 0 & 0 & 0 & v_{12} \\ v_{13} & 0 & 0 & 0 \end{bmatrix}, \quad \left[(\mathcal{C}_4)^4 \odot [G_4]\right] = \begin{bmatrix} v_1 & 0 & 0 & 0 \\ 0 & v_6 & 0 & 0 \\ 0 & 0 & v_{11} & 0 \\ 0 & 0 & 0 & v_{16} \end{bmatrix}$$

Figure 2: Graph $E_{\mathcal{C}_4}$

The corresponding 4×4 matrix representation is denoted by $\left[E_{\mathcal{C}_4}\right]$

$$\left[E_{\mathcal{C}_4}\right] = \begin{bmatrix} e_4 & e_5 & e_{10} & e_{15} \\ e_{14} & e_9 & e_8 & e_3 \\ e_2 & e_7 & e_{12} & e_{13} \\ e_{16} & e_{11} & e_6 & e_1 \end{bmatrix}$$

Remark 2. The matrix $\mathcal{C}_n$, is a special type of $n \times n$ square binary matrix that has exactly one entry of 1 in each row and each column and 0s elsewhere. It represents a permutation of the rows and columns of the identity matrix I_n . Multiplying any of $n \times n$ matrix A by $\mathcal{C}_n$ on the left side $(\mathcal{C}_n A)$ which cyclically permutes the rows of A. Similarly Multiplying any $n \times n$ matrix A by $\mathcal{C}_n$ on the right side $(A\mathcal{C}_n)$ which cyclically permutes the columns of A.

Theorem 1. Let $\mathcal{C}_n$ be the cyclic permutation matrix of order n, then

$$\sum_{i=1}^{n} \mathcal{C}_n^i = 1_{n\times n}$$

Where $1_{n\times n}$ is a unit square matrix of order n.

Proof

Let $e_1, e_2, \ldots, e_n$ be the standard basis vectors in R^n, where:

$$e_1 = \begin{bmatrix}1\\0\\0\\\vdots\\0\end{bmatrix}, \quad e_2 = \begin{bmatrix}0\\1\\0\\\vdots\\0\end{bmatrix}, \quad \dots \quad , e_n = \begin{bmatrix}0\\0\\0\\\vdots\\1\end{bmatrix}$$

We can observe the following cyclic properties of the matrix $\mathcal{C}_n^i$ on e_1:

$$\mathcal{C}_n(e_1) = e_2, \quad \mathcal{C}_n^2(e_1) = e_3, \quad \dots, \quad \mathcal{C}_n^{n-1}(e_1) = e_n, \quad \mathcal{C}_n^n(e_1) = e_1.$$

In general, for any i and j, we have

$$\mathcal{C}_n^i(e_j) = e_k, \qquad \text{where} \qquad \text{k} = \begin{cases}(i+j)\ mod\ n & \text{if } (i+j) \neq n\\ n & \text{if } (i+j) = n\end{cases}$$

We know that $e_i e_j^T$ is an $n \times n$ matrix whose (i,j) - th entry is 1, and all other entries are zero. Therefore,

$$I_n = \sum_{i=1}^{n} e_i e_i^T$$

Now, consider:

$$\sum_{i=1}^{n} \mathcal{C}_n^i = \sum_{i=1}^{n} \mathcal{C}_n^i I_n$$

Substituting the expression for I_n:

$$I_n = \sum_{i=1}^{n} \mathcal{C}_n^i \left(\sum_{j=1}^{n} e_j e_j^T \right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \mathcal{C}_n^i\, e_j e_j^T = \sum_{k=1}^{n}\sum_{j=1}^{n} e_k e_j^T = 1_{n\times n},$$

which gives us the $n \times n$ unit matrix.

Theorem 2. Let $[G_n]$ be an $n \times n$ matrix with non-zero real entries. Then the matrices $\mathcal{C}_n^i \odot [G_n]$ for $i = 1, 2, 3, \dots, n$ are disjoint, where $\odot$ denotes the Hadamard product (element-wise multiplication). Moreover, the following holds**:**

$$\sum_{i=1}^{n} \mathcal{C}_n^i \odot [G_n] = [G_n]$$

Proof

From the previous theorem, we have:

$$\sum_{i=1}^{n} \mathcal{C}_n^i = 1_{n\times n}$$

where $1_{n\times n}$ is the unit matrix (matrix of all ones).

Since each $\mathcal{C}_n^i$ is disjoint and the Hadamard product $\odot$ denotes element-wise multiplication, the matrices $\mathcal{C}_n^i \odot [G_n]$ are also disjoint for $i = 1, 2, 3, \dots, n$. Therefore, we can write:

$$\sum_{i=1}^{n} \mathcal{C}_n^i \odot [G_n] = \left(\sum_{i=1}^{n} \mathcal{C}_n^i \right) \odot [G_n] = 1_{n \times n} \odot [G_n] = [G_n]$$

This completes the proof.

Theorem 3. Let $[G_n]$ be an $n \times n$ vertex set. The elementary standard path $[E_{\mathcal{C}_n}]$ corresponding to $[G_n]$ is given by:

$$[E_{\mathcal{C}_n}] = \sum_{i=1}^{n} e_i \left[J_n^{\frac{(-1)^i+1}{2}} \{ (\mathcal{C}_n^i \odot [G_n]) \cdot 1_n(:,1) \} \right]^T$$

where:

$e_i = I_n(:, i)$ is the i-th column of the identity matrix I_n,

J_n is the exchange matrix (also called the reversal matrix, backward identity matrix, or standard involutory permutation matrix), For example, when $n = 3$, we have:

$$J_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

1_n is the matrix of ones, and for $n = 3$:

$$1_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$1_3(:,1) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, is the first column of 1_3

Here, $A \odot B$ represents the Hadamard product between matrices A and B.

Proof. Let $\mathcal{C}_n^i \odot [G_n]$ for $i = 1, 2, 3, \dots, n$ represent n disjoint $n \times n$ matrices, each matrix containing n vertices. For each $\mathcal{C}_n^i \odot [G_n]$, the vertex in the i-th row is adjacent to the vertex in the $(i + 1)$-th row if:

$$i = \begin{cases} 1,3,5,\dots,n & \text{if } n \text{ is odd}, \\ 1,3,5,\dots,(n-1) & \text{if } n \text{ is even}. \end{cases}$$

Each $\mathcal{C}_n^i \odot [G_n]$ gives a disjoint set of adjacent vertices. The matrix $(\mathcal{C}_n^i \odot [G_n]) \cdot 1_n(:,1)$ results in an $n \times 1$ column matrix of such adjacent vertices.

Then $e_i[(\mathcal{C}_n^i \odot [G_n]) \cdot 1_n(:,1)]^T$ represents an $n \times n$ matrix where the adjacent vertices are the row entries in the i-th row for:

$$i = \begin{cases} 1,3,5,\dots,n & \text{if } n \text{ is odd}, \\ 1,3,5,\dots,(n-1) & \text{if } n \text{ is even}. \end{cases}$$

Similarly, $e_i[J_n\{(\mathcal{C}_n^i \odot [G_n]) \cdot 1_n(:,1)\}]^T$ represents an $n \times n$ matrix where the adjacent vertices are the row entries in the i -th row if:

$$i = \begin{cases} 2,4,6,\ldots,n & \text{if } n \text{ is odd,} \\ 2,4,6,\ldots,(n-2) & \text{if } n \text{ is even.} \end{cases}$$

Therefore, the elementary standard path $[E\mathcal{C}_n]$ corresponding to $[G_n]$ is given by

$$\left[E_{\mathcal{C}_n}\right] = \sum_{i=1}^{n} e_i \left[J_n^{\frac{(-1)^i+1}{2}}\{(\mathcal{C}_n^i \odot [G_n]) \cdot 1_n(:,1)\}\right]^T$$

This matrix $\left[E_{\mathcal{C}_n}\right]$ represents the elementary standard path corresponding to the vertex set $[V_n]$.

Illustration

For $n = 4$

$$[G_4] = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ v_5 & v_6 & v_7 & v_8 \\ v_9 & v_{10} & v_{11} & v_{12} \\ v_{13} & v_{14} & v_{15} & v_{16} \end{bmatrix}$$

$$\sum_{i=1}^{4} e_i \left[J_4^{\frac{(-1)^i+1}{2}}\{\left(\mathcal{C}_4^i \odot [G_4]\right) \cdot 1_4(:,1)\}\right]^T$$

$$= e_1[I_4\{(\mathcal{C}_4^1 \odot [G_4]) \cdot 1_4(:,1)\}]^T + e_2[J_4\{(\mathcal{C}_4^2 \odot [G_4]) \cdot 1_4(:,1)\}]^T$$

$$+e_3[I_4\{(\mathcal{C}_4^3 \odot [G_4]) \cdot 1_4(:,1)\}]^T + e_4[J_4\{(\mathcal{C}_4^4 \odot [G_4]) \cdot 1_4(:,1)\}]^T$$

$$= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\left[\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \cdot \left\{\left(\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix} \odot \begin{bmatrix}v_1&v_2&v_3&v_4\\v_5&v_6&v_7&v_8\\v_9&v_{10}&v_{11}&v_{12}\\v_{13}&v_{14}&v_{15}&v_{16}\end{bmatrix}\right) \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}\right]^T$$

$$+ \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\left[\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix} \cdot \left\{\left(\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix} \odot \begin{bmatrix}v_1&v_2&v_3&v_4\\v_5&v_6&v_7&v_8\\v_9&v_{10}&v_{11}&v_{12}\\v_{13}&v_{14}&v_{15}&v_{16}\end{bmatrix}\right) \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}\right]^T$$

$$+ \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\left[\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \cdot \left\{\left(\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix} \odot \begin{bmatrix}v_1&v_2&v_3&v_4\\v_5&v_6&v_7&v_8\\v_9&v_{10}&v_{11}&v_{12}\\v_{13}&v_{14}&v_{15}&v_{16}\end{bmatrix}\right) \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}\right]^T$$

$$+ \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\left[\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix} \cdot \left\{\left(\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \odot \begin{bmatrix}v_1&v_2&v_3&v_4\\v_5&v_6&v_7&v_8\\v_9&v_{10}&v_{11}&v_{12}\\v_{13}&v_{14}&v_{15}&v_{16}\end{bmatrix}\right) \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right\}\right]^T$$

$$= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\left[\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\cdot\begin{bmatrix}v_4\\v_5\\v_{10}\\v_{15}\end{bmatrix}\right]^T + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\left[\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}\cdot\begin{bmatrix}v_3\\v_8\\v_9\\v_{14}\end{bmatrix}\right]^T$$

$$+ \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\left[\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\cdot\begin{bmatrix}v_2\\v_7\\v_{12}\\v_{13}\end{bmatrix}\right]^T + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\left[\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}\cdot\begin{bmatrix}v_1\\v_6\\v_{11}\\v_{16}\end{bmatrix}\right]^T$$

$$= \begin{bmatrix}v_4&v_5&v_{10}&v_{15}\\v_{14}&v_9&v_8&v_3\\v_2&v_7&v_{12}&v_{13}\\v_{16}&v_{11}&v_6&v_1\end{bmatrix} \equiv [E_{\mathcal{C}_4}]$$

3. Inverse Path of an Elementary Standard Path $E_{\mathcal{C}_n}$

Let $E_{\mathcal{C}_n}$ be an elementary standard path corresponding to P_{n^2}, a path of n^2 vertices. Now we discuss inverse path of $E_{\mathcal{C}_n}$ by $E'_{\mathcal{C}_n}$ in the decryption process.

Step 1: Correspondence Between $E_{\mathcal{C}_n}$ and P_{n^2}

To get a correspondence between $E_{\mathcal{C}_n}$ and P_{n^2} , connect the vertex e_i of $E_{\mathcal{C}_n}$ by an edge with the vertex v_i of P_{n^2}. The resulting graph is denoted by G'.

Step 2: Renaming the vertices of $E_{\mathcal{C}_n}$

Rename the vertices of $E_{\mathcal{C}_n}$ as follows.

If e_j is the k^{th} vertex of $E_{\mathcal{C}_n}$, then rename it as e_k, for $1 \le j,k \le n^2$. The resulting graph is G''.

Step 3: Spanning Subgraph G''' of G''

The spanning subgraph G''' of G'' obtained by deleting all the edges of $E_{\mathcal{C}_n}$ in G''.

Step 4: Edge Contraction

In G''' we apply edge contraction between vertices e_i of $E_{\mathcal{C}_n}$ and v_j of P_{n^2} and renamed it as e_i. The resulting graph formed by this edge contraction is denoted by EC'_n.

Illustration

For $n = 3$,

Correspondence between $E_{\mathcal{C}_3}$ and P_{3^2}

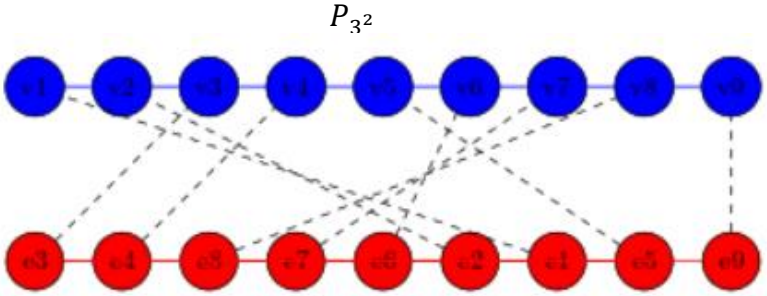


Figure 3: Graph G'

Renaming the vertices of $E_{\mathcal{C}_3}$

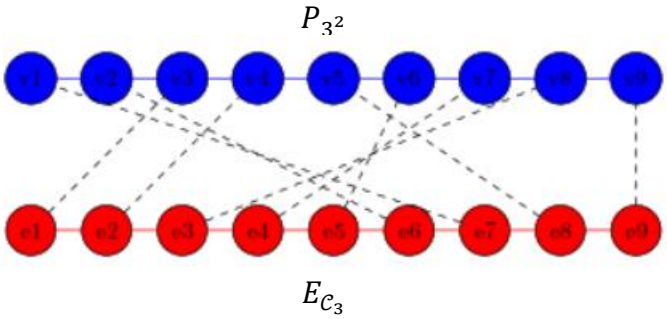


Figure 4: Graph G'' with renamed vertices in $E_{\mathcal{C}_3}$

Spanning subgraph G''' of G''

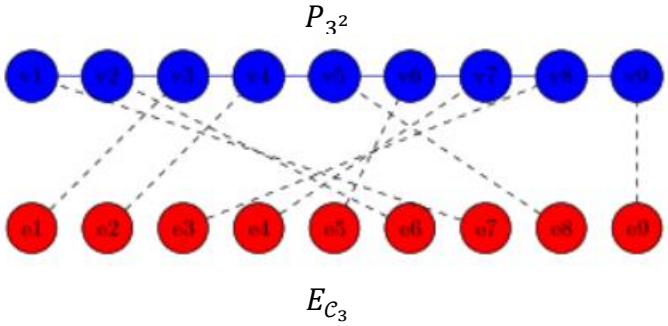


Figure 5: Graph G'''

Edge Contraction

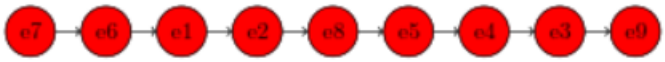


Figure 6: Graph $E\mathcal{C}'_3$

Theorem 4. Let $[G_n]$ be an n $\times$ n vertex set corresponding to a path P_{n^2}. Then the inverse path of an elementary standard path $E\mathcal{C}_n$ is denoted by $E\mathcal{C}'_n$ and the corresponding matrix is denoted by $\left[E'_{\mathcal{C}_n}\right]$. It is given by the formula:

$$\left[E'_{\mathcal{C}_n}\right] = \sum_{i=1}^{n} \mathcal{C}_{n^i} \left(\left[\left\{ (\mathcal{C}_{n^i})^{-1} \cdot \left(J_n^{\frac{(-1)^i+1}{2}} \cdot [G_n](i,:)^T \right) \right\} \cdot 1_n(1,:) \right] \odot I_n \right) \qquad (1)$$

Proof.

Let $[G_n]$ represent an $n \times n$ vertex set corresponding to the path P_{n^2}. For $i = 1, 2, \ldots, n$, the matrix $[G_n](i,:)^T$ represents the column matrix of order $n \times 1$, formed by taking the i-th row of $[G_n]$.

The operation $J_n^{\frac{(-1)^i+1}{2}}$ alternates between the identity matrix and a permutation matrix based on the parity of i. This alternation modifies the sequence of vertices to align with the inverse operation $(\mathcal{C}_n^i)^{-1}$, which reverses the cyclic shift of $\mathcal{C}_n^i$.

For each i, the expression

$$(\mathcal{C}_n^i)^{-1} \cdot \left(J_n^{\frac{(-1)^i+1}{2}} \cdot [G_n](i,:)^T \right)$$

represents the order of vertices under the reverse cyclic shift $(\mathcal{C}_n^i)^{-1}$.
The term

$$\left(\left[\left\{ (\mathcal{C}_n^i)^{-1} \cdot \left(J_n^{\frac{(-1)^i+1}{2}} \cdot [G_n](i,:)^T \right) \right\} \cdot 1_n(1,:) \right] \odot I_n \right)$$

produces an $n \times n$ diagonal matrix, where the diagonal elements correspond to the i-th row of $[G_n]$ under the reverse shift operation $(\mathcal{C}_n^i)^{-1}$.
By multiplying this diagonal matrix with $\mathcal{C}_n^i$, the diagonal elements are aligned with the nonzero positions of $\mathcal{C}_n^i$ in the respective order.
Finally, summing over all $i = 1, 2, \dots, n$,

$$\sum_{i=1}^{n} \mathcal{C}_n^i \cdot \left(\left[\left\{ (\mathcal{C}_n^i)^{-1} \cdot \left(J_n^{\frac{(-1)^i+1}{2}} \cdot [G_n](i,:)^T \right) \right\} \cdot 1_n(1,:) \right] \odot I_n \right),$$

aggregates the contributions of all reversed matrices to form the matrix $\left[E'_{\mathcal{C}_n}\right]$.

Illustration
For $n = 4$

$$[G_4] = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ v_5 & v_6 & v_7 & v_8 \\ v_9 & v_{10} & v_{11} & v_{12} \\ v_{13} & v_{14} & v_{15} & v_{16} \end{bmatrix}$$

$$\sum_{i=1}^{4} \mathcal{C}_4^i \left(\left[\left\{ (\mathcal{C}_4^i)^{-1} \cdot \left(J_4^{\frac{(-1)^i+1}{2}} \cdot [G_4](i,:)^T \right) \right\} \cdot 1_4(1,:) \right] \odot I_4 \right)$$

$$= \mathcal{C}_4^1([\{(\mathcal{C}_4^1)^{-1} \cdot (J_4^0 \cdot [G_4](1,:)^T)\} \cdot 1_4(1,:)] \odot I_4)$$

$$+\mathcal{C}_4^2([\{(\mathcal{C}_4^2)^{-1} \cdot (J_4 \cdot [G_4](2,:)^T)\} \cdot 1_4(1,:)] \odot I_4)$$

$$+\mathcal{C}_4^3([\{(\mathcal{C}_4^3)^{-1} \cdot (J_4^0 \cdot [G_4](3,:)^T)\} \cdot 1_4(1,:)] \odot I_4)$$

$$+\mathcal{C}_4^4([\{(\mathcal{C}_4^4)^{-1} \cdot (J_4 \cdot [G_4](4,:)^T)\} \cdot 1_4(1,:)] \odot I_4)$$

$$= \begin{bmatrix} 0 & 0 & 0 & v_1 \\ v_2 & 0 & 0 & 0 \\ 0 & v_3 & 0 & 0 \\ 0 & 0 & v_4 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & v_8 & 0 \\ 0 & 0 & 0 & v_7 \\ v_6 & 0 & 0 & 0 \\ 0 & v_5 & 0 & 0 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & v_9 & 0 & 0 \\ 0 & 0 & v_{10} & 0 \\ 0 & 0 & 0 & v_{11} \\ v_{12} & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} v_{16} & 0 & 0 & 0 \\ 0 & v_{15} & 0 & 0 \\ 0 & 0 & v_{14} & 0 \\ 0 & 0 & 0 & v_{13} \end{bmatrix}$$

$$= \begin{bmatrix} e_{16} & e_9 & e_8 & e_1 \\ e_2 & e_{15} & e_{10} & e_7 \\ e_6 & e_3 & e_{14} & e_{11} \\ e_{12} & e_5 & e_4 & e_{13} \end{bmatrix} \equiv [EC_4']$$

The vertices in the graph $[EC_4']$ is denoted using the letter 'e' instead of 'v' to reflect this standard path.

Figure 7: Graph E'_{C_4}

For

$$A = [E_{C_4}] = \begin{bmatrix} e_4 & e_5 & e_{10} & e_{15} \\ e_{14} & e_9 & e_8 & e_3 \\ e_2 & e_7 & e_{12} & e_{13} \\ e_{16} & e_{11} & e_6 & e_1 \end{bmatrix}$$

We get the inverse path matrix $[EC_4']$ as

$$[EC_4'] = \begin{bmatrix} e_1 & e_2 & e_3 & e_4 \\ e_5 & e_6 & e_7 & e_8 \\ e_9 & e_{10} & e_{11} & e_{12} \\ e_{13} & e_{14} & e_{15} & e_{16} \end{bmatrix}$$

3.1 SCAN Pattern

The matrix corresponding to the path E_{C_n} of $n \times n$ array of points is a new scan pattern to scan the $n \times n$ array of points. The pixel level permutation done by the path E_{C_n} and we get a scrambled image $[E_{C_n}]$ of size $n \times n$.\\
The decryption process done by the path E'_{C_n}, the corresponding matrix we get decrypted image of size $n \times n$.

Illustration: Encryption and Decryption of a matrix of size 10×10

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 \\ 51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\ 61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 \\ 71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\ 81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\ 91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100 \end{bmatrix}$$

Figure 8: Original Matrix

$$\begin{bmatrix} 10 & 11 & 22 & 33 & 44 & 55 & 66 & 77 & 88 & 99 \\ 98 & 87 & 76 & 65 & 54 & 43 & 32 & 21 & 20 & 9 \\ 8 & 19 & 30 & 31 & 42 & 53 & 64 & 75 & 86 & 97 \\ 96 & 85 & 74 & 63 & 52 & 41 & 40 & 29 & 18 & 7 \\ 6 & 17 & 28 & 39 & 50 & 51 & 62 & 73 & 84 & 95 \\ 94 & 83 & 72 & 61 & 60 & 49 & 38 & 27 & 16 & 5 \\ 4 & 15 & 26 & 37 & 48 & 59 & 70 & 71 & 82 & 93 \\ 92 & 81 & 80 & 69 & 58 & 47 & 36 & 25 & 14 & 3 \\ 2 & 13 & 24 & 35 & 46 & 57 & 68 & 79 & 90 & 91 \\ 100 & 89 & 78 & 67 & 56 & 45 & 34 & 23 & 12 & 1 \end{bmatrix}$$

Figure 9: Scrambled Matrix corresponding to the path $E_{C_{10}}$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 \\ 51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\ 61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 \\ 71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\ 81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\ 91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100 \end{bmatrix}$$

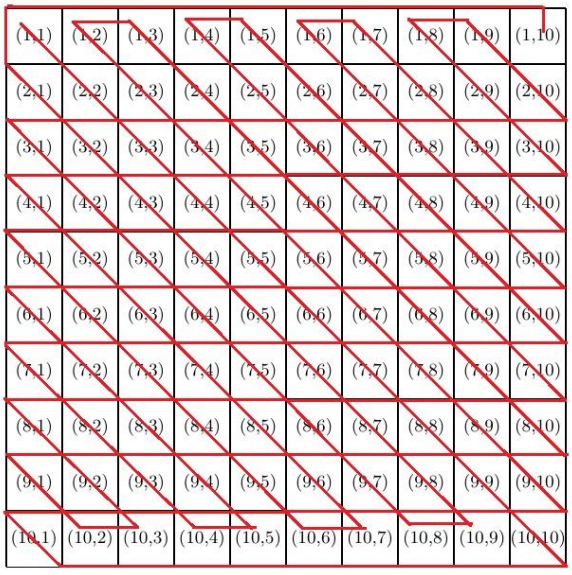
Figure 10: Decrypted Matrix corresponding to the path $E'_{\mathcal{C}_{10}}$

3.2 Applications to Digital Images

The proposed scanning pattern provides an effective approach for scrambling digital images. By employing this method, a 256 × 256 pixel image is represented as a matrix. From this matrix, the representation of the standard elementary path $[E_{\mathcal{C}_{256}}]$ is derived, which forms the scrambled matrix of the given digital image.

For the inverse process, the matrix representation of inverse path $[E'_{\mathcal{C}_{256}}]$ is utilized to regenerate the original image accurately. This ensures a reversible transformation, making the method suitable for secure image encryption and decryption applications.

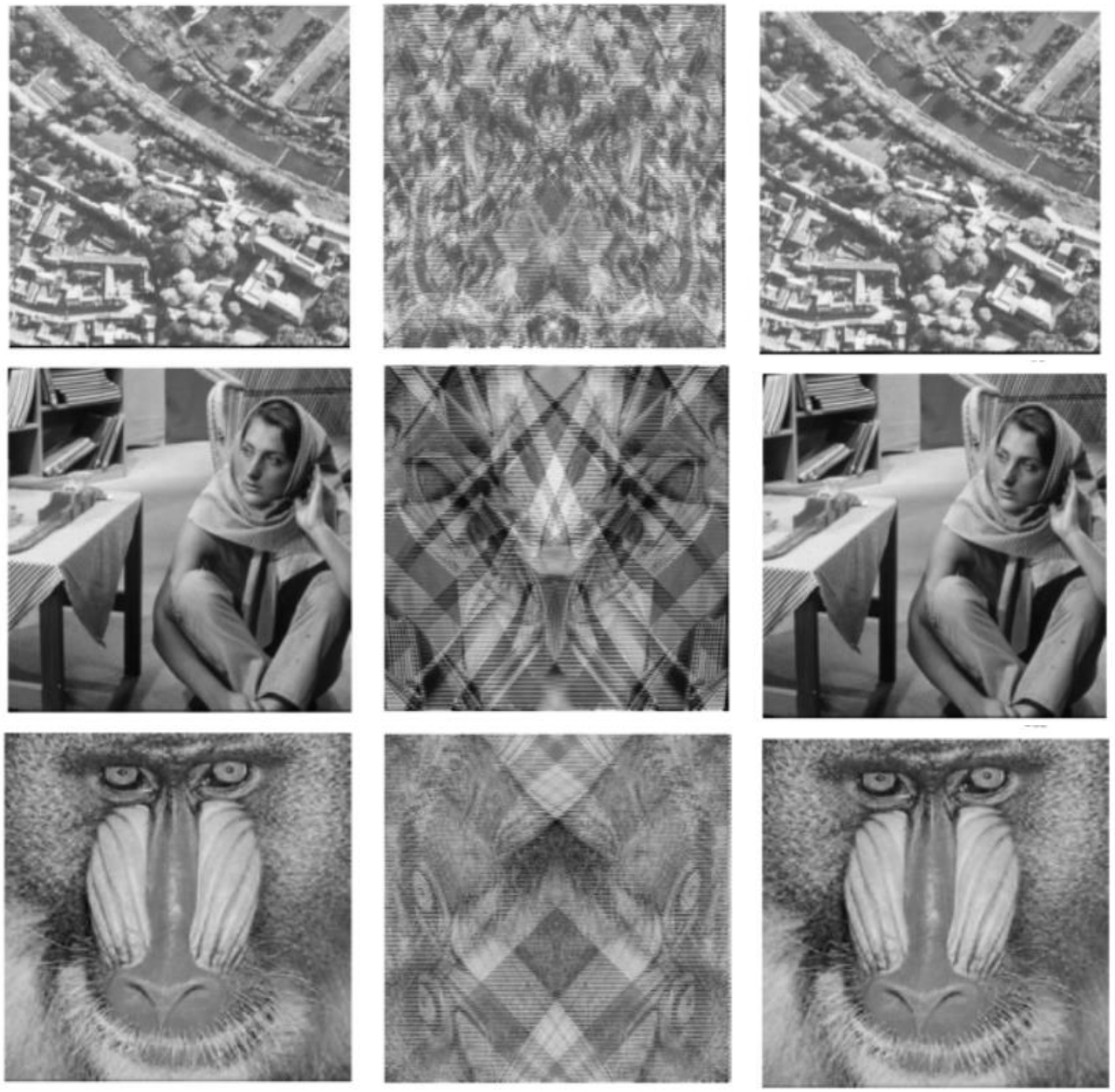
Such an approach highlights its potential in protecting sensitive image data, enabling secure transmission and storage, and offering robust solutions for image scrambling in various domains. Fig.12 illustrates the scrambling and descrambling of images using $[E_{\mathcal{C}_{256}}]$ and $[E'_{\mathcal{C}_{256}}]$.



(1,10)	(2,1)	(3,2)	(4,3)	(5,4)	(6,5)	(7,6)	(8,7)	(9,8)	(10,9)
(10,8)	(9,7)	(8,6)	(7,5)	(6,4)	(5,3)	(4,2)	(3,1)	(2,10)	(1,9)
(1,8)	(2,9)	(3,10)	(4,1)	(5,2)	(6,3)	(7,4)	(8,5)	(9,6)	(10,7)
(10,6)	(9,5)	(8,4)	(7,3)	(6,2)	(5,1)	(4,10)	(3,9)	(2,8)	(1,7)
(1,6)	(2,7)	(3,8)	(4,9)	(5,10)	(6,1)	(7,2)	(8,3)	(9,4)	(10,5)
(10,4)	(9,3)	(8,2)	(7,1)	(6,10)	(5,9)	(4,8)	(3,7)	(2,6)	(1,5)
(1,4)	(2,5)	(3,6)	(4,7)	(5,8)	(6,9)	(7,10)	(8,1)	(9,2)	(10,3)
(10,2)	(9,1)	(8,10)	(7,9)	(6,8)	(5,7)	(4,6)	(3,5)	(2,4)	(1,3)
(1,2)	(2,3)	(3,4)	(4,5)	(5,6)	(6,7)	(7,8)	(8,9)	(9,10)	(10,1)
(10,10)	(9,9)	(8,8)	(7,7)	(6,6)	(5,5)	(4,4)	(3,3)	(2,2)	(1,1)

(a) Proposed Method **(b) Scan Coordinate**

Figure 11: Pixel permutation using proposed method.



(a) Original Image **(b) Scrambled Image by $[E_{C_{256}}]$** **(c) Decrypted Image by $[E'_{C_{256}}]$**

Figure 12: Scrambling and Descrambling of images using $[E_{C_{256}}]$ and $[E'_{C_{256}}]$

4. Conclusions

This study demonstrates the effectiveness of the proposed scanning method for digital image scrambling and descrambling. Utilizing a newly defined graph structure derived from an $n \times n$ array of points, the method ensures a secure approach to data encryption and decryption. The two key theorems, describing the properties of scrambled and descrambled matrices for $n \times n$ digital images, denoted by $[E_{C_n}]$ and $[E'_{C_n}]$, establish a robust theoretical foundation. These results underscore the potential of this innovative technique to enhance image security in the multimedia era.

5. Future Works

Future research will explore the repeated application of the proposed method and investigate pixel value modifications using the same framework. This will further expand the applicability and robustness of the method in advanced image processing and security applications**.**

References

[1] C.E. Shannon, Communication theory of secrecy, Bell Labs Tech.J. 28(4),656-715 (1949)
[2] Vasyl Ustimenko. Cryptim:graphs as tools for symmetric encryption in:lecture notes in computer sci. Springer,New York, 2227, 2001.
[3] V. Ustimenko. Graphs with special arcs and cryptography. Acta Applicandae Mathematicae, 74:117–153, 11 2002.
[4] Dawn Song, J. Tygar, and David Zuckerman. Expander graphs for digital stream authentication and robust overlay networks. 05 2002.
[5] David Jao, Stephen Miller, and Ramarathnam Venkatesan. Expander graphs based on grh with an application to elliptic curve cryptography. Journal of Number Theory, 129:1491–1504, 06 2009.
[6] Denis Charles, Kristin Lauter, and Eyal Goren. Cryptographic hash functions from expander graphs. Journal of Cryptology, 22:93–113, 12 2008.
[7] Oded Goldreich. Candidate one-way functions based on expander graphs. Cryptology ePrint Archive, Paper 2000/063, 2000.
[8] Wael Etaiwi. Encryption algorithm using graph theory. Journal of Scientific Research and Reports, 3:2519–2527, 01 2014.
[9] P.L.K. Priyadarsini and Ramakalyan Ayyagari. Ciphers based on special graphs. Pages 460–465, 08 2013.
[10] M Yamuna and Elakkiya A. Planar graph in data encryption. International Journal of Advance Research in Science and Engineering,IJARSE, 04, 03 2015.
[11] Samid Gideon. Denial cryptography based on graph theory. US patent 6823068B1-2004, 2004.
[12] T. Sivakumar, R. Venkatesan, A new image encryption method based on knight's travel path and true random number. J. Inf. Sci. Eng.32 (1)(2016) 133-152
[13] S.S. Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN. Pattern Recognit. 34(6)(2001) 1229-1245.
[14] S.S. Maniccam, N.G. Bourbakis, Image and video encryption using SCAN patterns. Pattern Recognit. 37(4)(2004) 725-737.
[15] T. Sivakumar, R. Venkatesan, Image encryption based on pixel shuffling and random key stream, Int. J. Comput. Inform. Technol. 3(06)(2014)
[16] T. Sivakumar, R. Venkatesan, A novel approach for image encryption using dynamic SCAN pattern, IAENG international journal of computer science, 41(2).
[17]Li, Wenwei, A Note on the Classification of Permutation Matrix, 10.48550/arXiv.1803.02199,2017,01.