ASTERISK TEXT STEGANOGRAPHY TOOL

A highly secure text steganography approach

Abhijit Sharad Thakker
Mumbai, India
Abhijit.thakker@gmail.com

***Abstract* - Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent the message being detected by any other party. Steganography and encryption are both used to ensure data confidentiality. Steganography hides the existence of secret message and in the best case nobody can see that both parties are communicating in secret. This text steganography tool will help quick, efficient and highly secure text message transfers.**

***Keywords* – Steganography, Text Steganography, Text Steganography tool, Secure Text Message transfer, Asterisk Algorithm, Asterisk Text Steganography Tool.**

I. Introduction

There is a serious shortage of text steganography tools available. This made to the development of this text steganography tool. The main aim of this text steganography tool is to improve the confidentiality and security of information in text and also to provide a better hiding technique as compared to other steganography tools.

Steganography techniques are basically divided in three broad categories:

Pure Steganography: We call a steganography system pure when it does not require prior exchange of data like shared-keys. The definition can be mathematically described as: The set (C, M, D, E) where C is the set of covers, M the set of messages with $|M| <= |C|$, E the embedding function which maps $E: C \times M \rightarrow C$ and D is the extracting function which maps from $D:C \rightarrow M$ and the property $D(E(c,m))= m$ for all $(m E M, c E C)$ is a pure steganography system

Shared-secret Steganography: We call a steganography system a shared-secret or shared-key or secret when it does not require prior exchange of data like shared-keys. The definition can be mathematically described as: The set (C,M,S,Ds,Es) where C is the set of covers, M the set of messages with $|M| <= |C|$, e the embedding function which maps $C \times M \rightarrow C$ and S is the set of shared-secrets; $Ds: C \times S \rightarrow M$ and $Es: C \times M \times S \rightarrow C$ and the property $Ds(Es(c,m,s) , s) = m$ for all $(c E C, m E M, s E S)$ holds is called a shared-secret steganography system.

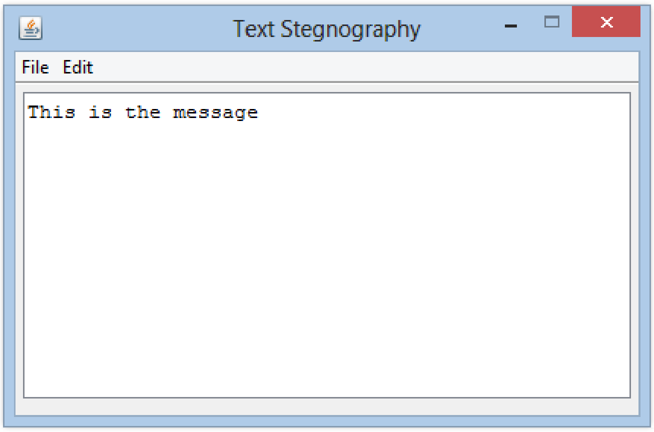
Public-key Steganography: This kind of steganography does not rely on shared-key exchange. Instead it is based on the public-key cryptography principle in which there are two keys, one being the public key which can be usually obtained from a public database and the other a private key. Usually in this case the public key is used in the embedding process and the private key in the decoding process.

The type of steganography technique used here is the shared-secret steganography. The format of the key is first decided by the end users and as the format of the key is decided, the same format can be used for all the keys that they use for data transfers. And later when they feel that their current format is no more secure, they can change the format of the key and use the new format of the key for secure message transfers. This format is interpreted in different ways by this tool, thus ensuring high data security and confidentiality.

This tool uses 54 unique data hiding algorithms. This makes the data more secure and difficult for the third person to know what the actual data is.

II. Proposed Tool

This tool basically helps achieve secure message hiding and helps to pass on text message from sender to receiver without any third person knowing that an important communication is taking place. In this tool the person who wants to send the message types a message in the text area in the tool (Fig. 1). And when the encrypt option is selected from the menu bar (Fig. 2), a dialog box appears which has a text field for typing in the password and 26 buttons having each alphabet from A-Z respectively and a button saying ‘Encrypt/Encode’ (Fig. 3). He would just type in the password with the decided format and what that person would get is text with jumbled characters (Fig. 4). He can than save it as a text file and sends it over to the receiver. He will open the text file and then type in the same password and get the original message (Fig. 5, Fig. 6).



This is the message

Fig. 1 Asterisk Text Steganography Tool

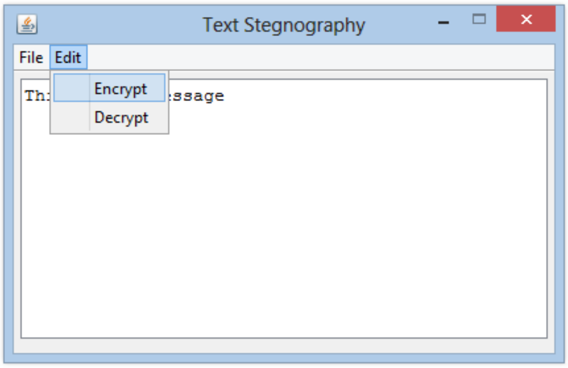
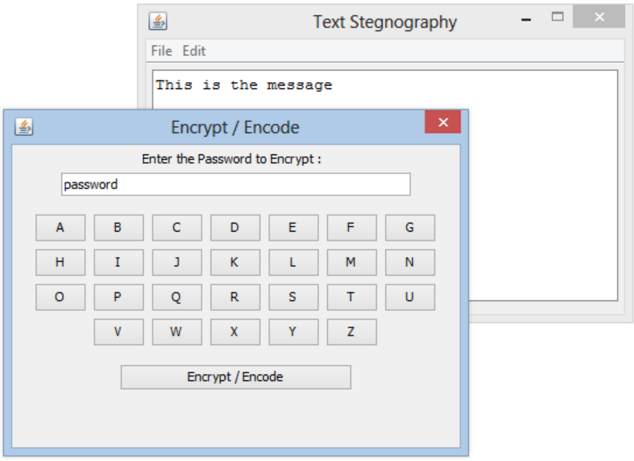


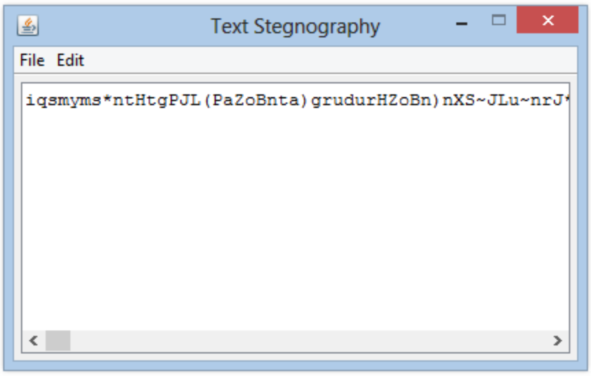
Fig. 2 Selecting Encrypt option



This is the message

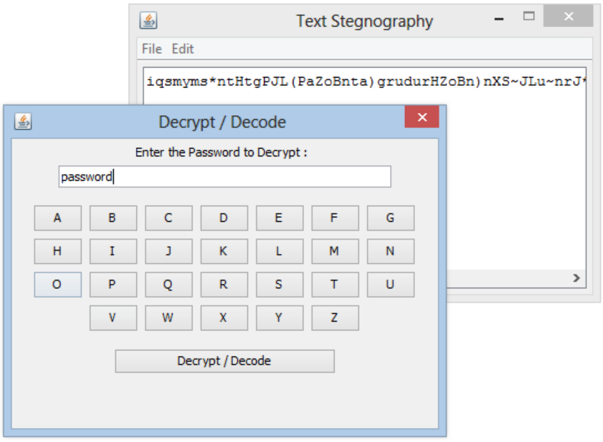
password

Fig. 3 On selecting Encrypt option



iqsmyms*ntHtgPJL(PaZoBnta)grudurHZoBn)nXS~JLu~nrJ*

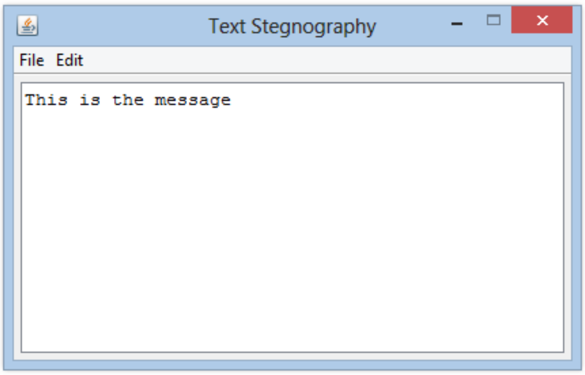
Fig. 4 The jumbled text which includes the hidden message after clicking on the Encrypt/Encode button as shown in Fig. 3



iqsmyms*ntHtgPJL(PaZoBnta)grudurHZoBn)nXS~JLu~nrJ*

password

Fig. 5 On selecting Decrypt option from Edit menu



This is the message

Fig. 6 After entering the correct password and clicking on Decrypt/Decode button as shown in Fig. 5

What is unique about this tool?

This is not the normal data hiding tool as others. The main thing about this tool is that it includes 54 algorithms all together - this includes 27 encryption algorithms and 27 decryption algorithms. That is, every alphabet button on the encryption and decryption dialogue box has a unique algorithm associated with it. That is password say “ABC” is typed and the button saying “Encrypt/Encode” is clicked - will get a different output and a password saying “AB*” and then clicking on the button saying “C” will give a different output. What this tool sees is for the Asterisk (*) character every time any button is clicked on the encrypt dialogue box or decrypt dialogue box. If an Asterisk (*) character is found as the last character in the password field, the button pressed after it encrypts the message in its own unique method as placed in the back end. So, with every alphabet button placed on the dialogue box which asks for the encryption and decryption password, there is a unique data hiding algorithm associated with it. So this gives us 27 data hiding algorithms behind 27 buttons on the encryption pad and 27 data retrieval algorithms behind 27 buttons on the decryption pad.

For example:

Suppose the sender and the receiver decides to apply the Asterisk (*) character coding algorithm at the end of every word in the password and if the password is “Hey my friend”.

1. So what the sender would do is that he would type the message in the message text area and then type “he*” in the password field on the encryption pad and then click on the button “Y” on the encryption pad.

2. The sender would get text with jumbled characters.

3. Then again select the encrypt option in the menu bar and type “m*” in the password field on the encryption pad and then again click button “Y” on the encryption pad.

4. The sender would again get text with jumbled characters which are nothing but the jumbling done in characters which we get in step 2.

5. Then again select the encrypt option in the menu bar and type “frien*” in the password field on the encryption pad and then click on button “D” on the encryption pad.

6. The sender would again get text with jumbled characters which are nothing but the jumbling done in characters which we get in step 4.

7. Then finally save the text file and send it over to the receiver.

8. The receiver would do the same using the decryption pad and gets the secret message.

If this password pattern is decided and changed after every few days it would be very difficult for the hacker to first of all get the password and on top of it again get the pattern with which the encryption has been done. Apart from this the size of this tool is very less. It is based on java. So it needs no extra plug-in or no more hardware requirements. The JAR file of this tool is also available for the other operating systems like MAC and LINUX. This makes this tool better than all the other tools available.

How would it be difficult for a third person to get the secret message?

1. The simple Look and feel would deceive the third person.

2. This third person would not know that there is an algorithm behind every button on the pad because if the last character in the password field is not Asterisk than the button acts as nothing but buttons in a virtual keypad.

3. Even suppose he has this tool than he would have to think of the password.

4. Even if he has the tool and somehow gets the password, he would not know the way in which that password is to be used. The pattern would not be known.

5. Even if the third person know has the tool has the password and has the pattern in which the password is to be used, still it won’t be easy for him because in this tool password “ABC” is not the same as password “   ABC”. This means that the spaces which you include in the password field also changes the way the data hiding/retrieval process is carried out. So all in all getting the original message is very difficult for the third person.

6. To get the original message the receiver should: Have this tool + know the password + know the pattern in which password should be used + the spacing that should be followed in the password to get the original message.

7. All this making it too difficult for the third person to crack the password and get the original message back.

8. Making the tool highly secure and helps secure and easy transfers of highly confidential messages.

Technical description:

The tool is built using advanced java language. The shuffling algorithms used here are basically associated with the integer (ASCII) value of each and every character. That is the ASCII value of every character in the password is taken and the characters in the message are shuffled accordingly. First the message is appended with a series of random characters and then the shuffling algorithms are implemented accordingly. This creates more complexity in the message that is to be sent after data hiding. The outputs change with every button in the encryption or decryption dialogue box pressed along with the Asterisk (*) character Steganography technique. This makes this tool every secure and very effective as compared to any other steganography tools available.

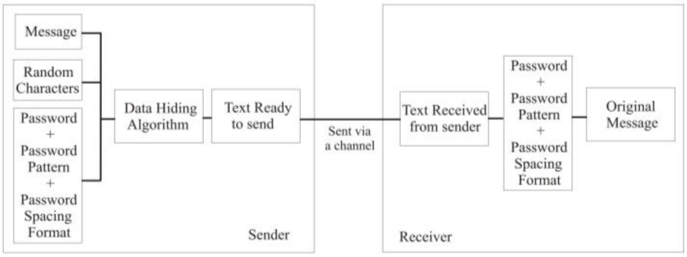

Message
Random Characters
Password + Password Pattern + Password Spacing Format
Data Hiding Algorithm
Text Ready to send
Sender
Sent via a channel
Text Received from sender
Password + Password Pattern + Password Spacing Format
Original Message
Receiver

Fig. 7 System Architecture

Algorithm:

```
1. Start

2. Get the message that needs to be hidden from the sender

3. Check for the message length.

4. If length of message= 0

    Go to step 7

5. Ask for password

6. If length of password= 0

    Go to step 8

5. If an Asterisk (*) character encountered as the last character in the password field and an alphabet button clicked

    Implement the shuffling method behind that button.

    End.

  Else

    Type the character on that button in the password field.
```

6. If the “Encrypt/Encode” or the “Decrypt/Decode” button clicked

    Implement the shuffling method behind that button.

    End.

7. Show message box stating that the hiding or retrieval process cannot be completed because the message field is empty and go to step 3.

8. Show message box stating that the hiding or retrieval process cannot be completed because the password field is empty and go to step 5.

III. Application

This tool is very helpful for the data hiding and retrieval purposes. First of all this tool has so many algorithms that there could be many number of passwords and password patterns possible. This gives the sender and the receiver a wide pool of patterns to decide from and also gives the hacker or the cracker much more difficulty to crack a particular message. This tool can be used for variety of purposes like secure message passing or all the applications where such security is very much needed like some very important information of a company can be kept encrypted and when needed by that authority, he can easily access by just typing in the password with the pattern decided upon. The size of this tool is very small hence sending this software along with the encrypted message file would not at all be an issue. Thus helping a successful and secure encryption and decryption of message and also sending and receiving the message with much more security. It can also be used in military applications. This tool thus helps us keep data highly secure and high confidential very easily. Getting high security with less effort is what everyone wants. And this is very well achieved in this Asterisk Text Steganography Tool.

IV. References

[1] W. G. Chambers, Basics of Communications and Coding, 1985, Clarendon Press Oxford, Oxford Science Publications.

[2] Sweeney, Error Control Coding: An Introduction, 1991, Prentice-Hall.

[3] R. E. Blahut, The theory and practice of error control codes, 1983, Addison-Wesley.

[4] Blah90, R. E. Blahut, Digital transmission of information, 1990, Addison-Wesley.

[5] Biss92, C. C. Bissell and D. A. Chapman, Digital Signal Transmission, 1992, Cambridge University Press.

[6] A. G. Konheim, Cryptography: A primer, 1981, John Wiley and Sons, New York .

[7] Chou94, A. K. Choudhury and N. F., Maxemchuk and S. Paul and H. G. Schulzrinne, Copyright Protection for Electronic Publishing over Computer Networks, 1994, Submitted to IEEE Network Magazine, June.