Chapter 15
Hiding Message in Map along Pre–Hamiltonian Path

Sunil Kumar Muttoo
University of Delhi, India

Vinay Kumar
National Informatics Centre, India

ABSTRACT

In this paper, an algorithm to embed information in a map along Hamiltonian path is presented. A file based data structure in which a graph is treated as a composition of three components, node, segment and intermediate points that constitute a segment, is used to store a graph. In a map with N nodes, each node can represent \( \lceil \log_2 N \rceil \) bits from message bit strings. Any bits (\( \geq 0 \)) from message between bit strings represented by adjacent nodes are embedded in a segment. In the case of a multi graph, a segment is selected based on the last two bits in the nodes. A pre Hamiltonian path is determined in the map starting from node represented by the first \( \lceil \log_2 N \rceil \) bits from message string to the last bit string \( \lceil \log_2 N \rceil \). The method is tested on different maps and messages of different sizes and robust results have been observed. Retrieval is based on the key \((S, |m|, \sum)\) and traversing along the pre Hamiltonian path starting from node S.

1. INTRODUCTION

The steganographic algorithm introduced in this paper uses a planar graph (Berge, 1962) as cover object. A planar graph is also called a map. Normal data structure used to represent a graph does not provide enough redundancy for hiding.

Before discussing the details, background of the approach, motivation behind the paper and the contribution that this paper can provide to the computing world need to be discussed.

1.1 Background

Steganography is the art of hiding a secret message inside a cover (host) object. The purpose is to
allow two parties to communicate surreptitiously, without raising suspicion from an eavesdropper. Steganography (Katzenbeisser & Petitcolas, 2000) and cryptography (Stallings, 1999) are two techniques used for secret communication. Cryptography attempts to hide the contents of a message while steganography attempts to hide the existence of a message (Anderson & Petitcolas, 1998). A digital cover object may be an image, audio, video or a graph – a vector data. The cover object with embedded secret message is called stego object i.e. 

\[ \text{cover} + \text{secret message} = \text{stego} \]

Stego object is the medium that carries the secret message (hidden data). Main requirement for any steganographic technique is undetectability, robustness, tamper resistance and embedding capacity (Cole, 2003; Johnson & Jajodia, 1998a). These properties of any steganographic algorithm are mainly influenced by following four factors:

- The choice of the cover object,
- The selection rule used to identify individual elements of the cover that could be modified (or used without any modification) during embedding,
- The type of embedding operations that modifies the cover elements, and
- The number of embedding changes.

The embedding capacity and robustness in steganographic algorithm are so diagonally opposite placed that it is difficult to achieve both simultaneously at the maximum level (Salomon, 2003; Kumar & Muttoo, 2008, 2009b). Thus, a steganographic algorithm achieves robustness at low embedding capacity. The placement of embedding changes in the cover is called a selection channel. A channel is kept secret by the communicating partners in the similar way a secret key is maintained in cryptography. After embedding, stego medium should maintain similarity with cover to avoid any detection of the hidden data. It is achieved by minimizing the distortion in the cover medium while embedding the hidden data (Anderson & Petitcolas, 1998).

The way a cover is stored in digital form plays an important role in minimizing distortion introduced in cover while embedding secret message. A cover is collection of some basic elements. Basic element in image is pixel while that in a graph is node and segment. A segment consists of many intermediate points (Kumar & Muttoo, in press). More is the amount of bits available to store one element of a cover medium, less is the visible distortion after embedding and vice versa.

1.2 Motivation

Today map is used for various purposes e.g. routing, tourism, online tracking of vehicle movement etc. It is freely exchanged using electronic communication devices like PDA and GPS. Using more generic cover for hiding relevant but secret message raises less or no suspicion at all. Moreover, with emergence of Geographic Information System (GIS), many countries have either developed their national spatial database or are in process of developing it. Out of the two main approaches: vector and raster, vector form takes less number of bits to store the same amount of spatial features (Kumar & Muttoo, 2006; Hetzl & Mutzel, 2005). This makes a vector form of spatial data more suitable for transmission and therefore it can be used to hide information at store as well as to hide information while transmitting data using public network that includes both wired and wireless.

Further according to Kerckhoff’s principle, the security of a hidden message must depend on keeping the stego key secret. It must not depend on keeping the steganographic algorithm secret (Cox et al., 2005, 2007). Further, if a particular type of cover is in use for longer period, it is easy for steganalyst to develop a tool to defeat the process. A GIS based vector covers i.e. map or