ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

An Hybrid Approach to Decoding Technique Using Mixed Case Font

Dr.Hemalatha K.L.[1]

Professor, Dept. of ISE, Sri Krishna Institute of Technology, Bengaluru,, Karnataka, India[1]

ABSTRACT: Decoding is often being used together with cryptography and offers an acceptable amount of privacy and security over the communication channel. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. This paper presents an overview of text decoding along with various existing text-based Decoding techniques. A new approach is proposed in information hiding using text file as a carrier for the secret message data in such a manner that the resultant text file attracts no attention and hold the same meaning of the original file. This paper also analyzed the significant drawbacks of each existing method and how our new approach could be recommended as a solution.

KEYWORDS: Decoding,Information hiding, Carrier, Secret message.

I. INTRODUCTION

Decoding, in today's electronic era, is the ability of hiding information in redundant bits of any unremarkable cover media. Its objective is to keep the secret message undetectable without destroying the cover media integrity. Decoding replaces unneeded bits in image, sound and text files with secret data. Instead of protecting data the way encryption does, Decoding hides the very existence of the data. With advancements in digital communication technology and the growth of computer power and storage, the difficulties in ensuring individual's privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another. Various methods have been investigated and developed in information hiding to protect personal privacy.

So how basic Decoding system is developed? When a decoding system is developed, it is important to consider the most appropriate work – it is the medium in which the message is embedded and serves to hide the presence of the message and also how to decode. The cover work with the secretly embedded message produced by the encoder- is to reach its recipient. With the Internet offering of so much functionality, there are many different ways to send messages to people without anyone knowing they exist. For example, it is possible that an image decoded could be sent to a recipient via email. Alternatively it might be posted on a web forum for all to see and the recipient could log onto the forum and download the image to read the message. Ofcourse, although everyone can see the decoded image, they will have no reason to expect that it is anything more than just an image[3].

In terms of development, Decodingis comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end.Fig1.1 shows one example of how Decodingmight be used in practice. Two inputs are required for the embedding process:-

- Secret message: usually a text file that contains the message you want to transfer.
- Cover work: used to construct a stegogramme that contains a secret message, it may be text, image, video clips or sounds.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

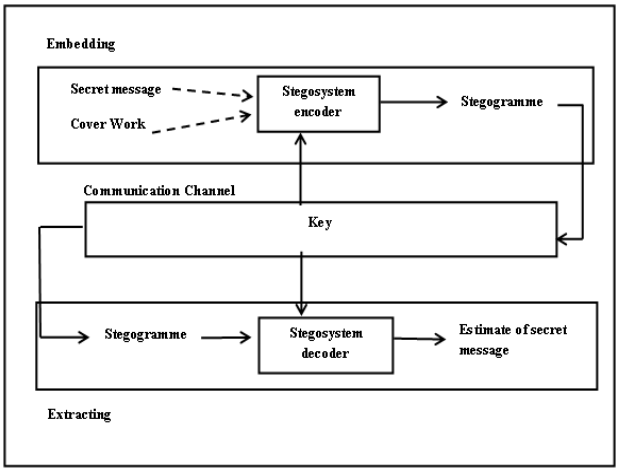

Fig.1.1: Basic Decoding System.

The next step is to pass the inputs through the Stego-system encoder, which will be carefully engineered to embed the message within an exact copy of the cover work such that minimum distortion is made; the lower the distortion, the better the chances of undetectability. The stego-system encoder will usually require a key to operate, and this key would also be used at the extraction phase. This is a security measure designed to protect the secret message. Without a key, it would be possible for someone to correctly extract the message if they managed to get hold of the embedding or extracting algorithms. However, by using a key, it is possible to randomise the way the stegosystem encoder operates, and the same key will need to be used when extracting the message so that the stegosystem decoder knows which process to use. This means that if the algorithm falls into enemy hands, it is extremely unlikely that they will be able to extract the message successfully. The resulting output from the stego-system encoder is the stegogramme, which is designed to be as closeto the cover work as possible, except it will contain the secret message .This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stego-system decoder where an estimate of the secret message is extracted[3].

So,Decodingis concerned with hiding information in some cover medium, by manipulating properties of the medium in such a way that the hidden information is not easily detectable by an observer. Also one of the information hiding technique is categorized into linguistic Decodingandtechnical Decoding.Technical Decodingis explained as carrier rather than a text[1].

Text Decoding

It is the most difficult kind of Decoding.

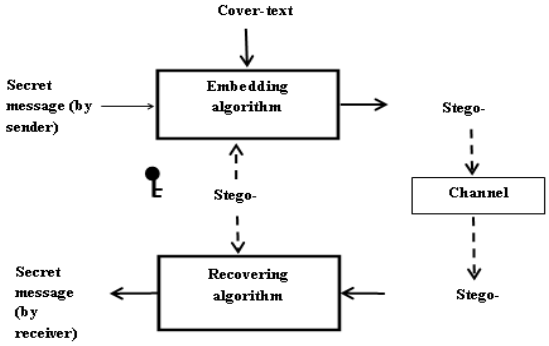

Fig.1.2: The Mechanism of Text Decoding

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Fig.1.2 shows the basic text Decodingmechanism. Firstly, a secret message (or an embedded data) will be concealed in a cover-text by applying an embedding algorithm to produce anstego-text. The stego-text will then be transmitted via communication channel, e.g. internet or mobile device to a receiver. To recover the secret message sent by the sender, the receiver needs to use a recovering algorithm that is parameterised by a stego-key to extract the secret message. A stego-key is used to control the hiding process as well as to restrict detection and/or recovery of the embedded data to parties who know it.

Text Decoding can be classified in three basic categories:-

1. Format-Based.
2. Random and Statistical Generation
3. Linguistic Method

Format-based methods use physical text formatting of text as a place in which to hide information.In [1] Bennett has stated that these format-based methods managed to trick most of the human eyes but it cannot trick once computer systems have been used.

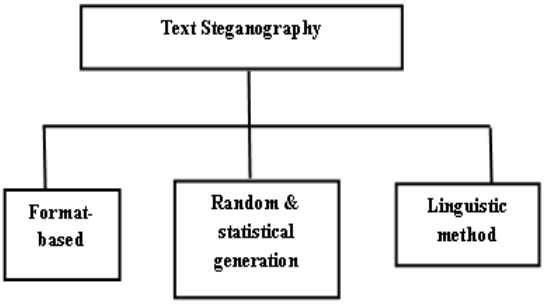

Fig 1.3: Three basic categories of text Decoding

Random and statistical generation is generating cover text according to the statistical properties. This method is based on character sequences and word sequences. The hiding of information within character sequences is embedding the information to be appeared in random sequences of characters. This sequence must appear to be random to anyone who intercepts the message[1].

The final category is linguistic method which specifically considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages. In fact, steganographic data can be hidden within the syntactic structure itself.

Finally it can be said that the goal of Decodingis to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. So, essentially with Decodingthe actual subject message transmission (be that text, sound or image) is untouched but hidden within another source. So,Decodingis a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive.

II. PREVIOUS WORK

Following is a list of work has been done on text Decoding.

In[2] they proposed a new method to hide info in any letters instead of pointed ones only. They used the pointed letters with extension to hold secret bit 'zero'. A very important note is that letter extension doesn't have any affect to the writing content. In fact, this Arabic extension character in electronic typing is considered as a redundant character only for arrangement and format purposes. But the problem in using the extension is that .not all letters can be extended with this extension character due to their position in words and Arabic writing nature. The extension can only be added in locations between connected letters of Arabic text; i.e. extensions cannot be placed after letters at end of words or before letter at beginning. So, whenever a letter cannot have an extension or found intentionally without extension it is considered not holding any secret bits.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

In [3] authors proposed a new approach on hiding information in manipulation of white spaces between words and paragraph. The proposed method was able to provide more capacity for hiding more bits of data into a cover-text. The previous embedding scheme was applied in the space which appears between the words. The major drawback of this method was that it requires a great deal of space to encode few bits. But by combining with inter-paragraph in hiding the secret bits can effectively utilizing most of the white spaces in a text document. So, they used inter-word and inter paragraph spacing for hiding information.
In [4] benefiting from (Gutub and Fattani,2007) Arabic Text Decodingmethod using letter points and extensions and trying to overcome the low capacity aspect, the authors proposed a technique to hide information in a suitable position inside words instead of pointed letters only. These positions are determined to keep the Arabic text beauty if the text is justified and this allows the message to be hidden without affecting the cover text. They insert the extension letter in the determined position to hold secret bit one and leaving the position empty to hold bit zero.

III. EMBEDDING TECHNIQUE USING MIXED CASE FONT

In this section, the proposed method will be presented which hides the secret message within a cover text file.While using the internet and searching for fonts or what so called "cool fonts" that are used for chatting or presentations, it has been found that new type of fonts appeared that type capital and small letters at the same time see figures (3.1, 3.2, 3.3) as example if you typed the word "hardware" the word will be typed like this "HaRdWaRe" sometimes with different sizes for each letter and at other times with same size for whole text. So, it was decided to use this new font with a new text Decodingmethod that holds bits of the secret message.

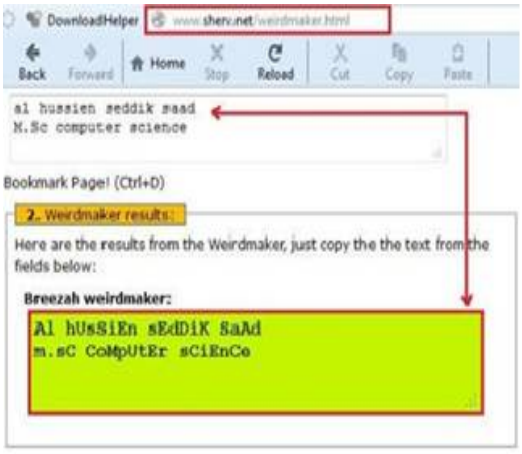

Fig 3.1: Font example 1

Fig 3.2: Font example2

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Fig 3.3:Font example 3

The method works as shown in the following algorithm:
Algorithm: Embedding Using Mixed-Case Font Method
Input: Text File T; Secret Message M.
Output: Stego Text S.
Steps:-

1) Choose a text file T.
2) Divide T into letters, T= {T_1, T_2..,T_n}.
3) Get the secret message M.
4) Convert secret message M into stream of bits b.
5) Divide b into bits, b = {b_1,b_2….b_n}.
6) Select T_i from T and b_i from b.
7) If the b_i is 'one' then change T_i case into capital else change T_i case into small.
8) Repeat steps 6, 7 till thewhole b is hidden.
9) The resultant file will be the stego text S.

IV. CONCLUSION

An approach of text Decodingmethod has been proposed using the letters of the cover file, not using extensions. In the proposed method the letter can be hidden in only 7 letters not 7 words as by using spaces between words. So, it's a large amount of data compared to other methods keeping the exact meaning of the text and make it look like these cool fonts. Finally, this method achieved the goals of Decodingand can be used efficiently.

V. FUTURE WORK

The Future work includes that, in place of calculating the length of secret message, the ASCII values will be generated for each character. So that more number of bits will get generated and it helps us to insert more number of redundant characters in it. This leads to more complexity in finding Hidden Messages. Many image Decoding techniques are only for gray scale images but not applicable for color image. Decoding is a "young", highly multidisciplinary discipline – involving cryptography, image processing, signal processing, information theory.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 7, Special Issue 6, May 2018*

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] L. Y. Por, B. Delina, Information Hiding: A New Approach in Text Decoding, 7th WSEAS International. Conference on Applied Computer and Applied Computational Science (ACACOS `08), Hangzhou, China, April 6-8, 2008.
[2] P. Wayner,"Mimic functions", Cryptologia archive Volume XVI, Issue 3, July 1992, pp.193-214.
[3] P. Bateman, H. G. Schaathun, "Image Decodingand Steganalysis", Department of computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom, 4th August 2008.
[4] J. Watkins, "Decoding– Messages Hidden in Bits, Multimedia Systems Coursework", Department of Electronics and Computer Science, University of Southampton, So171bj, UK, 15th December 2009.
[5] Shahreza M. S and Shahreza M. H. S (2007) ,"Text Steganography in SMS", International Conference on Convergence Information Technology, pp.2260-2265.