International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 5, August 2014, PP 153-159
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Genesis of Graphic Ciphering Techniques- A Brief Survey

Debajit Sensarma[1], Samar Sen Sarma[2]

[1] Research Fellow, Department of Computer Science & Engineering, University of Calcutta, Kolkata, West Bengal, India

[2] Professor, Department of Computer Science & Engineering, University of Calcutta, Kolkata, West Bengal, India

Abstract: *Graph is an omnipotent mathematical tool. As graph can be encoded efficiently, it has many real life applications in several fields. This paper focused on the field related with computer science and engineering and gives a brief literature survey of the applications of graph in the areas like designing secure cryptographic protocol, reducing search space in combinatorial search problems (e.g. Graph search), increasing network security by anonymizing the network graph, steganography, software watermarking, fingerprinting, graph coding, IP protection schemes etc.*

Keywords: *Graph, Automorphism, Cryptography, Ad- hoc Network*

1. INTRODUCTION

Many real world problems can be formulated in terms of graph by taking it as a mathematical tool such that solving the later problem can give a suitable solution to the former one. For instance, the psychologist Lewin proposed that the 'life space' of a person can be modeled by a planar graph, in which the faces represent the different environments [1]. As observed by D.E. Knuth [2] graph theoretical terminology and graph theorist are numerically comparable at this time. The field graph theory started its journey from the problem of Koinsberg bridge in 1735 [3]. Graph algorithms can be treated as unified solution approach in many classical and modern application areas. We are concern about how we can design and adapt the art to various and numerous areas of real life industrial and engineering problems.

This paper gives a brief literature survey on some application areas of graph in section 2 and section 3 concludes the paper.

2. BRIEF LITERATURE SURVEY

We have studied some other algorithms of well known areas like designing secure cryptographic protocol, reducing search space in combinatorial search problems (e.g. Graph search), increasing network security by anonymizing the network graph, steganography, software watermarking, fingerprinting, IP protection schemes etc.

Though in the past cryptography has been exclusively the occupation of the military, it is only during the last forty years that the study and practice of cryptography has reached the wide public. Graph can be used in encryption and decryption [15]. Here the author has investigated the cryptographic properties of infinite families of simple graphs of large girth with the special coloring of vertices. In [16], authors uses graph as the encryption key. While studying various graph properties we came across an important property namely Graph Automorphism. An automorphism [36] of a graph is a form of symmetry in which graph mapped onto itself while preserving adjacency. The Automorphism problem is to testing whether a graph has a nontrivial automorphism or not. It belongs to the class NP of computational complexity. Similar to the graph isomorphism problem, it is unknown whether it has a polynomial time algorithm or it is NP-complete [39]. In [56] the concept is applied in designing secure cryptographic protocol. An encryption algorithm is computationally secure if it cannot be

intruded with the standard resources. We use the concept of Graph Automorphism to design a constraint based cryptographic protocol. It is a graph based modified secure classical Data Encryption Standard algorithm (GMDES) based on partial symmetric key. The algorithm is depended on 4-cube graph and 16 non-Automorphic Hamiltonian paths are used as the sub-keys of 16 rounds of modified Data Encryption Standard (DES) algorithm. The idea is based on a constraint satisfaction [4,5] formulation of the problem i.e. the nodes of 4-cube graph act as variables, the objective is to find 16 Hamiltonian paths by the permutation of nodes of the original 4-cube graph such that the constraint i.e. the permutation never produces the Automorphic graph is satisfied. Besides this here a secure key exchange protocol [55] is used which is based on two keys (partial key and secret key) and a secret table only known to sender and receiver. The algorithm provides integrity, authenticity and non repudiation when transferring the message and public key. The efficiency of proposed algorithm surpasses the classical Data Encryption Standard (DES) algorithm in general. Here zero-knowledge Protocol (ZKP) is used for authentication purpose. The advantages of this algorithm are (a) it is not fully depended on secret key and produces different cipher text by applying same key on the same plain text which can prevent various types of malicious attacks, (b) if intruder can identify the secret key then also due to the huge search space of the key it is practically not possible to decrypt the required cipher text, (c) it can prevent Replay Attack, Chosen Cipher text Attack, Cipher text only Attack, Chosen Plain text Attack, Brute force Attack, Man-in-the-middle Attack etc., (d) in this algorithm a secure mapping table is used which is encrypted with senders private key, so at the time of decryption only authenticated receiver can decrypt the required cipher text, (e) our algorithm requires less encryption time than classical DES algorithm but the decryption time is depends on the receiver.

In recent days, graph theoretic approach to steganography has become very popular [17]. Here, a graph is constructed from the cover data and the secret message and ultimately the steganographic embedding problem is reduced to the well known combinatorial problem of finding a maximum matching in graph. Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified. Graph theoretic approach can be used to design software watermark in robust fashion [18]. This method works with control/data flow graphs and uses abstractions, approximate k-partitions, and a random walk method to embed the watermark. Graph based IP protection schemes are also classical [19]. This scheme uses a generic graph corresponding to a digital system design and watermarking of the graph and its encryption are achieved using a new linear feedback shift register (LFSR)-based locking scheme. Various Constraint based techniques have been used in designing watermarking Intellectual Properties (IP), e.g. graph coloring based IP protection scheme [44], SAT based IP protection scheme [45] etc. In another point of view, there are some graph based algorithms that produces same watermarked graph with the different messages or signatures. This violates the uniqueness of the watermark [58].

Graph theoretic approach of software Fingerprinting are there [20] which is a form of watermarking in which an individualized mark is embedded into a copy of the media.

The Graph Anonymization problem can be stated as, given a graph G, asks for the k-degree anonymous graph that stems from G with the minimum number of graph modification operations It is a well problem [21] and the technique [22] applied for social network graphs can help in privacy preserving network publication.

Graph searching [42] becomes very popular in recent days. But often symmetries of graphs (often called graph automorphism) can complicate combinatorial searching algorithms. Such obstacles can often be removed by detecting and breaking symmetries early [23, 24]. Graph automorphism [36]has

many applications in the field of Graph Mining [25], Graph Reconstruction [26], Model checking [27], Bioinformatics [28], in the field of Chemistry [29] and design of fault-tolerant multiprocessor systems which is an important issue [30] etc. We study some optimization problems which are intractable in nature. Two-level logic minimization is a central problem in logic synthesis and it is an intractable problem [6]. There are many existing algorithms like Karnaugh map, Quine-McCluskey procedure [8, 9]. But most of them are suitable for few variables. Now-a-days various heuristic based procedures have been proposed like ESPRESSO-EXACT [10] and SCHERZO [11] to obtain practical solution. Besides this, there exists many graph based Boolean function minimization procedure, e.g. M. Nosrati et al.[12] proposed a heuristic algorithm to apply maximum minimization to Boolean functions with normal SOP form using graph data structure. In [46, 47, 48] heuristic algorithm for Boolean sum of product (SoP) function minimization is proposed by taking the advantages of implicit representation of the graphical data structure Binary Decision Diagram (BDD). A BDD is the compact and canonical representation of Boolean functions and with proper variable ordering the size of the BDD increases linearly with the number of variables. In this method, at first we tried to design a heuristic to minimize the number of disjoint cubes by proper reordering of the variables and minimizing number of 1-paths of BDD. But it does not necessarily give the minimum cover, so a minimal cover is constructed with the help of divide and conquer technique to produce a near optimal solution.

Finding QoS aware optimal route in Mobile ad hoc network (MANET) is very difficult due to dynamic topology, limited resources, and limited energy of nodes. S. Radhakrishnan et al. [13] proposed a distributed algorithm that adapts to the topology by utilizing spanning trees in the regions where the topology is stable, and resorting to an intelligent flooding-like approach in highly dynamic regions of the network. In [49, 50, 51, 52, 53, 54] author proposed some nature inspired swarm based intelligent QoS aware routing protocols for MANET and theoretically showed some improvements over the existing QoS aware routing protocols. Besides routing problem, security has become a challenging issue in MANET and thus many preventive approaches [14] have been designed to provide protected and authenticated communication between mobile nodes in an un-trusted environment.

Classical one-dimensional Bin Packing problem is a famous NP-Hard problem [31]. It states that, given a sequence $L = \{a_1, a_2 \ldots a_n\}$ of items, each with size a $s(a_i) \in (0,1]$ and the objective is to pack the items into minimum number of unit-capacity bins. Many approximate algorithms exits to cope with the problem [32]. It has many real-world applications [32, 33]. Graph can be used to model this type of problem [57].

The Degree-Constrained Minimum Spanning Tree (d-MST) problem attempts to find a minimum spanning tree with an added constraint that no nodes in the tree have a degree larger than a specified integer‘d’. It is known that computing the d-MST is NP-hard for every ‘d’ in the range $2 \leq d \leq (n-2)$, where n denotes the total number of nodes [34].It has many applications in constraint-based network design [35].

In Coding theory [37] point of view graph can be used to design linear block codes. The circuit matrix (or cut-set matrix) of a linear graph ‘G’ generates a binary linear code of distance ‘d’ and length n-an (n, d) code-where n is the number of branches in G and d is minimum number of branches in a circuit (or a cut-set) of G [40]. Such code is referred to as graph theoretic codes. The main problem in coding theory is to find good code (n, M, d) [n=total length of a code, M= efficiency, d=distance] that has small n (for fast transmission of messages), large M (to increase efficiency) and large d (to correct

many errors). This is an intractable problem [40 and it can be used to design secure cryptographic protocol, termed as code based cryptography [41], which is very useful in Post-quantum cryptography.

3. CONCLUSION

In this paper a brief survey on application of the mathematical tool graph is introduced. The problems considered here are usually intractable in nature and cannot be solved in finite amount of time and space.

In future we will try to reduce uncountable infinite time and storage space to countable infinite time and storage space to represent the problems in finite state machine and apply the algorithms in many real life problems solving that may help the human being using efficient ciphering of graph. We will study and explore more representative areas to establish our above goal.

ACKNOWLEDGEMENT

The authors would like to thank University Of Calcutta, West Bengal, India, Department of Science & Technology (DST), New Delhi, for financial support and the reviewers for their constructive and helpful comments and specially the Computer without which no work was possible.

REFERENCES

[1] LEWIN, K.: Principles of Topological Psycology. Mc-Graw-Hill, New York, 1936.

[2] Knuth D. E., The Art of Computer Programming, Vol. 4,Fascicle 0, "Introduction to combinatorial algorithmsand Boolean functions", Addison-Wesley PublishingCompany, 2008.

[3] Deo, N. (2004). "Graph theory with applications to engineering and computer science." PHI Learning Pvt. Ltd..

[4] Tsang, E. "Foundations of constraint satisfaction". London: Academic press, Vol. 289, 1993.

[5] Kumar, V. "Algorithms for constraint-satisfaction problems: A survey." AI magazine 13, no. 1 (1992): 32.

[6] Umans, C., Villa, T., Sangiovanni-vincentelli, A., "How Hard is Two-Level Logic Minimization: an Addendum to Garey& Johnson," Proceedings of International Workshop on Logic and Synthesis, Lake Arrowhead, California, June 2005, pp. 169-176.

[7] Quine, Willard V. "The problem of simplifying truth functions." American Mathematical Monthly (1952): 521-531.

[8] McCluskey, E.J., "Minimization of Boolean functions." Bell Syst.Tech. J.35(6), 1417–1444 (1956).

[9] Quine, W.V.O., "On cores and prime implicants of truth functions,"AmericanMath. Monthly, Vol. 66, pp. 755–760, 1959.

[10] Rudell, R.L., "Logic Synthesis for VLSI Design," PhD Thesis, UCB/ERL M89/49, 1989.

[11] Coudert, O., Madre, J.C. and Fraisse, H., "A new viewpoint on two-level logic minimization,"Proc. 30th DAC, Dallas, TX, USA, pp. 625–630, June 1993.

[12] Nosrati, M., and Hariri, M., "An Algorithm for Minimizing of Boolean Functions Based on Graph DS". World Applied Programming, 1(3), 209-214, 2011.

[13] Radhakrishnan, S., GopalRacherla, Chandra N. Sekharan, N. S. V. Rao, and Steven G. Batsell. "DST-a routing protocol for ad hoc networks using distributed spanning trees." In Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE, pp. 1543-1547. IEEE, 1999.

[14] Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks."IEEE communications surveys 7.4 (2005): 2-28.

[15] Ustimenko, V. "On Graph-Based Cryptography and Symbolic Computations."Serdica Journal of Computing 1, no. 2 (2007): 131-156.

[16] Gideon, S. "Denial cryptography based on graph theory", United States Patent number: 6823068, 2004.

[17] Hetzl, S., and Petra, M. "A graph–theoretic approach to steganography." In Communications and Multimedia Security, pp. 119-128. Springer Berlin Heidelberg, 2005.

[18] Venkatesan, R., Vazirani, V., and Sinha, S. "A graph theoretic approach to software watermarking." In Information Hiding, pp. 157-168. Springer Berlin Heidelberg, 2001.

[19] Halder, R., Dasgupta,P.,Naskar,S., and Sarma., S. S. "An Internet-based IP Protection Scheme for Circuit Designs using Linear Feedback Shift Register-based Locking."Engineering Letters 19, no. 2 (2011): 84.

[20] Collberg, Christian S., Thomborson, C. and Gregg M. Townsend. "Dynamic graph-based software fingerprinting." ACM Transactions on Programming Languages and Systems (TOPLAS) 29, no. 6 (2007): 35.

[21] Liu, K., and Terzi, E. "Towards identity anonymization on graphs." InProceedings of the 2008 ACM SIGMOD international conference on Management of data, pp. 93-106. ACM, 2008.

[22] Zou, L., Chen, L., &Özsu, M. T. "K-automorphism: A general framework for privacy preserving network publication." Proceedings of the VLDB Endowment, 2(1), 946-957, (2009).

[23] Albertson, Michael O., and Karen L. Collins. "Symmetry breaking in graphs." Electron. J. Combin 3, no. 1 (1996): R18.

[24] Harary, F. R. A. N. K. "Methods of destroying the symmetries of a graph." Bull. Malasyan Math. Sc. Soc 24, no. 2 (2001): 183-191.

[25] Zampelli, S., Deville, Y., andDupont, P. "Symmetry breaking in subgraph pattern matching." Symmetry and Constraint Satisfaction Problems(2006): 31.

[26] Hartke, S. G., Kolb, H., Nishikawa, J., andStolee, D. "Automorphism groups of a graph and a vertex-deleted subgraph." the electronic journal of combinatorics 17, no. R134 (2010): 1.

[27] Zhang, S. J., Sun, J., Sun, C., Liu, Y., Ma, J., & Dong, J. S.,"Symmetry Detection for Model Checking.", 2013.

[28] Jothi, R., Kann, M. G., andPrzytycka, T. M.."Predicting protein–protein interaction by searching evolutionary tree automorphism space." Bioinformatics 21.suppl 1 (2005): i241-i250.

[29] Bohanec, S., and Perdih, M. "Symmetry of chemical structures: A novel method of graph automorphism group determination." Journal of chemical information and computer sciences 33.5 (1993): 719-726.

[30] Dutt,S. and Hayes,J.P. "Designing fault-tolerant systems using automorphisms." Journal of Parallel and Distr. Computing, July 1991, pp. 249-268.

[31] Garey, Michael R., and David S. Johnson. "Computers and intractability". Vol. 174. San Francisco: freeman, 1979.

[32] Coffman Jr, E. C., Garey, M. R., and Johnson, D. S. "Approximation algorithms for bin packing: A survey." In Approximation algorithms for NP-hard problems, pp. 46-93. PWS Publishing Co., 1996.

[33] Bansal, N., Liu, Z., &Sankar, A. "Bin-packing with fragile objects and frequency allocation in cellular networks."Wireless Networks 15, no. 6 (2009): 821-830.

[34] Celso C. Ribeiro , Maurício C. Souza , C. Souza, "Variable Neighborhood Search For The Degree-Constrained Minimum Spanning Tree Problem." Journal Discrete Applied Mathematics - Special issue: Third ALIO-EURO meeting on applied combinatorial optimization, Volume 118, Issue 1-2, 15 April 2002.

[35] Liang, C. K., Huang, Y. J., and Lin, J. D. "An energy efficient routing scheme in wireless sensor networks." In Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on, pp. 916-921. IEEE, 2008.

[36] Biggs, N."Finite groups of automorphisms." course given at the University of Southampton, October-December 1969. Vol. 6. CUP Archive, 1971.

[37] Hamming, R. W.,"Coding and information theory." Prentice-Hall, Inc., 1986.

[38] Basu, S. K., "Design methods and analysis of algorithms." PHI Learning Pvt. Ltd., 2013.

[39] Agrawal, M., andArvind, V.,"A note on decision versus search for graph automorphism."Information and computation, 131(2), 1996, 179-189.

[40] Hakimi, S. L., &Bredeson, J. G.,"Graph theoretic error-correcting codes."IEEE Transactions on Information Theory, 14(4), 1968, 584-591.

[41] Overbeck, R., &Sendrier, N.,"Code-based cryptography." In Post-quantum cryptography (pp. 95-145). Springer Berlin Heidelberg, 2009.

[42] Mears, C., De La Banda, M. G., & Wallace, M.,"On implementing symmetry detection." Constraints, 14(4), 2009, 443-477.

[43] Jiang, H., Wang, H., Yu, P. S., & Zhou, S.," Gstring: A novel approach for efficient search in graph databases." In Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on (pp. 566-575). IEEE, (2007, April).

[44] Qu, G., &Potkonjak, M.,"Hiding signatures in graph coloring solutions." In Information Hiding (pp. 348-367). Springer Berlin Heidelberg, (2000, January).

[45] Kahng, A. B., Lach, J., Mangione-Smith, W. H., Mantik, S., Markov, I. L., Potkonjak, M., & Wolfe, G., "Constraint-based watermarking techniques for design IP protection."Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 20(10), 1236-1252, 2001.

[46] Sensarma, D., Basuli, K, and Sarma, S. S. "How to cope with an Intractable Problem", Lambert Academic Publishing GmbH & Co. KG, Germany, ISBN: 978-3-659-43739-7, 2013.

[47] Sensarma, D., Banerjee, S., Basuli, K., Naskar, S., &Sarma, S. S. "On an optimization technique using Binary Decision Diagram", International Journal of Computer Science, Engineering and Applications (IJCSEA), Volume 2, Number 1,73-86,February 2012.

[48] Sensarma, D., Banerjee, S., Basuli, K., Naskar, S., &Sarma, S. S. "Minimizing Boolean Sum of Products Functions Using Binary Decision Diagram", The Second International Conference on Computer Science and Information Technology ,Vol. 86, Part III, pp 36-48, Proceedings of CCSIT- 2012,Springer,2012.

[49] Sensarma, D., &Majumder, K. "A Comparative Analysis of the Ant Based Systems for QoS Routing in MANET." In Recent Trends in Computer Networks and Distributed Systems Security (pp. 485-496). Springer Berlin Heidelberg, 2012.

[50] Sensarma, D., andMajumder, K. "AMTR: The ANT Based QOS Aware Multipath Temporally Ordered Routing Algorithm for MANETs", AISC- 2013, CS & IT-CSCP 2013, pp. 389–396, 2014.

[51] Sensarma, D., andMajumder, K. "An efficient ant based qos aware intelligent temporally ordered routing algorithm for manets." International Journal of Computer Networks & Communications (IJCNC), Vol. 5, No. 4, PP.189-203, Jul. 2013.

[52] Sensarma, D., and Majumder, K. "HAQR: The Hierarchical ANT based QOS aware On-demandRoutingfor MANETS." WimoA- 2013,CS & IT-CSCP 2013, pp.193-202, 2013.

[53] Sensarma, D., andMajumder, K. "A Novel Hierarchical Ant Based QoS aware Intelligent Routing Scheme for MANETs." International Journal of Computer Networks & Communications (IJCNC), Vol. 5, No. 6, PP.215-229, Nov. 2013.

[54] Sensarma, D., andMajumder, K. "IWDRA: An Intelligent Water Drop Based QoS-Aware Routing Algorithm for MANETs." Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. Springer International Publishing, 2014.

[55] Sensarma, D., Banerjee, S., and Basuli, K. "A New Scheme for Key Exchange." International Journal of Modern Engineering Research (IJMER), 2(3), 2012.

[56] Sensarma, D., and Sarma, S. S. "GMDES: A GRAPH BASED MODIFIED DATA ENCRYPTION STANDARD ALGORITHM WITH ENHANCED SECURITY."International Journal of Research in Engineering and Technology, eISSN: 2319-1163,Vol. 3, Issue. 3, PP. 653-660, Mar-2014.

[57] Jansen, K., & Öhring, S. (1997). Approximation algorithms for time constrained scheduling. Information and Computation, 132(2), 85-108.

[58] Zhu, W., & Thomborson, C. (2006). Algorithms to watermark software through register allocation. In Digital Rights Management. Technologies, Issues, Challenges and Systems (pp. 180-191). Springer Berlin Heidelberg

AUTHOR'S BIOGRAPHY

Debajit Sensarma is presently pursuing his PhD degree from the department of Computer Science and Engineering, University of Calcutta, Kolkata, India with DST INSPIRE Fellowship. He has published several papers in International journals and conferences.

Dr. Samar Sen Sarma is presently working as the Professor of the department of Computer Science and Engineering, University of Calcutta, Kolkata, India. He has published several papers in International journals and conferences.