Secured Communication using Steganography Framework with Sample RTF Implementation

Vijayaratnam Ganeshkumar[1], Assoc. Prof. Ravindra L. W. Koggalage[2]
[1]*Department of Computing, Informatics Institute of Technology, Sri Lanka*
Chief Technology Officer, The Associated Newspapers of Ceylon Limited, Sri Lanka
gvijayaratnam@bcs.org[1], koggalage@yahoo.com [2]

***Abstract* –It is important to have secured communication channels as we often need to share our secret information. Encryption is one of the widely used techniques to ensure secure communication, however, sending encrypted messages often draw eavesdropper's attention to intercept the messages and reveal the original message. The concept of steganography focuses on embedding secret information into the digital media such as images, audio, video files and even in text documents, without drawing any attention of eavesdropper to think that such information is embedded. In this paper, a novel approach is proposed in information hiding, by using a common framework that will generate the digital stegano medium. As a proof of concept, we propose a module that will support this framework, using inter-character spacing and an optimized approach for message compression by custom bit encoding on RTF documents (Rich Text Format). Level of security is further enhanced by supporting encryption and diffusion, before applying the Steganography.**

Key words: Steganography, Encryption, Security

I INTRODUCTION

Internet has evolved so fast in last few years and has become an essential part of our day to day life. However, irrespective of whether the user is an absolute beginner or an expert in IT, everyone has a concern in security over internet. So, we might have questions in mind such as "Is my data which I send over the internet is secured?" or "The information which I send is received only by the recipient who is intended to receive?" If we try to find out the answers for such questions, we will get to know the importance of data security.

Various methods like encryption, cryptography including steganography are used to send secret messages. Steganography is an art of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes that there is a hidden message [1]. This is a distinguish advantage between steganography and other methods. For an example, in the case of encryption, eavesdropper is aware of the existence of secret message by observing the encrypted message. This will always draw attention of eavesdropper to break the encryption and try to reveal the secret message. To avoid this problem we need a technique that will not draw any attention of an eavesdropper and at the same time, the secret message must also be transmitted to the recipient. This is the exact idea behind the concept of Steganography.

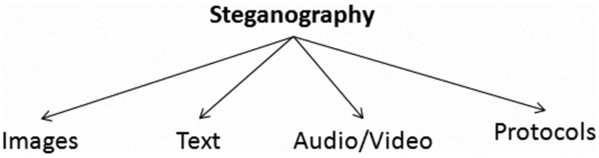

Fig. 1 Categories of steganography

The word *steganography* is a Greek origin and meaning "*covered or hidden writing*". *Demaratus* (The king of *Sparata* from 515 until 491 BC) sent a warning message about the forthcoming attack to Greece by writing it on wooden panel and covered in wax [1], and this believed to be where the steganography had started. Time to time steganography has evolved and nowadays it is mostly performed on images, multimedia files, text, word and PDF files. According to recent researches, they have proved that steganography can be performed on H.264 video sequence [4], power point files [3] and stego-digital-signals [2][5]. If we look deeper in steganography, it's very hard for an end-user who is not familiar with Steganography concepts to generate a stegano message using normal programming techniques. Not only that, but also it is still difficult to find an easy to use Steganography method.

II ADDRESSED PROBELM

In this paper we address the issue that need of a common Steganography Framework that can be easily used by any user. For an end-user, how a stego cover medium generated is not that important and what really desired is an application or framework that would generate stego message with minimum effort. It also should provide facilities such as flexibility, ease of use and high security.

This paper presents a layered architecture for a Steganography Framework supported by pluggable modules. As a proof of concept we have developed a

978-1-4244-4837-1/09/$25.00 ©2009 IEEE