MIS Review Vol. 17, No. 1, September (2011), pp. 19-37

A Graph Theoretic Approach to Sustainable Steganography

Vinay Kumar[1], Sunil Kumar Muttoo[2]

[1]*Scientist 'E,' National Informatics Center, MoCIT, Government of India.*

[2]*Department of Computer Science, University of Delhi*

ABSTRACT: *An algorithm based on graph-theoretic approach is introduced in this paper. A bipartite graph is created from message and cover object. Message M is broken into units of x (= 2, 4, or 8) bits long. For each x, a matching with m number of such x bits from cover file is determined using the bipartite graph. Wherever a matching for a node in left side is found with a node in right side then this part of the message is treated as either naturally or cross embedded in that port of the cover. Nodes in left side correspond to bits in message and those in right side correspond to group of bits in cover. The matching relationship is then embedded in the extra bytes of cover, fully utilizing the available redundancy or alternatively the sequence of indices is compressed and sent through separate channel. The algorithm achieves almost 100% matching for message elements in cover elements. The embedding algorithm has been put through mathematical and statistical test to ensure that it not only retains visual similarity in stego with cover file but also leaves other statistics of cover undistorted after embedding. Therefore it achieves sustainability. In this paper, we have taken BMP file to implement the algorithm.*

KEYWORDS: *Extra Bytes, Graph Theoretic Approach, Steganography, Information Hiding, Sustainable Embedding, Natural Embedding, Partial Embedding, Cross Embedding, Explicit Embedding.*

1. Introduction

Steganography, also called "covered writing" is defined as the art and science of communicating in a way that hides the very existence of the communication. Steganography and Cryptography are excellent means to achieve privacy and secrecy of information to be shared between communicating partners. A mechanism to combine them provides multiple layers of security. Statistical and visual undetectability of a stego object when compared with cover object is an important consideration for any steganographic schemes. By undetectability, we understand the inability of an attacker to distinguish between stego and cover objects with success rate better than random guessing, given the knowledge of embedding algorithm and the source of cover media.

There are a number of steganographic approaches in use for hiding information in digital images. The spatial domain, frequency domain and spread spectrum technique are mostly used for information hiding (Anonymous, 1995; Sellars, 2006). The simple