Journal for Research | Volume 04 | Issue 04 | June 2018
ISSN: 2395-7549

Text Steganography- An Approach

Subhas Naskar
Department of Computer Science & Engineering
University of Calcutta, India

Asthik Samanta Gayen
Department of Computer Science & Engineering
University of Calcutta, India

Prof. Samir Kumar Bandyopadhyay
Department of Computer Science & Engineering
University of Calcutta, India

Abstract

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. Steganography is of many types such as image steganography, text steganography, audio/video steganography etc. Text Steganography is quite difficult than other techniques because of less amount of redundancy and changes can be detected quite easily. This paper proposed a method for data hiding.
Keywords: Text Steganography, Cryptography, Data Hiding

I. INTRODUCTION

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing [1]. The purpose of steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information [2]. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it.

II. REVIEW WORKS

The most of today's steganographic systems use images as cover object because people often transmit digital images over email and other communication media. Several methods exist to utilize the concept of Steganography as well as plenty algorithms have been proposed in this regard. To gather knowledge in this particular research field, we have concentrated on some techniques and methods which are described below.

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover object. For images as a covering media, the LSB of a pixel is replaced with an M's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel by modifying the LSBs of R, G and B array. To the human eye, the resulting stego image will look identical to the cover image [1, 2]. Hiding data in the features of images is also an important technique which uses the LSB modification concept. In this method, to hide data in an image the least significant bits (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process [2, 3].

An interesting application of steganography and cryptography has been developed by Sutaone, M.S., Khandare, M.V, where a steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method. In that method, the secret data are spread out among the cover image in a seemingly random manner. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out. The advantage of this method is that it incorporates some cryptography in that diffusion is applied to the secret message [4].

The next interesting application of steganography is developed by Miroslav Dobsicek, where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information [5].

In 2007, Nameer N. EL-Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse steganalysis too [6].

S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das in 2008 has also proposed a heuristic approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique [7].

III. PROPOSED METHOD

Unlike the two aforementioned proposed approaches in which cover is dynamically generated and stego file consists of a list of words, this approach makes use of a pre-determined cover file which can be any meaningful piece of English text and can be drawn from any source (For example, a paragraph from a newspaper/book). The approach works by hiding a message using start and end letter of the words of a cover file. This approach works on the binary value of a character as opposed to the above two proposed approaches which work on the ASCII value. After converting the cipher text to a stream of bits, each bit is hidden by picking a word from the cover file and using either the start or the end letter of that word depending on the bit to be concealed. Bit 0 or 1 is hidden by reading a word, sequentially, from the cover file and including the starting letter or the end letter, respectively, of the word in the stego key. A word having same start and end letter is skipped. Since no change is made to the cover, the cover file and its corresponding stego file are exactly the same.

A. Hide Algorithm

1) Get a cover file.
2) Convert the input file to its binary equivalent (bin).
3) Read a bit (x) from the bin.
4) Read a word from the cover file and write it in stego file.
5) If start and end letter of the word is same, then read the next word of the cover file and write it in the stego file.
6) s = start letter of the word and e = end letter of the word.
7) If x = 0, write s in the stego key.
8) Else if x = 1, write e in the stego key.
9) Repeat steps 3 to 8 till the end of the bin file.
10) Send the stego file and the stego key to the receiver.

B. Seek Algorithm

1) Read a character (c) from the stego key.
2) Read a word from the stego file.
3) If start and end letter of the word is same, then skip that word and read the next word from the stego file.
4) Get the start letter (s) and end letter (e) of the word.
5) If c = s, then bit b = 0.
6) Else if c = e, then bit b = 1.
7) Write b in a file.
8) Execute above steps repeatedly till the end of the stego key.
9) Convert the file into its character equivalent.

This algorithm is supposed to be more efficient as here from the resultant image it is difficult to guess the actual data that is hidden behind it. Application of strong encryption technique is also introducing further security over the hidden data. Again we have followed the zone wise pixel's LSB replacement scheme in the steganography part unlike normal method of data hiding using LSB bit modification. So to unhide the data, a definite heuristic approach is required unlike normal implementation. So, this type of introduction of steganography with cryptography will obviously discern our attempt from the existing one. Again, during the implementation phase we have seen that there is a possibility to hide huge number of characters (approximately 23130) in minimal amount of time which is not present in any kind of existing techniques.

The proposed approach has many applications in hiding and coding messages within standard media, such as audios or videos. Also, the model does not depend on the type of the text that is to be hidden. We can use any type of text (even text of different language) here and to work with it, the corresponding number system has to be chosen (here, we have used ASCII). As future work, we intend to study some more steganalytic techniques for text messages and to extend our model to mobile communication. The following outputs show the proposed method.

INPUT: "THE MESSAGE IS VERY ESSENTIAL FOR INDIAN ARMY."

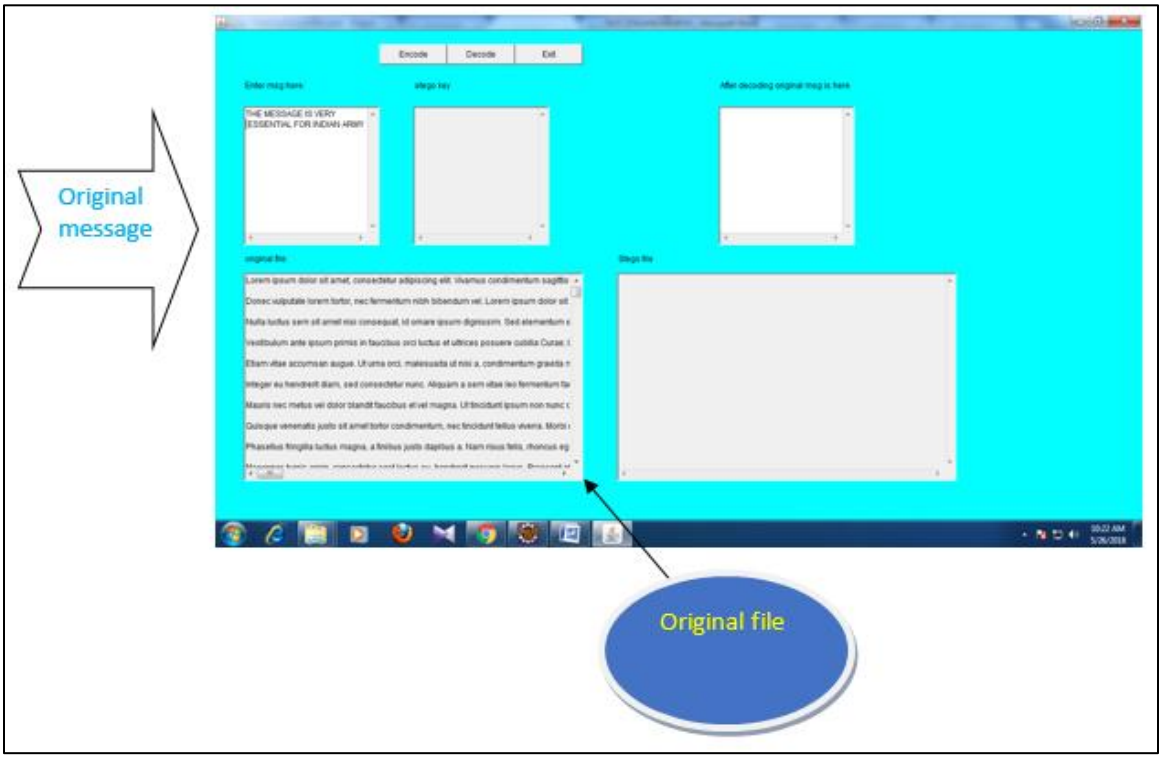

Fig. 1: After Clicking Encode Button Create a Stego Key and Stego File

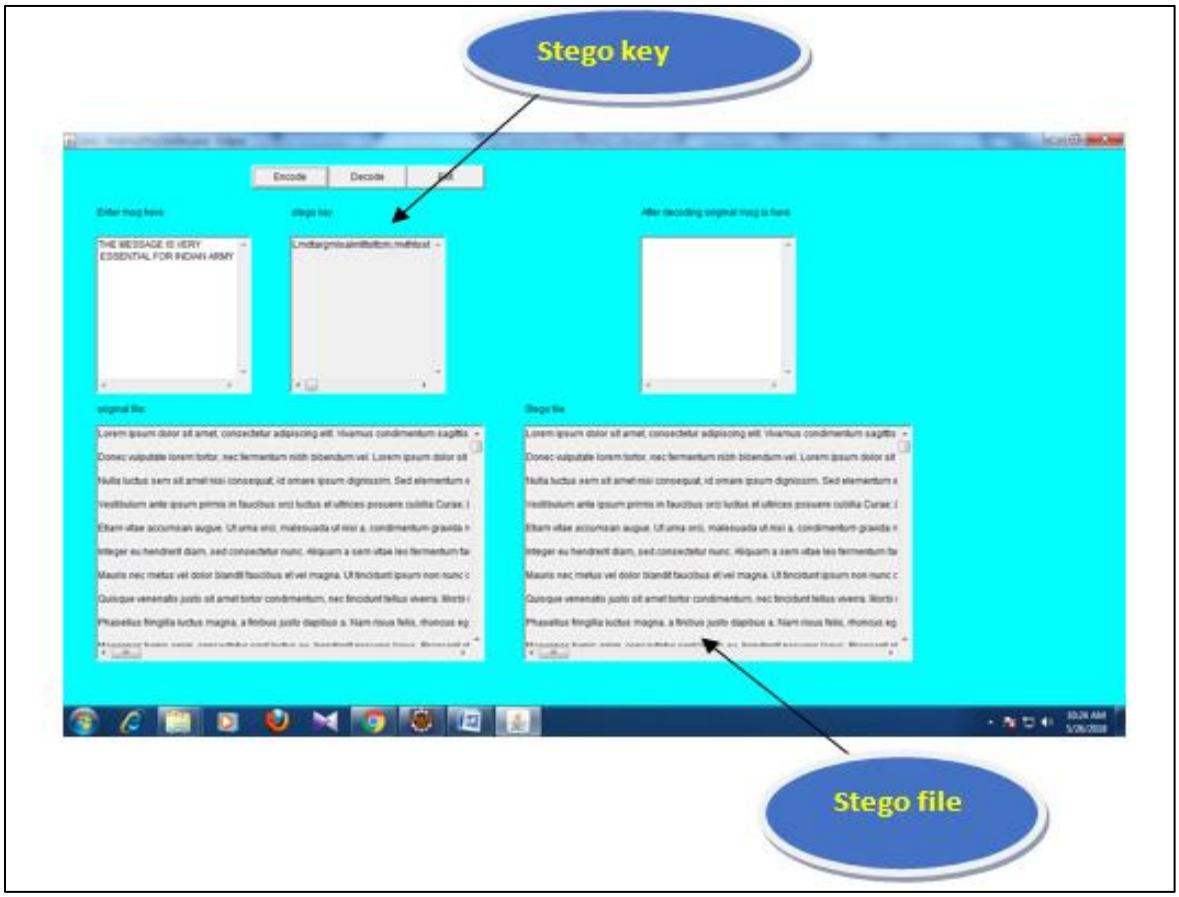

Fig. 2: After Clicking Decode Button Extract Original Messege from Stego File

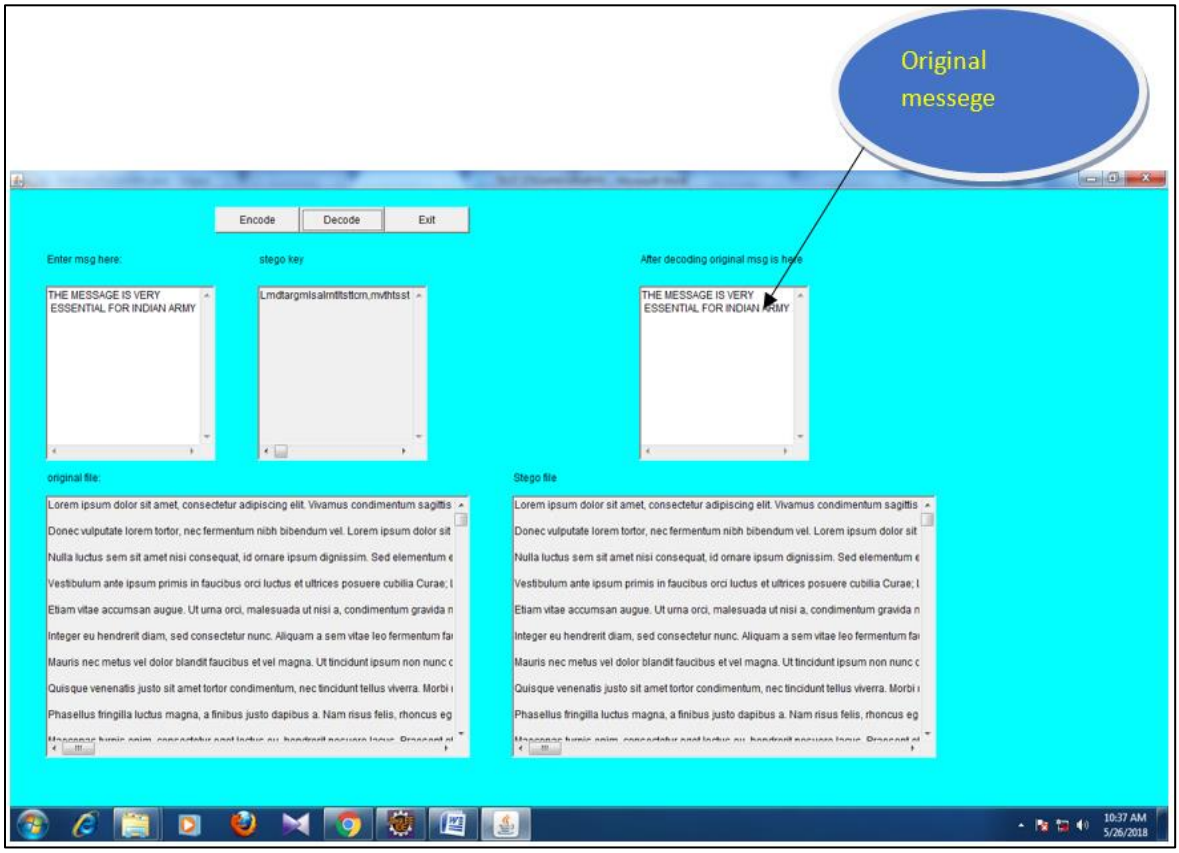

Fig. 3:

IV. CONCLUSION

In this paper, the major importance is given on the secrecy as well as the privacy of information. So, to obtain privacy we have used the concept of cryptography and on the other hand to implement secrecy, we have used steganography. But, again we have felt that the introduction of another level of security layer can make the existing technique a stringent one. Thus with the addition of one layer of security, this model has been designed to obtain the Multilayer data security.

REFERENCES

[1] Johnson, N. F. and Jajodia, S, "Exploring steganography: Seeing the unseen", IEEE Computer Magazine, pp. 26-34, February 1998.
[2] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Tutorial Review on Steganography", IC3 Noida, pp. 106-114, August 2008.
[3] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4, April 2007.
[4] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", IEEE WMMN, pp. 146-151, January 2008.
[5] M. Dobsicek, "Extended steganographic system", 8th International Student Conference on Electrical Engineering, FEE CTU 2004, Poster 04.
[6] Nameer N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science, Page(s): 223 – 232, April 2007.
[7] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Secure Scheme for Image Transformation", IEEE SNPD, pp. 490-493, August 2008.