International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Message Transfer using Associated Matrices

Yazhini Gopalakrishnan, M. Yamuna

Abstract*: Communication is the act of sharing information, ideas and thoughts through writings and speeches. Communication has played a significant role in attaining ones freedom and rights. Communication dates back from 3200BC. In the early development messengers were employed to transfer messages. In this modern era of technology data is transferred through the use of internet. As the pattern of message transfer changes, security of the encrypted message becomes a message. New methods are developed for this purpose. This paper would focuses on the secure transfer of information using properties of vector spaces and graph theory.

***Keywords*: Coding, Cryptography, Decoding, Vector Space, Graph**

I. INTRODUCTION

We live in a world occupied by 7.7 billion people. With such a voluminous population comes the difficulty of connectivity and communication. We also live in an era dominated by technology. Technology has been developing at an alarming rate and it is also inconceivable of what would come next. However with the advent of technology the issue of staying connected has become easier. Smartphones and social media has revolutionized how we interact with one another. Unfortunately, technology threatens privacy and has also reduced the amount of control we have over our personal data. Messages sent through the internet is quickly hacked and used without the knowledge of the sender. Cyber hacking has victimized several innocent people. Stolen data's include credit card pin number, photographs and private information. In order to secure important details, messages are sent through techniques like steganography, Morse code, Yodeling and many more. Graph theory has been extensively used in message transfer. In [1] degree of vertices have been used in message transfer. In [2] a method of encrypting the molecular formula of drugs is proposed using level order tree traversal. In [3] a chemical equation is encrypted using directed graphs. Linear Algebra is also used in message transfer. In [4] a method of transferring message using matrices is explained. In this paper we propose yet another method to communicate important information through coding and decoding messages using vector space and graph theory.

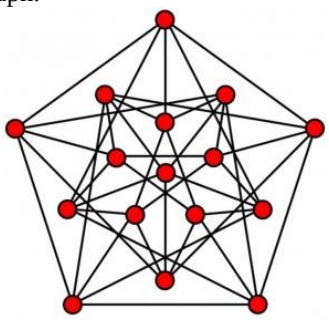
Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Yazhini Gopalakrishnan, Vellore Institute of Technology, Vellore, India.
M. Yamuna*, Department of Mathematics, Vellore Institute of Technology, Vellore,

II. PRELIMINARY NOTE

In this section we provide the basic definitions and results required for easy understanding of the proposed method.
For results and definitions in Linear Algebra, we refer to [4].

Graph

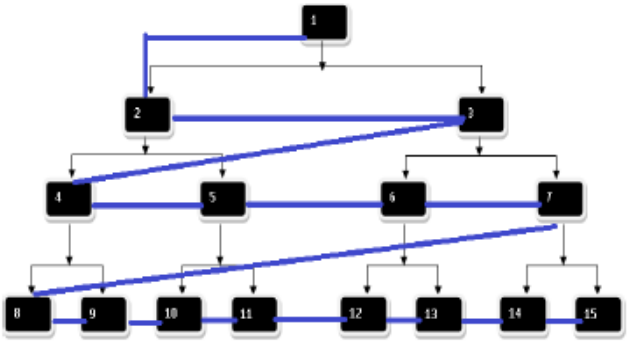
A graph is a collection of points and lines connecting some subset of them. The points of a graph are known as vertices. The lines connecting the vertices of a graph are known as edges [5]. A weighted graph is a graph in which each edge is assigned some numerical value . Snapshot – 1 [6] provides an example of graph.



Snapshot – 1

Level Order Tree Traversal

It starts at the tree root and explores the neighbor nodes first, before moving to the next level neighbors [7]. Snapshot - 2 [8] provides an example of level – order tree traversal.



Snapshot – 2

Linear Transformation

Let V and W be vector spaces. A function T: V→ W is said to be a linear transformation if for all x, y ∈ V, and scalar k the following conditions hold

- T (x + y) = T (x) + T (y)
- T (kx) = k T (x)

Associated Matrix

Let T: V→ W be a linear transformation with basis α = { v1, v2,…, vn} and β = { w1, w2, …, wm } respectively.

Then $T(v_j) = \sum_{i=i}^{m} a_{ij} w_i, 1 \le j \le n.$

The matrix

$[T]_{\alpha}^{\beta} = \begin{bmatrix} a_{11} & L & a_{1n} \\ M & & M \\ a_{m1} & & a_{mn} \end{bmatrix}$ is called the associated matrix with respect to the transformation T.

III. PROPOSED ENCRYPTION SCHEME

Any normal encryption can be chart can be used. Let us consider the case of transferring a regular message which contains only alphabets.

Let us use the following sample chart

A	B	C	. . .	Z	Blank space
1	2	3		26	27

Table – 1

ENCRYPTION ALGORITHM

Let M be the message encrypted. Let length of M be k. Let M: **GOOD JOB** be the message to be encrypted.

In this case k = 8.

Step 1 Convert M into numbers using Table 1.

This creates a string of numbers

S: $w_1, w_2, w_{3...}w_k$

For our example S: 7, 15, 15, 4, 27, 10, 15, 2

Step 2. Create a matrix A of order n x n, $n^2 \ge k$, where aij represents string S row wise, that is

$$A = \begin{bmatrix} w_1 & w_2 & L & w_n \\ w_{n+1} & w_{n+2} & L & w_{2n} \\ M & M & & M \\ w_{n(n-1)+1} & w_{n(n-1)+2} & L & w_{nn} \end{bmatrix}$$

If $n^2 > k$, assign any integer greater than or equal to 27, or assign the value zero.

For our example

$$A = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 27 & 10 \\ 15 & 2 & 0 \end{bmatrix}$$

Note that k = 8 here, so a_{33} is chosen as zero

Step 3 Choose a suitable linear transformation that generates an associated matrix of order of n x n,

For our example since A is of order of 3 x 3, we need to choose a suitable transformation that generates an associated matrix with at least 8 entries.

Let us choose the transformation T: $R^3 \rightarrow R^3$with standard bases $\alpha = \{ e_1, e_2, e_3 \}$ defined by

$T(x, y, z) = (2x - 3y + 4z , 5x - y + 2z , 4x + 7y)$

Step 4 Let P = A + T

For our example

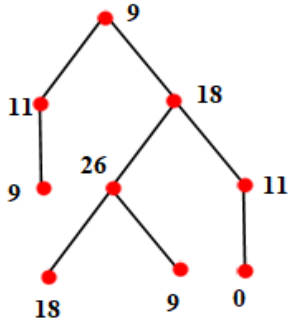
$$P = \begin{bmatrix} 9 & 12 & 19 \\ 9 & 26 & 12 \\ 19 & 9 & 0 \end{bmatrix}$$

Step 5 Choose a tree T with n^2 vertices. Assign the weights of matrix P using level order transversal in the order of P_{11}, $P_{12...}P_{1n}$, $P_{21,...}P_{2n,}$ $...P_{n1,}$ $...P_{nn}$

For our example we need a tree with 9 vertices

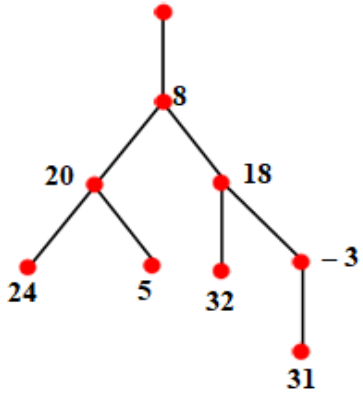
The resulting tree is as seen in the figure 1.

Step 6 Send the tree T to the receiver.



DECRYPTION

Decryption can be done by reversing the procedure. Suppose the received tree T is as seen in figure 2.



T has 9 vertices, so matrix S is of order 3 x 3 using level order traversal

$$S = \begin{bmatrix} 8 & 8 & 20 \\ 18 & 24 & 5 \\ 32 & -3 & 31 \end{bmatrix}$$

Suppose the transformation used is T: $R^3 \rightarrow R^3$ defined by $T(x, y, z) = (2y + z , x - 4y, 3x)$ with basis $\beta = \{ e_3, e_2, e_1 \}$

$$\text{Then } [T]_{\beta} = \begin{bmatrix} 0 & 7 & 4 \\ 2 & -1 & 5 \\ 4 & -3 & 2 \end{bmatrix}$$

$$A = S - T = \begin{bmatrix} 8 & 1 & 16 \\ 16 & 25 & 0 \\ 28 & 0 & 29 \end{bmatrix}$$

S= 8, 1, 16, 16, 25, 0, 28, 0, 29. From string S, we should remove integers greater than or equal to 27 and any integer that is zero. So the message part from string S is 8, 1, 16, 16, 25.

Convert this into message using Table 1.Therefore the message decrypted is **HAPPY**.

IV. CONCLUSION

The proposed method uses double encryption. It is almost impossible to decode the message without the key without the following reasons

- If level tree traversal is not used, then the correct message cannot be decoded. For the tree in figure 2,9 vertices are there, which means that it can be arranged in 9! ways (9!= 362880). Therefore the

Probability P(correct guess) = 1/ 9! or in general $1/n^2$.

Note that n^2! becomes a larger number as the size of the message increases.

- Matrix T is also used as a key for encryption as well as for decryption. Until the correct transformation and bases is known, creating the associated matrix is highly impossible.

Among the n number of matrices available, it is impossible to guess T as an associated matrix.

Without this A = S – T is not possible.

- Integer zero and integers ≥ 28 are not considered when the encoding chart is used. If one attempts to decrypt a message along with these integers then they would end up encoding a wrong message.

So the data to be encrypted is protected at multi levels.

Therefore the data is secure between the encoder and decoder preventing the misuse and the privacy of the data.

REFERENCES

1. M. Yamuna, “Degree sequence in message transfer,” Materials Science and Engineering., vol. 263, Aug. 2017, pp. 1–7.
2. M. Yamuna, A. Eakkiya, “Periodic table in medical molecular formula safe transfer,” Der Pharmacia Lettre., vol. 8, 2015, pp. 135 –142.
3. M. Yamuna, A. Eakkiya, “Chemical ewuation as a directed graph,” Der Pharma Chemica., vol. 7, 2015, pp. 49 – 55.
4. Jin Ho Kwak, Sungpyo Hong , Linear Algebra. Boston: Springer International, 2004, ch. 4.
5. http://securityaffairs.co/wordpress/33879/security/dna-cryptography.html
6. http://mathworld.wolfram.com/Graph.html
7. https://en.wikipedia.org/wiki/Tree_%28graph_theory%29.