International Journal of Computer Science and Informatics

Volume 3 | Issue 1 Article 4

July 2013

A Hybrid Method of Hiding The Text Information Using Stegnography

M.Grace Vennice
CSE Dept, CMRCET, Hyderabad, India ., grace_vennice@yahoo.co.in

M. Swapna
CSE Dept, CMRCET, Hyderabad, India, swapna_manthena2007@yahoo.com

A Hybrid Method of Hiding The Text Information Using Stegnography

M.Grace Vennice, M.Swapna, MD.Ahmad Ali & T.Dharma Reddy

CSE Dept, CMRCET, Hyderabad, India .
E-mail : grace_vennice@yahoo.co.in, swapna_manthena2007@yahoo.com

Abstract - The Often Distribution of encrypted messages will depict the concentration of third parties. The attempts can be made to break and expose the actual messages by the hackers and crackers. To conceal the subsistence of message steganography is introduced by hiding a secret message inside another credulous message. . Steganography along with cryptograph y is used and offers suitable amount of privacy and security over the communication channel. In this paper along with various existing text-based steganography techniques, an overview of text steganography and a concise history of steganography can be presented. The problems present in the text steganography and issues with existing solutions are highlighted. In information hiding, a novel approach is proposed by using inter-word spacing and inter-paragraph spacing as a hybrid method. Based on the length of the secret message, the proposed method provides dynamic generated stego-text with six options of maximum capacity. The considerable drawbacks of every existing method and how our new approach might be recommended as a solution can be analyzed in this paper.

Keywords- *steganography, stego-image,XML schema,interword spacing, interparagraph spacing.*

I. INTRODUCTION

Information hiding is a general term encompassing many subdisciplines. One of the most important subdisciplines is steganography as shown in Fig.1.

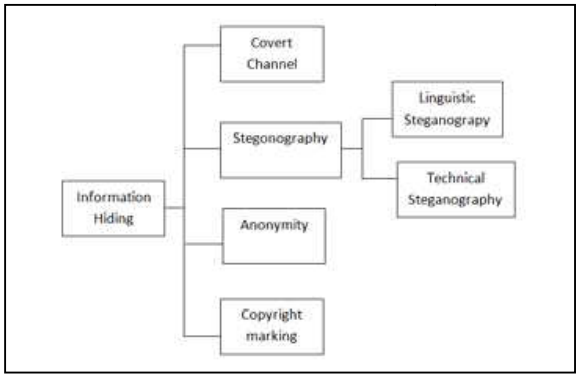

Fig.1: A Classification of Information HidingTechniques

The goal of steganography is to transmit a message through some innocuous carrier i.e text, image, audio and video over a communication channel where the existence of the message is concealed. Based on Fig.1, steganography is one of the information hiding techniques and which can be categorized into linguistic steganography and technical steganography. Linguistic steganography defined by Chapman as "the art of using written natural language to conceal secret messages". A more specific definition by Krista Bennet in explaining linguistic steganography as a medium which required not only the steganographic cover that is composed of natural language text, but the text itself can be either generated to have a cohesive linguistic structure, or the cover text that begin with natural language. On the other hand, technical steganography is explained as a carrier rather than a text which can be presented, as any other physical medium such as microdots and invisible inks. The principle of information hiding is pioneered and documented *On the Criteria to be Used in Decomposing Systems Into Modules* in 1972, whereby Parnas designed a software system and each module's "interface of definition was chosen to reveal as little as possible about its inner workings". Many researchers are trying to carry out research by applying this concept in information hiding. There are three aspects in information hiding systems contend with each other: capacity, security and robustness. Capacity refers to the amount of information that is able to be hidden in the medium, whereas security is important when a secret communication is kept to be secret and undetectable by eavesdroppers. Lastly, robustness can be explained as the amount of modification the stegomedium can withstand before an adversary can destroy hidden information.

Fig.2 shows the basic text steganography mechanism. Firstly, a secret message (or an embedded

data) will be concealed in a cover-text by applying an embedding algorithm to produce a stego-text. The stego-text will then be transmitted by a communication channel, e.g. Internet or mobile device to a receiver. For recovering the secret which sent by the sender, the receiver needs to use a recovering algorithm which is parameterised by a stego-key to extract the secret message. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it.

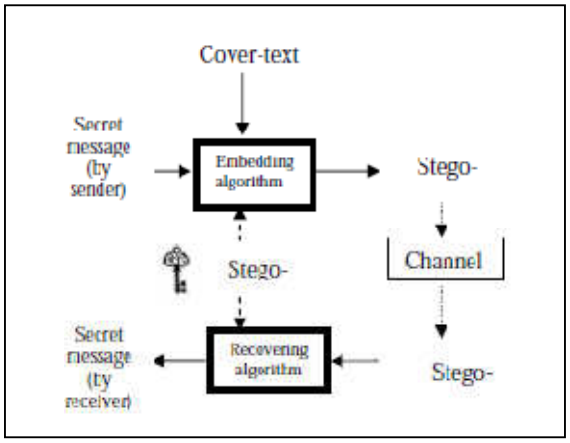

Fig. 2: The Mechanism of Text Steganography

Text steganography can be classified in three basic categories-format-based, random and statistical generation and linguistic method.

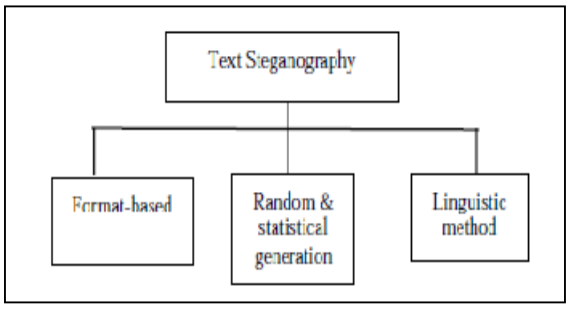

Fig.3: Three basic categories of text steganography

In this paper, a new approach is proposed for text steganography by creating a hybrid method in utilising whitespaces between words and paragraphs in right-justification of text. This method can be an improvement of open space method because it is not using a sole method of encoding data. By combining both methods which is inter-word spacing and interparagraph spacing into an embedding algorithm, a larger capacity for embedding hidden bits is provided.

II. PROPOSED MODULES

In this paper we are going to propose the following four parts.

1. Registration.
2. Encrypt text information.
3. Mapping through that XML schema.
4. Decrypt that information to another language of environment.

Registration:

Registration is a method of officially recording something. Usually something is registered to claim more rights, or to protect ownership, or because the law says it must be registered to be used legally. A register was a large book. It was used like a diary to record business dealings or other events. To enter personal information about that particular user. To enter that username and password identification mechanism. To give that successful solution identification information. To get that window in the form message transformation.

Encrypt Text information:

To give that any message information that can be converted in the form bit format identification manner. To generate bit format identification process can be involved in the form substitution technique. To substitution technique is called as Mapping through that XML language to generate one of dictionary moment identification process.

Mapping through that XML schema:

To give that full description of information through that classification methodology to introduce in the form tree structure identification technique. After that to generate identification of correct decision making identification process. To expose data information currently available data.

Decrypt that information to another language of environment:

After encoding that information it can be transferred and stored inside the same view message. This view message identification process is called as new generate XML schema which can be generated inside that database.

III. DESIGN & IMPLEMENTATION

In this section we are going to discuss about the implementation of how the text information is hidden. The below given code will generate a form which ask for the user who wants to send a hide the text to a receiver.

```
private void btnSendActionPerformed
(java.awt.event.ActionEvent evt) {
try {
String sys=JOptionPane.showInputDialog
("Enter Receiver Name or IP Address:");
File file=new File(asciiemb.path);
FileInputStream fis=new FileInputStream(file);
byte[] b=new byte[fis.available()];
fis.read(b);
String data=new String(b);
String fnme=file.getName();
String key=txtKey.getText();
Socket socket = new Socket(sys, 5680);
ObjectOutputStream oos = new
ObjectOutputStream(socket.getOutputStream
());
oos.writeObject("Data");
oos.writeObject(data);
oos.writeObject(fnme);
oos.writeObject(key);
oos.writeObject(fnme.subSequence(0,
fnme.lastIndexOf("."))+".key");
} catch (FileNotFoundException e) {
e.printStackTrace();
} catch (IOException e) {
e.printStackTrace(); }}
```

Fig.4 : Code for user to give receiver name and IP address

The below code in Fig.4 describes how the generated key is saved in-order to decode the received text message at the receiver side.

```
private void btnSavekeyActionPerformed
(java.awt.event.ActionEvent evt) {
try {
String key = asciiemb.getKeyFile();
FileOutputStream fos = new FileOutputStream
(key);
fos.write(txtKey.getText().trim().getBytes());
fos.close();
JOptionPane.showMessageDialog(null, "Key File
Saved");
} catch (Exception e) {
e.printStackTrace();
}}
```

Fig 5: Code to save the key

On the other hand the receiver browse the text from received n number of message for which the given code will be used.will receive the Message or the text and he has to

```
private void browseMessage() {
JFileChooser jfr = new JFileChooser
();
int check = jfr.showOpenDialog(this);
if (check ==
JFileChooser.APPROVE_OPTION) {
String path = jfr.getSelectedFile
().getPath();
try {
FileInputStream fis = new
FileInputStream(path);
byte b[] = new byte[fis.available()];
fis.read(b);
jtaMsg.setText(new String(b).trim());
} catch (Exception e1) {
e1.printStackTrace();
}}}
```

Fig.6: Code to browse the received text

After selecting the desired text and decoding it the text has to be displayed to the receiver so the given code will be used to achieve it.

```
private void browseOutput() {
JFileChooser jfr = new
JFileChooser();
int check = jfr.showOpenDialog
(this);
if (check ==
JFileChooser.APPROVE_OPTION) {
String path = jfr.getSelectedFile
().getPath();
txtOutPath.setText(path);
try {
FileInputStream fis = new
FileInputStream(path);
byte b[] = new byte[fis.available
()];
fis.read(b);
jtaOutText.setText(new String
(b).trim());
} catch (Exception e1) {
e1.printStackTrace();}}}
```

Fig.7: Code to browse the output

RESULTS

The following are the produced screen shots of the paper.

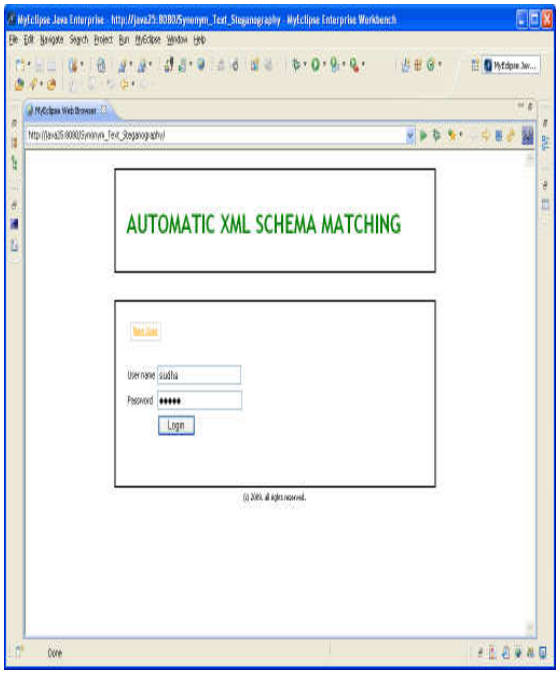

Fig.8: Login Page

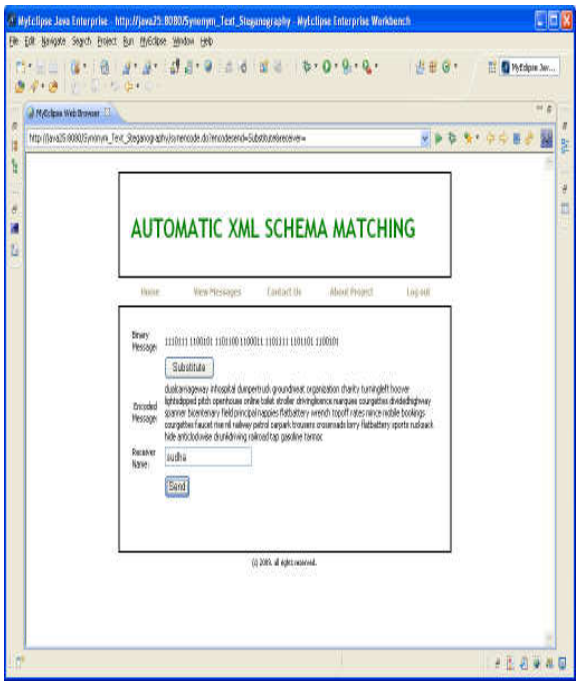

Fig.9: Sending Encoded Text Message

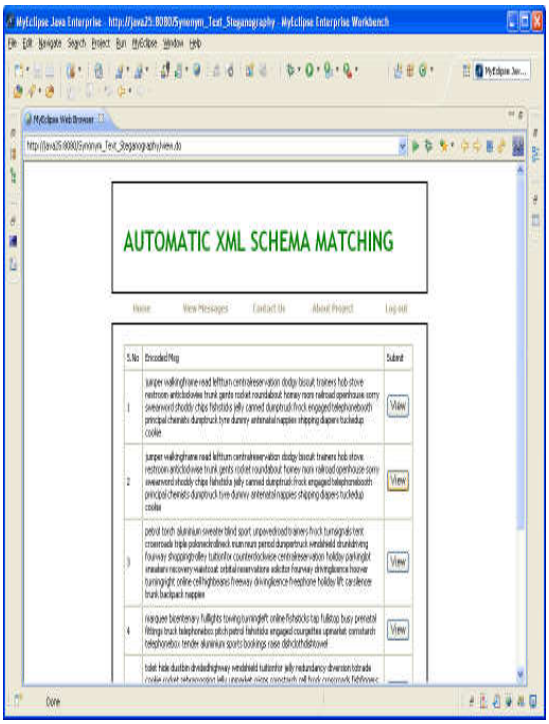

Fig.10: To browse the received text

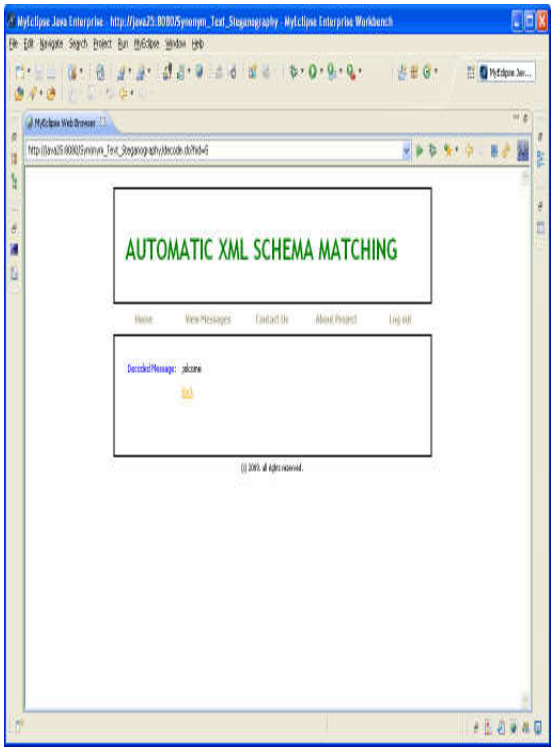

Fig.11: Receiver decoding the message

CONCLUSION

We have presented a new approach of text steganography method using inter-word and interparagraph spacing for hiding information. The unique feature about the method is to generate a cover-text dynamically by offering six options for user according to their length of the secret message. The future work should be focused towards optimizing the robustness of the decoding algorithm. This is because the hidden data will be destroyed once the spaces are deleted by some word processing software. Besides that, it is important to improve the capacity of the embedded scheme by taking other compression method into consideration.

REFERENCE

[1] N. Provos, P. Honeyman, "Hide and Seek: An Introduction to Steganography", The IEEE Computer Security, 2003.

[2] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, July 1999, pp. 1062 – 1078.

[3] Bret Dunbar, "A Detailed Look At Steganographic Techniques and Their Use in Open-Systems Environment", SANS Institute, 2002.

[4] B. Pfiztzmann, "Information Hiding Terminology." pp. 347{350, ISBN 3-540-61996-8, results of an informal plenary meeting and additional proposals, 1996.

[5] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report, 2004.

[6] P. Wayner, "Mimic functions", Cryptologia archive Volume XVI, Issue 3, July 1992, pp.193 – 214.

[7] P. Wayner. "Strong Theoretical Steganography". Cryptologia, XIX(3), July 1995, pp. 285-299.

[8] M. Chapman, G. Davida. "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text". Master Thesis, Milwaukee: University of Wisconsin- Milwaukee, 1998.

[9] "Spammimic", 2000. [Online] Available: http://www.spammimic.com [Accessed March 8 2008]

[10] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE Computer, February 1998, pp.26−34.

[11] P. Wayner, Disappearing Cryptography: Being and Nothingness on the Net, Academic Press, Inc., 1996

◈◈◈