APPLICATIONS OF PLANAR GRAPH IN CRYPTOGRAPHY

Smt. Sarwar Sultana
Assistant Professor of Mathematics
Government Women's First Grade College Jewargi Colony.,Kalaburagi.

Abstract

A small perfect weighted planar graph with corresponding string is defined for different length of words. A secret code of planar graph with respect to regions is proposed. In this paper the perfect weighted planar graph is the public key while regions and different aspects of planar graphs are used to generate secret key.

Key Words and Phrases: Perfect weighted planar graph, secret code.

Graphs

Graph theory has become a very important component in many applications in the computing fields including cryptography and networking

A graph G is an ordered pair (V (G), E (G)) where i) V(G) is a non-empty finite set of elements, known as vertices. V (G) is known as vertex set. ii) E(G) is a family of unordered pairs (not necessarily distinct) of elements of V, known as edges of G. E(G) is known as Edge set. [2] Let G be a connected graph. An edge e of G is said to be a bridge or an isthmus if subgraph G – e is a disconnected graph. Every edge of a tree is an isthmus. An edge of a connected graph is an isthmus if and only if e does not lie on any cycle of G. [7] Let G be a connected graph. A set of edges S of G, whose removal from G disconnects graph G, is called a disconnecting set of G. A cut set of a connected graph G is defined as a minimal disconnecting set i. e. no proper subset of a disconnecting set is a disconnecting set of graph. Let G be a connected graph. The number of edges in a smallest cut set of G is called the edge connectivity of G and it is denoted by λ(G). Thus λ(G) is the smallest number of edges of connected graph G whose removal disconnects G. Let G be a connected graph. A vertex v in V (G) is said to be a cut vertex or cut node or articulation point of graph G if subgraph G – v is a disconnected graph. If v is a cut vertex of G then subgraph G – v has two or more components. [7]

Planar Graphs

A graph G is a planar graph if it is possible to represent it in the plane such that no two edges of the graph intersect except possibly at a vertex to which they are both incident. Any such drawing of planar graph G in a plane is a planar embedding of G.[1], [7]

Coloring of Graphs

The coloring of all vertices of a connected graph G such that ad-jacent vertices have different colors, is called a proper coloring or vertex coloring or simply a coloring of G. A graph G is said to be properly colored graph if each vertex of G is colored according to a proper coloring. The chromatic number of a graph G is denoted by χ(G) and

defined as the minimum number of colors required to color the vertices of G so that adjacent vertices get different colors. If graph G is k- chromatic graph then $\chi(G) = k$.

*Isomorphic Graphs

Two Planar Graphs are said to be *isomorphic graphs if their geo- metric duals are isomorphic. Every graph is * isomorphic to itself. If H and K are *isomorphic to K and P, respectively, then H and P are * isomorphic. Thus, *isomorphism is an equivalence relation. [2]

HB Graphs

A region of planar graph G is said to be pivot region of G if it is adjacent to all remaining regions of G. The number of pivot regions of planar graph is called the pivot region number of that graph. It is denoted by PRN (G). A planar graph G having non zero PRN is called HB graph.[3]

The Geometric Number of Graphs

Let Gn be a simple planar connected graph with n vertices. The non-zero integer m is called the geometric number of graph Gn if there exist at least one graph with m number of edges, whose geometric dual is a simple graph. [4] The smallest non-zero integer m is called the first geometric number of graph Gn if there is at least one graph with m number of edges whose geometric dual is a simple graph. It is denoted by F (Gn). A selective encryption mechanism is defined by using spanning tree concept of graph theory. Graph coloring is used for network security and coding. Geometric dual of graphs plays an important role for the encryption and decryption of the secret message. [6]

Region Set of Planar Graph

Let G be a planar graph. The set of all boundary edges and vertices of a region R with proper order is called the region set of that region. Thus the planar graph is the set of all its region sets.

Perfect Weighted Graphs

A weighted graph is a graph in which each edge is assigned a nu- merical weight. A graph G is said to be perfect weighted graph if a number (weight) is associated to each edge and vertex of G. A per- fect weighted graph which is planar is called the perfect weighted planar graph.

String of a Region

An alternating sequence of edges or vertices of a planar graph ac- cording to some rule without repetitions which encloses region is called a string of that region. The number of edges and vertices of a string is called its length. Consider the following rules to write the string of a region.

1. A string of length one is denoted by a single vertex.
2. If the length of a string is an even, then it starts with the vertex and ends with an edge.
3. If the length of a string is an odd then it starts and ends with an edge.
4. If a pendent edge is present in the region then start a string with the pendent edge but do not take the pendent vertex in the string.
5. If the pendent edge is absent in the region then start string with the vertex with dark circle.

We use clockwise orientation to write string of a region. Consider the following table which gives the length of words, strings and the corresponding graph representations.[Table1]

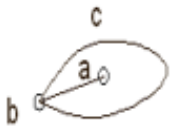
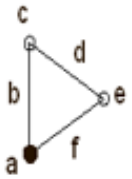
Sr. No.	Length of word	String	Graph Representation
1	1	a	
2	2	ab	
3	3	abc	
4	4	abcd	
5	5	abcde	
6	6	abcdef	

Table 1: Strings and Corresponding Graphs

Similarly we can generate string and the corresponding graph for word of any length.

Encryption Algorithm

Let H be a perfect weighted planar graph. Let S be the message to be encrypted. $|S|$ = Number of words in S. Let $|S| = \alpha$ Consider the following steps.

Step1: Choose a planar graph H with α number of regions. **Step2:** According to your secret message, generate a sequence of words by using regions say R_1, R_2, R_3, . . . $R\alpha$

Step3: Assign proper weights to the edges and vertices of H according to your message.

Step4: Add some new vertices and edges to graph H with arbitrary weights without disturbing required regions and denote it as G. **Step5:** Send the new weighted graph G (or any graph which is *isomorphic to G) to the receiver, which is the public key.

Step6: Send the secret code to receiver which will be the private key

Generation of Secret Code

The following methods are used to generate secret code.

Method I: Write secret code in three components as (α, R, β), where $\alpha = |S|$ = Number of words in the secret message = $|R|$. R is the set of regions to be used for the generation of Secret code. That is, if we want to select regions R_4,R_2,R_3,R_1, then we write it as 4+β, 2+β, 3+β, 1+β, where β is any number. For β= 2, R will become 6,4,5,3. Thus, the secret code will become (4, 6, 4, 5, 3, 2). In particular, the secret code (5, 6, 5, 3, 2, 4, 1) represents message with 5 words and words are formed by using regions 6-1=5, 5-1=4, 3-1=2, 2-1=1, 4-1=3 i. e. R_5,R_4, R_2, R_1, R_3.

Method II: Use binary number system to write secret code in method I.

Method III: Use β = Pivot Region Number of a graph=PRN(G).

Method IV: Use β = Chromatic number of a graph.

Method V: Use β = The First Geometric Number of a graph. **Method VI:** Use β = The Greatest Geometric Number of a graph. **Method VII:** Use β = The Rank of a graph.

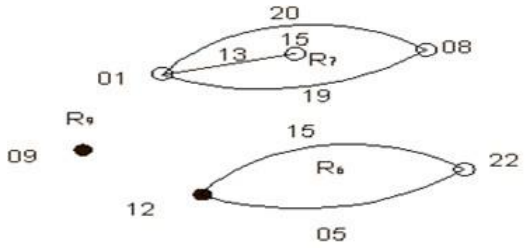


Figure 1: Original graph H

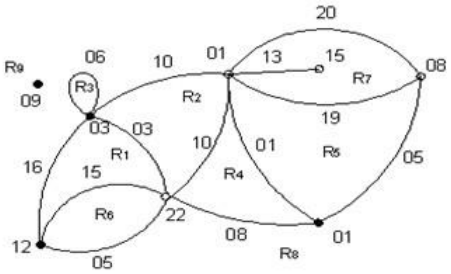


Figure 2: Public key graph G

Consider the example which explains above algorithm in detail. Let S: I LOVE MATHS, be the secret message. Therefore, S =3=α

I L O V E M A T H S

09 12 15 22 05 13 01 20 08 19

The required graph of S is as shown in figure 1 and 2.

Now, add some dummy vertices and edges with the arbitrary weights to the original graph and denote it as graph G.We can use any planar graph G whose subgraph is *isomorphic to original graph H.

Here, α = 3, R = (9 6 7). Let β = -1. So the secret code is(α, R, β) =(3, 8, 5,6,-1). Hence send G and secret code to the receiver. Fordecrypting the message, we reverse the above procedure. We have8 + 1 = 9, 5 + 1 = 6, 6 + 1 = 7. So actual R is 9 6 7. Therefore, use three regions R_9, R_6, R_7 without disturbing sequence. R_9: 09 : I; R_6: 12 15 22 05 : L O V E; R_7: 13 01 20 08 19 : M A T H S. Hence the decrypted message is “I LOVE MATHS”

Conclusion

The region sequence can be selected by any order. If planar graph G has R regions and the message to be encrypted is of length α then the number of possible permutations for the selection of regions is ${}^{R}P\alpha$ Without the meaning of three parameters α, R, β, no one can decrypt the message. For decryption one htry so many permutations. There are so many graphs available in the universe, so it is very difficult to find the correct graph. Hence the proposed method is very safe for cryptography.

References

1. F. R. K. Chung and L. Lu, Complex Graphs and Networks, CBMS Regional Conference Series in Mathematics, American Mathematical society, volume 107, (2006).

2. H.R. Bhapkar and J. N. Salunke, *isomorphism of graphs, In- ternational Journal of Mathematical Sciences and Engineering Applications, Vol. 8, No. II, 0973-9424, (2014), 225-235.

3. H. R. Bhapkar and J. N. Salunke, The Geometric Dual of HB Graph, *outerplanar Graph and Related

Aspects, Bulletin of Mathematical Sciences and Applications, ISSN 2278-9634, Vol- ume 3, No. 3, pp 114-119, (2014), 114-119.

4. H. R. Bhapkar and J. N. Salunke, Geometric Number of Planar Graphs and Related Aspects, International Journal of Innova- tive Research in Science, Engineering and Technology, ISSN: 2319-8753, (2016), 1111-1117.

5. J. A. Bondy and U. S. R. Murty, "Graph Theory with Appli- cations". Elsevier, MaccMillan, New York - London, 1976.

6. Menezes A., Oorschut, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

7. Narsingh Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice –Hall of India,2003.