Microsoft Power Point Files: A Secure Steganographic Carrier

Rajesh Kumar Tiwari, RVS College of Engineering & Technology, India
G. Sahoo, Birla Institute of Technology (BIT) Mesra, India

ABSTRACT

One of the major characteristic of cryptography and steganography is unlimited and limited secret data conversion and embedding respectively. In steganography, concealing unlimited secret data in cover media is unfeasible. Majority of researchers have taken image, text, html, executable files as a steganographic cover media. In this proposed work the authors have considered Microsoft Power Point Files as a cover medium. The authors have developed a methodology which consist two techniques for embedding the valuable unlimited data with three layers of security and high robustness. The resultant stego file undoubtedly can be transmitted any where using any channel. Experimental results show the feasibility of the proposed methodology.

Keywords: Appending, Data Hiding, Encryption, Information Security, Microsoft Power Point File, Rubbish Space, Steganography

INTRODUCTION

The digital information revaluation has brought important changes in our society and our life. Many advantage of digital information have generated new opportunities for innovation. Along with powerful software, new devices, such as digital camera, high quality printer and scanner, digital voice recorder, audio player etc. have reached consumer worldwide to create, manipulate and enjoy digital data. With the ease of editing of the digital data and also perfect reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of digital data have raised serious concern. The common approach is to convert the digital data in different form so that the resultant data can be understood only by those who can get it back into its original form. This technique is known as encryption. A major drawback of this method is that the existence of data is not hidden. Giving enough time the unreadable encrypted data can be obtained in its original form.

As a part of solution to this kind of problems, the concept of steganography has considerably given much attention in recent years. The word steganography is a Greek word giving a meaning to it as ‘writing in hiding’. The main goal of steganography is to communicate message securely in a complete undetectable manner (Allan, 2001; Amin, Salleh, Ibrahim, Katmin, & Shamsuddin, 2003; Bender, Gruhl, Morimoto, & Lu, 1996; Dunbar, 2002; Castiglione, De Santis, & Soriante, 2007). It has been emerged as a skill of concealing private information.
inside a carrier that can be considered for all intents and ideas (Zou & Shi, 2005; Artz, 2001; Gutub, Al-Qahtani, & Tabakh, 2009; Johnson & Jajodia, 1998). Digital technology gives us a new way to relate steganographic techniques including hiding information in digital medias. It not only goes well beyond simply by embedding a text in an image, but also pertains to other media, including voice, text, binary files and communication channels (Swanson, Zhu, & Tewfik, 1996; Petitcolas, Anderson, & Kuhn, 1999; Anderson & Petitcolas, 1998).

It can be mentioned here that steganography, in respect to constructive approach, generally provides vast potential security and legal data hiding. As far as corporate sectors are concerned, if they cannot hide their important information, this may lead to damage extremely the company’s profitability as well as its sustainability. Again, as a destructive approach, even if steganography is not a threat in general, it may have some bad impacts on the areas where one wants to deal with some kind of unwanted illegal matters (Shejul & Kulkarni, 2010; Sahoo & Tiwari, 2008; Sutaone & Khandare, 2008; Liu & Tsai, 2007; Yan & Ping, 2009).

LITERATURE REVIEW

Embedding secret information in text file can be a challenging task. This is because text files have small amount of redundant data that is to be replaced with a secret message. Another drawback is the easy alteration of characters which can be done by unwanted parties. There are some methods by which we can accomplish text based steganography. These methods are:

- Open Space Method
- Syntactic Method
- Semantic Method

There are numerous ways to employ the open space in text files to encode the information. The methods employing open spaces work because a casual reader may avoid one extra space at the end of the line and an extra space between two words does not prompt abnormally. The extra space can be used to conceal one bit either 0 or 1. However, inter-sentence space method encodes a “0” by adding a single space after a period in English prose. Adding two spaces would encode a “1”. The left-shift encoding involves actually shifting each line of text vertically up or down by as little 3 centimeters. The End-of-line space method exploits white space at the end of each line.

Syntactic methods exploit the use of punctuation and structure of text to hide data without scientifically altering the meaning of the message. For example the two phrases “bread, butter, and milk” and “bread, butter and milk” are grammatically correct but differ in the use of comma. One can use this structure alternatively in a text message to represent either a “1” or “0”. Semantic methods assign two synonyms a primary or a secondary value. These values are then translated into binary “1” or “0”. For example, the word “big” is assigned primary and the “large” is assigned secondary. Therefore, decoding a message would translate the use of primary to a “1” and secondary to a “0”. The main hurdle is that replacement of the synonyms may change the meaning of the structure of the sentence.

Artz (2001) has designed a methodology for hiding the secret data by changing the order of characters or words. Ordering data that does not have an ordering constraint is often an effective method of steganography. Each permutation of a set of characters or words can be mapped to a positive integer. This mapping can then be used to encode hidden data by altering the order of characters or words.

Shejul and Kulkarni (2010) introduced steganography method based on biometrics with skin tone region of images. Secret data is embedded within skin region of image that provided an excellent secure location for data hiding. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding...
Cybercrimes Technologies and Approaches

[www.igi-global.com/chapter/cybercrimes-technologies-and-approaches/115758?camid=4v1a](www.igi-global.com/chapter/cybercrimes-technologies-and-approaches/115758?camid=4v1a)