ISBN: 978-81-19149-52-0

11. Data Protection by MIS Technique

S. K. Pal

School of Computing & Analytics,
N.S.H.M. Knowledge Campus,
Kolkata, WB.

B. Datta

Dept. of CSE,
B.B.I.T.,
Kolkata, WB.

A. Karmakar

Dept. of CSE,
M.A.K.A.U.T.,
Nadia, WB.

Abstract:

Data protection on digital platforms is becoming a critical problem due to the internet of things' (IoT) fast adoption of digital gadgets. The nature of threats continuously changing day-by-day. The researchers and professionals are continuously working and innovating several models to protect confidential information form anonymous people. Since security is never ending process therefore a novel information protection algorithm is presented in this paper which is based on identification of maximal independent set (MIS) using graph Colouring technique. In this paper the idea of tree parity machine is used to generate random graph. The proposed information hiding method is simple and effective as per needs. The presented algorithm can be used to embed confidential information in the digital devices to maintain privacy and validity of data integrity in the IoT platform as well.

Keywords:

Cryptography, Encryption, Decryption, Information hiding, Ciphering, MIS.

11.1 Introduction:

The process of transforming Information to unreadable format called encryption and unreadable data is cipher text. The reverse process that is conversion of cipher text to its original text is named decryption. The whole method of encryption and decryption is called cryptography. The Cryptography algorithms classified mainly into three major categories: symmetric/Private-key cryptography, asymmetric/Public-key cryptography and hash function (compression functions). Private-key cryptography uses identical key used for encoding and decoding process by sender and receiver.

The key is shared separately and secretly between the sender and receiver. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are best instance of Private-key cryptography. In public-key or as you say asymmetric key crypto system sender and receiver uses two dissimilar keys for encryption and decryption data.

Two types of keys exist in this method, a private key and a public key. Data encryption and decryption require the public and private keys, respectively. Public keys can therefore be freely shared, whilst private keys must remain confidential.

In Graph Coloring, assign colours to each vertex of a graph G in the graph colouring technique so that neighbouring vertex colours never match. (Pal, S. K., & Chakraborty, N. 2017, Pal, S. K., & Mishra, S. 2019). The objective is to accustom the fewest possible colours overall to colour a graph. The chromatic number of a particular graph is the least number of colours used to colour it. Graph colouring is currently an NP Complete Category problem.

The idea of graph coloring is used for conflict determination in problem. The type like, the certain couples of elements are in-compatible in a vertex set V. The issue is to determine the fewest possible subsets of elements that can coexist by fencing off vertex set V (Qu, G., & Potkonjak, M. 1998, Berghel, H., & O'Gorman, L. 1996).

The situation can be explained by a straightforward connected graph, G= (vertices V, edges E), in which all pairs of incompatible elements are used to form the vertex set V, and edge set E.

In order to properly colour that graph, the vertex set can be divided into k subsets, which is equivalent to the total number of colours used (Gu, J., Qu, G., & Zhou, Q. 2009, Croitoru, C., Luchian, H., Gheorghies, O., & Apetrei, A. 2002). A polynomial time algorithm cannot solve the NP-complete problem of identifying the chromatic number of a graph.

An independent set is a subset of nodes in an undirected graph where nodes in the subset cannot be adjacent. If no node can be added to the subset without creating an irreverent independent set known as the maximum-independent-set, the independent set is maximal. A set with a maximum cardinality is referred to as the maximum independent set (MIS) (Qu, G., & Potkonjak, M. 1998, Pal, S. K., & Sarma, S. S. 2012).

Here, in this model a random graph is created assuming probability of edge density by using the idea of tree parity machine. A degree-constraint-matrix is created based on the created random graph (Pal, S. K., Datta, B., & Karmakar, A., 2021).

The help graph colouring has been used in this paper to describe an information hiding technique. The suggested technique used to determine independent set(s) of the original graph and give each set a different colour. Watermarking is the specific arrangement of independent sets and its vertices.

By recreating the independent sets in the precise order of creation, the message, which takes the form of a binary string, can be extracted from the watermark.

11.2. Terminologies:

In this section some terminology has defined which has been used further in next sections of this paper.

11.2.1 Degree Constraint Matrix:

A degree constraint matrix (DCM) is created from the graph G, which contains fields like, node n_i, adjacent vertices corresponding to each node n_i, of graph, and degree-sum of all the adjacent nodes.

11.2.2 Vertex Colouring:

Vertex colouring involves giving each vertex in a graph a different colour, in a way such that adjacent vertex cannot have similar colour. The assignment of colour is done in a way such that it only uses a few colours to colour each vertex. The minimum number of colour by which all vertices of the graph is coloured is called chromatic number.

11.2.3 Watermark:

Watermark is the method of embedding message in the image, audio, or even in video, in a way such that original message cannot extract by anonymous person. The embedded message can be extract only if know the embedding procedure. Watermark is used to protect, identify an object.

11.2.4 Tree Parity Machine:

The multi-layered feedforward network that makes up the tree parity machine has (KxN) input neurons, K hidden neurons, and a single output neuron (Pal, S. K., Datta, B., & Karmakar, A. 2021, Pal, S. K., & Mishra, S. 2019).

Here, input of the network is X_{ij}.= (-1, 0, +1).

A weight is assigned to the link have in between the input to hidden neurons is, W_{ij}= {-L, …, 0, …, +L}.

The hidden layer output is calculated using formula,

$$\sigma_i = sgn\left(\sum_{j=1}^{N} W_{ij} X_{ij}\right)$$

Signum function return following values,

sgn(x)= {-1 when value of x less than 0,

0 when value of x equal to 0,

1 when value of x greter than 1}.

The formula below is used to calculate the output.

$$\tau = \prod_{i=1}^{k} \sigma_i$$

11.3. Algorithm for Information Hiding:

- **Step 1:** Start
- **Step 2:** Enter number of nodes (n), and probability of edge (p), of graph.
- **Step 3:** Created random a graph G (n, p), using tree parity machine.
- **Step 4:** Input message(m) and convert it into ASCII number.
- **Step 5:** Degree-constraint-matrix (DCM) of the current graph was created by adding the degrees of all of the adjacent nodes, or degree-sum. Every node of the DCM matrix is taken into consideration for this operation.
- **Step 6:** Select a node n_i, from DCM which is corresponding to the value highest degree-sum.
- **Step 7:** Find out length l, of the message to be hide in round one using formula $2^{\lfloor n_i \rfloor}$, where node n_i, in respect to the maximum degree-sum of present-graph.
- **Step 8:** Eliminate the node n_i, and stored it in the set MIS.
- **Step 9:** The neighbours of n_i, is removed the graph and keep it in redraw-matrix (RD).
- **Step 10:** Modify present-graph after removed the node n_i, and it neighbours.
- **Step 11:** The vertices reorder again of the newly formed graph that is, present-graph.
- **Step 12:** Repeat step 5 to step 11, till present graph contains more than two nodes.
- **Step 13:** Construct new present graph using vertices of redraw-matrix (RD = existing-graph - MIS).
- **Step 14:** Continue step-5 to step-13 till message(M) not empty.
- **Step 15:** Stop.

11.4. Retrieve of Message:

The maximal independent set created with specific sequence of the vertices is actually hiding of message in the graph is watermark. The binary string messages can retrieve from created watermark rebuilding the maximal-independent-set in the specified order. The original message in binary form is encrypted in the maximal-independent-set which was created by the proposed methods. The specific order of selected maximal-independent-sets regulates credibility. A vertex may include in any one maximal-independent-set of graphs. The order of vertices in the maximal-independent-set has an important role therefore keep maintain specific order (Pal, S. K., &Sarma, S. S. 2012). A maximal-independent-set with k nodes, that are arranged differently will produce different messages. However, the likelihood of getting similar maximal-independent-set from dissimilar messages after encryption. If the sequence is rearranged using the same technique's maximal-independent set indexes, the concealed binary string will be altered.

11.5. Experimental Analysis:

The presented algorithm has an O (log n) time complexity, because message has been embedded into the nodes of a graph is exactly once. The message embedding process will continue until message is empty. The C programming language has been used to implement the algorithm provided in this study. The experimental result compared and analysed with the existing algorithm (Qu, G., & Potkonjak, M. 1998, Pal, S. K., &Sarma, S. S. 2012). The programs were executed by creating a simple connected random graph with different number nodes and edge density. The specified node count (n) and edge density (p) are used to generate the graph. The execution time of each algorithms corresponding is mentioned, Table 1 lists the number of nodes and edge densities. A comparative chart of the algorithm's performance given in the figure 11.1.

Table 11.1: Execution Time Taken by The Programs

Node Count	Edge	Algorithm Execution time (in second)		
		(Qu, G., & Potkonjak, M. 1998) algorithm	(Pal, S. K., &Sarma, S. S. 2012) algorithm	Presented algorithm
10	42	35.80	35.72	35.49
15	72	100.55	98.76	97.22
20	97	233.67	224.32	221.34
25	78	430.65	424.31	428.57
30	30	578.44	559.22	553.42
35	121	1276.45	1229.57	1189.79
40	66	987.43	971.89	957.61
45	86	1188.33	1118.76	1081.59

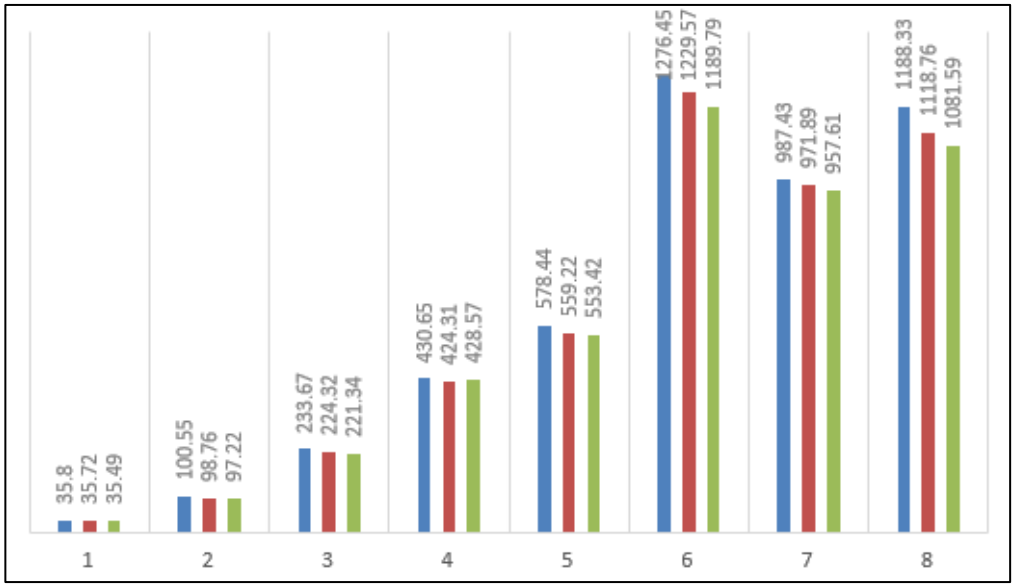

Figure 11.1: Pictorial representation of data given in table 11.1.

11.6. Conclusion:

The cryptography is a tool which is used to increase security level of data during communication even data is passing through insecure public channel. By applying dynamic cryptography tools and techniques the protection of data can improve in the area defence, banking, digital business industry and even in government sector. It is true cryptography alone is not enough to provide data protection and privacy in reality but it cannot ignore too. The algorithm presented is developed using unique approach of identification on maximal independent set by graph colouring. The graph is generated randomly using tree parity machine.

11.7 References:

1. Berghel, H., & O'Gorman, L. (1996). Protecting ownership rights through digital watermarking. *Computer*, *29*(7), 101-103.
2. Croitoru, C., Luchian, H., Gheorghies, O., &Apetrei, A. (2002, September). A new genetic graph coloring heuristic. In *Computational Symposium on Graph Coloring and Generalizations COLOR* (Vol. 2).
3. Gu, J., Qu, G., & Zhou, Q. (2009, July). Information hiding for trusted system design. In *Proceedings of the 46th Annual Design Automation Conference* (pp. 698-701).
4. Pal, S. K., &Sarma, S. S. (2012). Graph coloring approach for hiding of information. *Procedia Technology*, *4*, 272-277.
5. Pal, S. K., & Chakraborty, N. (2017). Application of Cosmos's law of Merge and Split for Data Encryption. *International Journal of Computer Network and Information Security (IJCNIS)*, *9*(5), 11-20.
6. Pal, S. K., & Mishra, S. (2019). Revolutionary Change in Cryptography. *Invertis Journal of Renewable Energy*, *9*(2), 43-54.
7. Pal, S. K., Datta, B., & Karmakar, A. (2021). An ANN Approach of Twisted Fiestel Block Ciphering. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3* (pp. 47-56). Springer Singapore.
8. Pal, S. K., & Mishra, S. (2019). An TPM based approach for generation of secret key. *International Journal of Computer Network and Information Security*, *11*(10), 45-50.
9. Qu, G., & Potkonjak, M. (1998, November). Analysis of watermarking techniques for graph coloring problem. In *Proceedings of the 1998 IEEE/ACM international conference on Computer-aided design* (pp. 190-193).