A Language Independent Algorithm to Send Secret Messages using Steganography

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

***Abstract* – The radical growth of internet & cybercrime during the last few years has forced us to think about how to improve information security efficiently during communication. Protecting the information during communication via the internet is the major challenge against eavesdropper. Encryption is a widely used technique to ensure secure communication; however, sending encrypted messages often draws an eavesdropper's attention. Steganography is a method of writing secret messages in a way that nobody, except for the sender and the recipient, suspects the existence of a hidden message. In this paper a new steganographic technique is proposed to transmit concealed messages in multi-language or combination of languages, which can be represented in Unicode. Use of inter-character spacing technique is proposed as the steganographic technique and a prototype implementation has been done with Rich Text Format (RTF) documents. An additional optimized compression technique is also proposed with enhanced user defined codes, to support Unicode language. Another advantage is that the secret message (hidden) can be in a different language than which is transmitted through the communication channel.**

Key words: Steganography, Encryption, Security, Unicode

I INTRODUCTION

Over the last few years, the usage of the internet has radically increased from an absolute beginner to an expert. Not only has the internet has become an essential part of our daily life, but also been a reason for the increase of in cybercrime and cyber terrorism. Consequently, users have raised the level of anxiety in information security on their communication. The common question that any computer user would raise is 'how secret message communication can be made securely over the internet?' Answering the question will clarify the importance of information security.

Cryptography is accepted by most experts as a secure method in sending information. However it has its own inherited weaknesses; such as the eavesdropper can easily suspect that important information is encrypted and transmitted; hence the eavesdropper may try cryptanalysis technique to reveal the original message. As a solution to this weakness, there is a need for a technique that will not draw any attention of an eavesdropper and at the same time, the secret message must also transmit to the receiver securely. 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]. The main advantage of steganography when compared to cryptography is that the third party would not suspect that there is a hidden secret message, as it may not draw their attention. While cryptography is about protecting the content of messages, steganography is about concealing their very existence [1]. This is the exact idea behind the concept of Steganography.

The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos (στεγανός) meaning "covered or protected", and graphein (γράφειν) meaning "to write". The first recorded use of the term was in 1499 by *Johannes Trithemius* in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic [2]. The first recorded uses of steganography can be traced back to 440 BC, when Herodotus mentions two examples of steganography in *The Histories of Herodotus. Demaratus* sent a warning about a forthcoming attack to Greece by writing it on the wooden backing of a wax tablet before applying beeswax on its surface [1], and this is believed to be where steganography had started. From the day it started, steganography is performed on images, multimedia files, and text, word and PDF files. Time to time steganography techniques have evolved, and modern techniques are performed on H.264 video sequence [3], power-point files [4] and stego-digital-signals [5]. As a practice, when a message is entered, usually one language is used, because of this reason most of the steganography algorithms are languages dependent. Researcher *Natthawut Samphaiboon* has proposed a steganography method for Thai text [6], *Mohammad Shirali-Shahreza* proposed a method for Persian/Arabic Unicode text [7] and *Changder* presents new techniques for Hindi language [8].

II PROBLEM ADDRESSED

According to the previous researches in steganography techniques, each of them provides a language dependent algorithm, so that they cannot be used to send multi language messages. In this paper a language independent steganographic algorithm is proposed, to facilitate multi Unicode language support.

2010 International Conference on Advances in ICT for Emerging Regions (ICTer)
978-1-4244-9042-4/10/$26.00 ©2010 IEEE