Vertex Magic Total Labelling and its Application in Cryptography

[1]Rahul Chawla, [2]Sagar Deshpande, Manas M.N., Saahil Chhabria, Krishnappa H. K.

Department of Computer Science and Engineering, Rashtreeya Vidyalaya College of Engineering, Bengaluru, Karnataka - 560059, India

[1]rahulchawla2801@gmail.com, [2]sagardespande.76@gmail.com,
manasmn@rvce.edu.in, saahil.work@gmail.com,
krishnappahk@rvce.edu.in

Abstract. Vertex Magic Total Labelling, VMTL of a graph G is a labelling concept wherein for each vertex, the sum of all the weights of incident edges on a vertex and the weight of the vertex is a constant, and this constant is known as magic constant. VMTL is a labelling which generates constant, unique number patterns for a particular graph. Such labelling of a graph can be leveraged to develop a cryptosystem by mapping sensitive data on VMTL and encrypting the data. For every word in the input text, different labelling is achieved based on the characteristic of the text so that two same word in different messages have different encoded form. A hash function is used for the same which takes in the date of text and size of the word to generate a hash value which is the order of the graph, for which VMTL is achieved and then the word is mapped on it. Efficiency for generating labelling for the graph plays an important role thus low, odd ordered complete graphs are considered.

Keywords : Vertex Magic Total Labelling, Cryptosystem, Complete Graphs, Hashing.

1 Introduction

It is a known fact that Vertex Magic Total Labelling, VMTL is exhibited by all complete graphs, among other graphs. Labelling obtained through the process of VTML on a graph has applications in domain of data mining and network security. We refer algorithm by Krishnappa, Srinath, Ramakanth from [1] to understand how a VMTL table is generated for an odd complete graph. Each column in the table stores the weights of all the incident edges on a vertex and weight of that vertex. The sum of all the weights in a column is a constant that is magic constant. The pattern of numbers generated are unique and constant with respect to a particular graph and thus mapping and unmapping of text on such stream of numbers is easily achievable. Sender and receiver use same algorithm to encrypt and decrypt the messages. The computation speed of VMTL table for odd ordered complete graphs is evaluated on a regular system and a graph of number of vertices versus time is plotted and it is quite evident that computation speed grows in an unproportionate manner. Only odd ordered graphs are considered and used for mapping as achieving labelling for it is simpler than even ordered graphs.

Depending on the characteristic of the input text example word length, date of creation the stream of numbers is generated which are nothing but labellings of a particular order of complete graph. The cryptosystem considered here involves a hash function which for each word in the input text returns the order of the graph and then that word is mapped on the labellings of the graph fetched. As these characteristics are constant even after encoding, the receiver at the receiving end can use a similar hash function to decode the message.

2 Related Work

The research on applications of Vertex Magic Total Labelling in the field of computer science is relatively new. Few algorithms exist to achieve labelling on different types of graphs, although our research is limited to dealing with labelling of only complete graphs and applying in cryptography. Cryptography is a domain in computer science now, but it existed way before the onset of Internet and was facilitated by mathematicians working on mathematical functions to form ciphers. New algorithms have been introduced in recent years which contribute to the efficiency and throughput of the cryptosystem, like algorithm explained by Nilesh and Nagle in [2]. Cryptography can be broadly classified in two ways, first is to convert the sensitive data to ciphertext using a cipher which both sender and receiver side share, and the second is to hide sensitive data in audio-video files as explained by Praveen and Arun in [3], a technique called as Steganography. Our technique falls in the first category which deals with conversion of sensitive text to an encoded form.

The algorithms to compute Vertex Magic Total Labelling are well known which include the method proposed by authors in [1] that deals with labelling of complete graphs. They propose two algorithms to construct the VMTL table, one for each odd and even number of vertices in the graph. Security has always been concern since the onset of internet till today as full assurance is not achieved by conventionally used RSA algorithm to obtain perfect secrecy. An extra mapping that will make the cryptosystem more robust as explained by authors in [4] is necessary as double layered encryption are hard to decipher without a key if data packet are sniffed in between the transmission. Multi threading is used for dividing the encrypting process among threads also providing them with locks while dealing with shared variables in order to make significant impact on computation speed as described by Balasubramani and Subba Rao in [5].

3 Methodology

The process involves encrypting message by mapping the text on the content of the vertex magic total labelling of different orders of graphs retrieved by feeding a key to a hash function, H1 as shown in the Fig.1. to generate hash values. The structure of the key and the hash function can be decided beforehand by both the communicating parties. In this case let's assume key includes the date of the creation of the message and word length of different words in the message. The hash function is

$$H(D,L) = D*10 +(2*L +1) = \text{hash value} \quad (1)$$

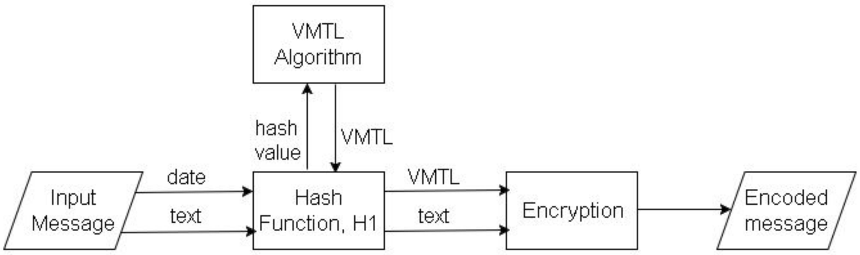

Fig. 1. Encryption

where L is the word length, D is the day of the month ranging from 1 to 31. Hash value returned in equation (1) will always be odd and it is nothing but the order of the graph whose labelling are to be considered for mapping. For instance, the message is sent on 01/02/2015 and the word length is 4, the hash value becomes 19, thus vertex magic total labelling of graph of order 19 is considered using the algorithm referred from [1]. The adjacency matrix has 19*19=361 different numeric values which can be used for encoding by mapping 3 61 different characters on it.

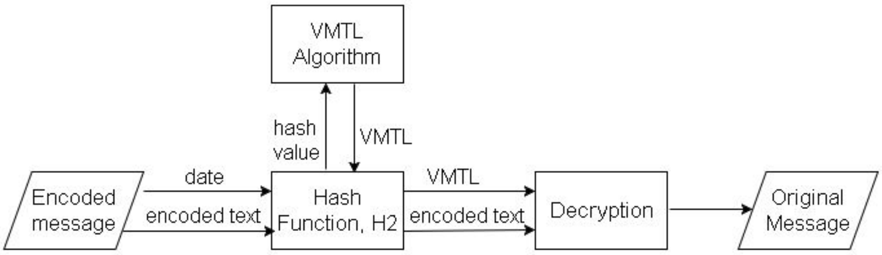

Fig. 2. Decryption

The ASCII code of the character in the input word acts as index in the adjacency matrix of the labelled graph to retrieve a code for the character. The boundary conditions are taken care of as the minimum hash value is 13 which contains 13*13 =

169 that is 169 different characters can be mapped on the labelling which is greater than 128 different ASCII characters that is the range of characters in the input text.
As shown in the figure the sender side generates hash values and sends it to the script running the algorithm to compute the vertex magic total labelling. For each word a thread is created so that the execution can takes place asynchronously and the time complexity is reduced. The labellings are returned to the sender side, encryption takes place by mapping the characters on labelling and then sent to the receiver. The receiver on the other side has similar hash function, H2 as shown in the Fig.2. to decrypt the code.

4 Experimental Analysis

Execution time for algorithm expressed by authors in [1] to compute VMTL for odd ordered complete graph is recorded for different orders. This is done to check whether dynamically computing VMTL for every word while encrypting the message is feasible or not. The graph as shown in the Fig.3. is formulated for the computation time in seconds of labelling for different vertices. It can be clearly observed that the time taken for computing labelling for low orders is less and increases unproportionally for higher orders. It is quite evident that low order labellings can be easily computed dynamically while encrypting and won’t hinder the efficiency.

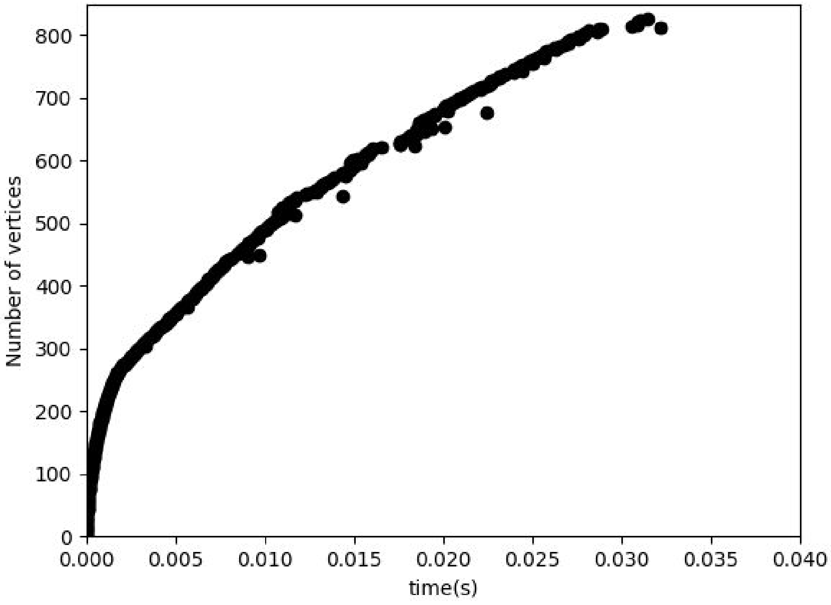

Fig. 3. Order Vs Time

5 Conclusion

Vertex magic total labelling of a complete graph produces stream of numbers which are unique and constant for each graph The efficiency of computing labelling for odd ordered complete grows unproportional thus using low odd ordered graphs for encryption is a feasible solution.

This property helps in mapping sensitive text to the labelling and form encoded text which can be transferred to the receiver side with secrecy even if security breach takes place and packets get sniffed in between the transmission. Selection of a specific VMTL of a complete graph is determined by the size of the word which acts as input key to the hash function which returns order of the graph as hash value. Data is mapped on the labellings achieved on the ordered graph which is in the form of stream of numbers.

6 Future Scope

The encryption of information in a way that same words have different encoded form in same message depending on other factors such as length of the document, placement of word in the document, serial number of the original message, occurrence of data around specific keywords, date of the message transmission all together in considering the selection of ordered graph labelling thus making the cryptosystem robust.

Encryption of audio-video files can be achieved once the computation of labelling for high ordered complete graph is efficient as size of such files is big and will require high ordered graph mapping. Caching of stream of numbers for graph labelling at the sender and receiver side for a message rather than computing the labelling again and again for every word will be a huge step up in the complexity.

References

1. Krishnappa H.K., N.K.Srinath, Ramakanth Kumar P, Vertex Magic Total Labelling of Complete Graphs, AKCE International Journal of Graphs and Combinatorics, Vol. 1, Issue 6, 2009
2. Dudhatra Nilesh, Malti Nagle, The new cryptography algorithm with high throughput, International Conference on Computer Communication and Informatics, 2014
3. Praveen. P, Arun. R, Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm, International Journal of Engineering Inventions, Vol. 2, Issue 4, 2014
4. Krishnappa H.K., N.K.Srinath, S. Manjunath, Vertex Magic Total Labelling of Complete Graphs and their Application for Public – Key Cryptosystem , International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 2, 2013
5. A. Balasubramani, Chdv. Subba Rao, Sliced Images and Encryption Techniques in Steganography Using Multi Threading For Fast Retrieval, International Journal of Applied Engineering Research, Volume 11, Number 9, 2016