

# **SREENIDHI INSTITUTE OF SCIENCE & TECHNOLOGY**

**(AUTONOMOUS)**

**(Affiliated to JNT University Hyderabad, Hyderabad and approved by AICTE- New Delhi)**

**Yamnampet, Ghatkesar, R.R district, Hyderabad – 501301**

**TECHNICAL SEMINAR REPORT**

**On**

**STEGANOGRAPHY**

**in**

**BACHELOR OF TECHNOLOGY**

Department of

**INFORMATION TECHNOLOGY**

**II YEAR – 2ND SEMESTER**

By

**I.SRAVAN**

**20315A1203**

Under the guidance of



# **SREENIDHI INSTITUTE OF SCIENCE & TECHNOLOGY**

**(AUTONOMOUS)**

**(Affiliated to JNT University Hyderabad, Hyderabad and approved by AICTE- New Delhi)**

**Yamnampet, Ghatkesar, R.R district, Hyderabad – 501301**

**CERTIFICATE**

This is to certify that the Technical Paper Writing & Seminar report entitled “**STEGANOGRAPHY**

**”** being submitted by **I.SRAVAN** bearing roll no. **20315A1203**in partial fulfilment for the award of the Degree of **BACHELOR OF TECHNOLOGY (II YEAR 2ND SEMESTER)** in **INFORMATION TECHNOLOGY** to the **Jawaharlal Nehru Technology University, Hyderabad,** is bonafied work carried out by him under our guidance and supervision.

By

**STEGANOGRAPHY**

ABSTRACT

There are plenty of text resources available for text steganography. Microsoft word being a commonly used communication medium can be well utilized as a cover document to hide the data. In this paper, a new steganographic method is presented which hides data in MSword documents. It uses one special feature of Microsoft word: change tracking. The process of data hiding is divided into two steps: message embedding and message extraction. On the sender’s side, a secret message is embedded inside a cover document to obtain a stegodocument. Depending on the data, the position where it should be embedded is decided. The embedded secret message is revised back again which makes the cover document look normal and also produces a stegodocument. On the receiver’s side, the hidden message is extracted back from the stegodocument. The paper shows comparison between two encoding techniques used for message embedding, namely Huffman and block encoding.

**INTRODUCTION**

Steganography is the art of sending hidden or invisible messages. The name came from the Greek word having meaning “covered writing”. While much of modern steganography focuses on images, audio signals, and other digital data, there is also a plethora of text sources in which information can be hidden. While there are various ways in which one may hide information in text, there is a specific set of techniques that uses the linguistic structure of a text [9] as the space in which information is hidden. Text steganography uses text as the medium in which information is hidden. Text steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts [10]. With any of these methods, the common thing is that hidden messages are embedded in characterbased text.

**OBJECTIVE**

Though the steganographic method presented in this paper focuses on Microsoft Word, the idea can be applied to some other communication mediums also. The robustness of the system can be increased by increasing randomness in the input and the degeneration database. As the work appears to be the effort of collaborative writing, is less likely to be under close scrutiny. The results obtained from the implementation show that embedding capacity of the Huffman coding is less as compared to the block encoding. Better results are obtained when a message is compressed using arithmetic encoding before embedding

**References**

[1] “A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique”, Tsung-Yuan Liu, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding—A survey,” Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] R. Stutsman, C. Grothoff, M. Attallah, and K. Grothoff, “Lost in just the translation,” in Proc. ACM Symp. Applied Computing, 2006, pp. 338–345.

[4] F. Johnson and S. Jajodia, “Steganalysis: The Investigation of Hidden Information,” in Proc. IEEE Information Technology Conf., Syracuse, NY, Sep. 1998, pp. 113–116

[5] WordNet v2.1, a lexical database for the English language. Princeton Univ., Princeton, NJ, 2005. <http://wordnet.princeton.edu/>

[6] Google, Google SOAP Search API (beta), [Online]. Available: http://www.seochat.com/c/a/Google-OptimizationHelp/Using-the-Google-SOAP-Search-AP

[7] K. Bennett, “Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text,” Purdue Univ., West Lafayette, IN, CERIAS Tech. Rep. 2004– 13, May 2004.

[8] J. T. Brassil and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text Documents,” Proc. IEEE, vol. 87, no. 7, pp. 1181–1196, Jul. 1999.

[9] P. Wayner, “Mimic functions,” Crypt., vol. XVI, no. 3, pp. 193–214, 1992.

[10] M. Chapman, I. D. George, and R. Marc, “A practical and effective approach to large-scale automated linguistic steganography,” in Proc. Information Security Conf., Malaga, Spain, Oct. 2001, pp. 156–165.

**By**

**I.SRAVAN**

**20315A1203**

**It-A**