

**International Journal of Advanced Research in Computer Science** 

**RESEARCH PAPER** 

# Available Online at www.ijarcs.info

# A Novel Approach Text Secure Steganography using Cheating Text by Genetic Operators Crossover

Dr. Ch. Rupa\* Associate Professor Dept of CSE, VIT, Nambur,Guntur(dt), India rupamtech@gmail.com

Dr. P. S. Avadhani Professor, BOS, Dept of CS & SE, Andhra University, Visakhapatnam. India, psavadhani@yahoo.com B. Sai Jyothi Assistant Professor Dept of CSE, VIT, Nambur, Guntur(dt), India. sai16879@yahoo.com

V. Sowjanya Student (M. Tech), Dept of ECE, Andhra University, Vizag, India

*Abstract:* Sending the data securely in the communication channel is exigent task. While transmitting the various text documents through communication channels there have been used different methods for hiding the information in the text (Text Steganography). This paper proposes a new method for embedding the original text in a cover text. In this, the ciphertext of the secret message is embedded instead of the secret message directly. Genetic operator crossover method is used for encrypting the original text. Cheating text method is used for embedding the ciphertext into the Cover text. By using generic operator crossover (GOC) and cheating text methodology, security can be improved and will have a perfect perceptual transparency. And it does not make any apparent changes in the original text.

Keywords: Genetic Operator Cross over (GOC), Cheating text, Text Steganography, Cover text, Secret message

# I. INTRODUCTION

Steganography is a term encompassing many sub disciplines. Its main feature is hiding the original information using cover data such as text, audio, video, Image etc as shown I the Fig 1 for making undetectable or keeping the original information secret. If the hidden message is reveal, the goal of steganography is defeated. The term steganography is a Greek word means "covered writing". As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. The message is hidden in another media such that the transmitted data will be meaningful and innocuous-looking to everyone. Compared with cryptography attempting to conceal the content of the secret message, steganography conceals the very existence of that.

Steganalysis is the art of detecting the hidden data on the communication channel. Various types of stegaography are existed such as Text steganography, where the secret information is hide in the text data. Audio steganography, the secret information is covered in to the audio files such as .arr, .wav, etc. Video steganography, where original information will be hidden in the video files such as .mp3,.wmp etc. Image steganography, information is storing in to the images like .jpg, .bmp etc. Among them Image steganography is the popular method. In this method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate human eyes [2, 3, 4]. The most difficult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to a image or audio [5, 6]



Figure 1. Types of Steganography

Text stegaography have been widely used and consequently various methods for hiding the information in texts have been developed so far. Text steganography classified into three categories [1]. Those are

- A. Format based
- B. Random and statistical generation
- C. Linguistic Method.

In steganography two aspects are usually addressed. First, the cover-media and stego media should appear identical under all possible statistical attacks. Second, the embedding process should not degrade the media fidelity, that is, the difference between the stego media and the cover-media should be imperceptible to human perceptual system. In the Text Steganography, a secret message is embedded in a cover text by using embedded algorithm and a secret key. The result, stego text is transmitted over a communication channel to the receiver. Receiver extracts the secret text by using extraction algorithm and a secret key. During transmission the stego text can be monitored by unauthenticated viewers for extracting the original information. ]. A block diagram of generic text steganographic system is shown in the figure 2.



Figure 2. General Procedure of Text Steganography

In this paper, a new method for text steganography is proposed. It supports linguistic steganography [10]. Now day security techniques are well developed. Biotechnology is playing a vital role in the information security. In genetic algorithms, **crossover** is a genetic operator used to vary the programming of a chromosome or chromosomes from one generation to the next. It is analogous to reproduction and biological crossover, upon which genetic algorithms are based. In this method secret text is encrypted by using genetic operator encryption algorithm. The result cipher text will be hidden in a text which is called as cheating text. The result will e participated in the transmission. Section 2 and Section 3 describe the encryption algorithm by using genetic operators [1] and cheating text method [7, 9] for embedding the original message.

# **II. ALGORITHMS**

#### A. Encryption Algorithm

This section consists of a message encryption algorithm which is done using basic operations of genetic operators cross over [1].

- a. Select text message as text.
- b. Loop i = 1 to length(text)/2.
- c. if i is even then s1 = length(text) + 2 i.
- d. if i is odd then s1 = (length(text)/2) + 2 i.
- e. if s1 > length(text msg) then
- s1= (length(text)) then s1=(length(text)/2)+1 f. Convert i and s1 position of text to its 8 bit
- Representation and store it to msg bin.
- g. loop p = 1 to 8
- h. if i is even and p belongs to {3,4,7,8} then swap p and i position value of text msg bin.
- i. if i is odd and p belongs to {1,2,5,6} then swap p and
- j. i position value of text msg bin.
- k. Convert i<sup>th</sup> and s1<sup>th</sup> position to its character representation.

k. End.

#### B. Decryption Algorithm

Message decryption is done at the receiver side using the different reverse operation compared to what is done at the sender side.

#### III. TEXT STEGANOGRAPHY BY CHEATING TEXT

# A. Cheating Text Methodology

In this concept original message is embedded in a meaningful text called cheating text. The positions of the characters of the plain text in the cheating text are stored as Real Message Index File (RIF) based on Character location table (CLT). This file is encrypted and sent along with the cheating text. The receiver, in turn, decrypts the RIF table and gets back the original message from the received cheating text. According to the plaintext and depending on the cheating text we can make a special index file, called Real Message index file (RIF). Therefore, the real data we send via the channel is the cheating text and the encrypted index file [7, 9]. Thos process is shown in fig 3.



Figure 3. Process of Cheating text Method

#### B. Proposed Method

The proposed system, a novel approach in Text steganography consists of two modules as shown in fig 4. In the first module, the original message, nothing but a secret message is encrypted by using basic operations of generic operators cross over encryption algorithm. The result is hiding into a meaningful text called as cheating text by cheating text methodology [7, 9]. Embedded the ciphertext in a cheating text is a second module. The results are discussed in section IV.

The following are the advantages with the proposed system:

- a. Improves the security by using genetic operators crossover operations.
- b. Secure transfer of message with the addition of cheating text steganography.
- c. It satisfies the security services via linguistic stego method.
- d. Perfect perceptual transparency.
- e. The hiding capacity can be improved.
- f. It does not make any apparent changes in the original text.
- g. It can achieve high level of security through genetic operators crossover.
  - This paper presented a new approach of text

steganography by linguistic text steganography method. Embedded an encrypted message in to a cover text such as cheating text will be improved the confidentiality and authentication.



Figure 4. Text Steganography by cheating text

# IV. RESULTS AND DISCUSSION

Fig 5 describes the information as original text which is transmitted by the sender.

	Note
Enter Plain Text	
hello	
OK Cancel	
	Enter Plain Text hello

Figure 5. Secret Message

Fig 6 consists of the cipher text of the secret message which is encrypted by the generic operator crossover along with the suitable cheating text as cover text which is embedded the secret message.



Figure 6. suitable Cheating text

Fig 7 gives original text after extracting from the cover text at the receiver side.

Messag	e 🔀
(i)	Receiver side: hi,Girls are all wonderful Original Text: hello
	ОК

Figure 7. Extraction of Secret Message

#### V. ACKNOWLEDGMENT

We thank management of VVIT, Nambur and Andhra University, vizag to provide the infrastructure for completing this research work

#### **VI. REFERENCES**

- Souvik Bhattacharyya. and Gautam Sanyal. "Implementation and design of an image based steganographic model.", In Proceedings of IEEE International Advance Computing Conference, Patiala India, 2009.
- [2] Kran Bailey Kevin Curran. "An evaluation of image based steganography methods", International Journal of Digital Evidence, Fall 2003, 2003.
- [3] Jr. L. M. Marvel, C. G. Boncelet and C. T. Retter. "Spread spectrum image steganography", IEEE Trans. on Image Processing, 8:1075–1083, 1999.
- [4] Nasir Memon R. Chandramouli. "Analysis of lsb based image steganog-raphy techniques", In Proceedings of IEEE ICIP, 2001.
- [5] N.F. Maxemchuk J.T. Brassil, S. Low and L. O.Gorman. "Electronic marking and identification techniques to discourage document copying", IEEE Journal on Selected Areas in Communications, 13:1495–1504, 1995.
- [6] N.F.Johnson. and S. Jajodia. "Steganography: seeing the unseen" IEEE Computer, 16:26–34, 1998.
- [7]. Ch.Rupa, P. S. Avadhani, "Message Encryption Scheme using cheating Text", pp 80-85 organized by ITNG 2009 at Lasvegas, Nevada on April-09.(indexed by DBLP,EI,IEEE).
- [8] The Unicode consortium, The Unicode standard, http:// www.unicode.org.
- [9] Ch. Rupa and P. S. Avadhani, "Performance Evaluation of Message Encryption Scheme using Cheating Text", Global Journal of Computer Science and Technology, Vol 1. 2, No 13, pp. 77-80, 2009.
- [10] K. Moon Y. Kim and I. Oh. "A text watermarking algorithm based on word classification and inter-word space statistics" In Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), pages 775–779, 2003.