

# **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.

**INDEX**

|  |  |  |
| --- | --- | --- |
| S.No | Topic | Page NO. |
| 1. | ABSTRACT | 4 |
| 2. | INTRODUCTION | 4-5 |
| 3. | EVOLUTION OF STEGANOGRAPHY | 5 |
| 4. | STEGANOGRAPHY VS CRYPTOGRAPHY | 5-6 |
| 5. | TYPES OF STEGANOGRAPHY | 6 |
| 6. | DISSECTING STEGANOGRAPHY | 6-7 |
| 7. | STEPS FOR HIDING AN IMAGE USING STEGANOGRAPHY | 7 |
| 8. | DIGITAL WATERMARKING | 7-8 |
| 9. | WHAT IS “STEGANALYSIS” | 8 |
| 10. | CONCLUSION | 8 |
| 11. | REFERENCE | 8-9 |

**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

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

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

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

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

In 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.

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.

**I. 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.

The word steganography literally means covered writing as derived from Greek. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. In broad sense, term Steganography is used for hiding message within an image.

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present. Steganography is in the (especially military) literature also referred to as transmission security or short TRANSEC.

**II**. **EVOLUTION OF STEGANOGRAPHY**

* CODE BREAKERS : David Kahn's The Code breakers and Bruce Norman’s Secret Warfare: The Battle of Codes and Ciphers recounts numerous tales of steganography .
* INVISIBLE INK : An innocent letter may contain a very different message written between the lines with invisible ink. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated. Later on, more sophisticated inks were developed which react to various chemicals.

* MICRODOTS: The Germans developed microdot technology. Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself (for a while). Besides being so small, microdots permitted the transmission of large amounts of data including drawings and photographs

**III.STEGANOGRAPHY VS CRYPTOGRAPHY**

Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not.

Steganography cannot be detected. Therefore, it is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ.

**IV. TYPES OF STEGANOGRAPHY**

MESSAGES IN TEXT program is called SPAM MIMIC.

MESSAGES IN STILL IMAGES most popular tool is outguess.

MESSAGES IN AUDIO data is hidden in layer III of encoding process of MP3 file. Messages in audio are always sent along with ambient noise.

MESSAGES IN VIDEO embedding information into multimedia data has gained increasing attention lately.

AN EXAMPLE

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

“Send lawyers guns and money”

Most communication channels like telephone lines and radio broadcasts transmit signals which are always accompanied by some kind of noise. This noise can be replaced by a secret signal that has been transformed into a form that is indistinguishable from noise without knowledge of a secret key and this way, the secret signal can be transmitted undetectable.

**V. DISSECTING STEGANOGRAPHY**

Steganography is a term used for hiding messages within an image. Any color pixel is made of a combination of red –green-blue mode(RGB) wherein each RGB component consist of 8 bits. If letters in ASCII are to be represented within the color pixels, the rightmost digit, called the least significant bit (LSB), can be altered.

Any variation in the value of this bit leads to very minimal variation in color. If we have to hide the word ‘digit’ in the image, we take the LSB of every color and hide each bit of the word in its RGB combination.

To insert the letter ‘D’ we modify three color pixels with three bits in each color pixel, we utilize 14 color pixels to hide the entire word with only 1 bit in the 14th pixel.

CONTD…

Suppose we have a 24-bit image 1024 x 768 (this is a common resolution for satellite images, electronic astral photographs and other high resolution graphics). This may produce a file over 2 megabytes in size (1024x768x24/8 = 2,359,296 bits). All color variations are derived from three primary colors, Red, Green and Blue. Each primary color is represented by 1 byte (8 bits). 24-bit images use 3 bytes per pixel. If information is stored in the leastsignificant bit (LSB) of each byte, 3 bits can be a stored in each pixel. The "container" image will look identical to the human eye, even if viewing the picture side by side with the original.

**VI. STEPS FOR HIDING AN IMAGE USING STEGANOGRAPHY**

Start s-tool and window explorer using the later as drag and drop interface the software. Drag and drop the image to be used as the carrier file from the explorer onto the actions window in s-tool. Drag and drop the data file on the carrier file. Give pass phrase and encryption algorithm when prompted. Pass these to receiver too. The hidden file is ready. Receiver has to click on the “reveal” button to extract the data.

**VII. DIGITAL WATERMARKING**

Usually carrier file carry hidden data unrelated to the content in which it is embedded, but digital watermarking holds information about its carrier medium.

Information such as a number or a text into a multimedia file can be added to carrier file through slight data modification. this process has gained huge acclaim from the media for enabling copyright for their products.

Video steganography is more suited to avoiding piracy and is mostly used for digital watermarking.

**Types of digital watermarking**

ROBUST DIGITAL WATERMARKING A robust watermark is

embedded in the file in such a way that even if the file is later

transformed, the watermark will not be removed

FRAGILE DIGITAL WATERMARKING is similar to fragile

analog watermarks-if the data is altered or copied in exactly, the

watermark is corrupted

For ensuring the integrity of data, digital signatures are preferred but fragile digital watermarking can detect data tempering without alerting the culprit. Compatible players refuse to play content that does not bear a valid watermark.

**VIII. WHAT IS “STEGANALYSIS”**

The art of detecting, decoding and altering messages hidden via steganography is called steganalysis. It is easiest when before as well as after steganography copies of file are present.

Steganalysis can make the hidden data work against the creator. Any malicious interceptor could alter as carrier file without the knowledge of sender or the intended receiver. Hence inaccurate or wrong data could be passed under identity of the original sender.

**CONCLUSION**

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

**REFERENCE**

[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.