International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

A New Approach of Text Steganography Using ASCII Values

Keshav Joshi
Student, Bachelor of Technology in Computer Science
Lovely Professional University, Phagwara, India

***Abstract* -- Steganography is the art of concealing text inside other carriers (i.e. text, image, video or audio) in order to provide data security and confidentiality without any suspicion. In this paper, an implementation of new text steganography method is proposed. The approach based on combining character's ASCII value with the RGB values of a pixel, so that an individual character can be stored into a single pixel. The main purpose of this method is to provide maximum payload capacity, an image can ever have that is the total number of pixels it contains.**

Keywords: Steganography, Iimage Processing, ASCII Value, Inforation Hiding

I. INTRODUCTION

Securing data becomes one of the basic demands of information technology and communication because of the advent of World Wide Web and owing to huge rise in digital networks. Information hiding is one of such powerful techniques used in information security. There are two general approaches Cryptography and Steganography to hide information over network. Cryptography was initially developed and used as a technique for securing the confidentiality of information. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of message secret and the concept responsible for that is Steganography [2]. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "writing" [8]. Steganography is practice of hiding secret message within any media. It can be classified into four categories image, text, audio and video steganography that is depending on the cover media used to embed secret message. Most data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in way that they both are used to protect secret information. If both the techniques: cryptography and steganography is used then the communication becomes double secured [9]. The main difference between Steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of message secret [11].

In terms of development, steganography is 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 two. The extraction process is traditionally a much simple process as it is simply an inverse of the embedding process, where the secret message is revealed at the end. When it comes to security, the algorithmic efficiency plays a vital role. To evaluate the effectiveness of steganography algorithm various evaluation parameters are identified and listed below [7].

- Security: A steganography algorithm is said to be secure if it ensures non-detectability against an attacker who knows the stegno-object but has no information available. The algorithm provides highest level of security if there is no significant difference between original image and resultant image.
- Payload Capacity: It implies the maximum amount of data that can be effectively hidden within a selected medium without causing any visual impairment to the image.
- Imperceptibility: Stegno images are expected to have no visual artifacts. Maintaining the same level of security, higher fidelity of images implies better imperceptibility.
- Runtime Performance: Time complexity plays a vital role in steganography as it evaluates the applicability of algorithm for embedding data into very large images and performance for low resource systems like mobile devices etc.

II. PREVIOUS STUDIES

Text steganography can be classified into three major categories. Firstly, the Format based, which changes the formatting of the cover text to hide data. Secondly, random and statistical generation to avoid comparison with a known plain text, steganographers often resort to generating their own cover text. Lastly, Linguistic methods specially consider linguistic properties of generated and modified text; in this method a pre selected synonyms of words are used [3-5]. Apart from this classification, there are some other techniques which were introduced in this field. One of the oldest methods to hide a message inside a text is to take the first letter of each word. To illustrate this, suppose the following sentence "Fusion is Future and Hiding is trending". By taking the first letter of each word we get the secret message which is 'Secret inside' [9]. Even later, the Germans developed a technique called microdot. Microdots are photographs with the size of a printed period but contain full page information. The microdots where then printed in a letter or on an envelope and being so small, they could be sent unnoticeable [10].

A lot of studies cover text steganography such as:

Gutub A. and M. Fattani. A in [6], "That Benefiting from Shirali-Shahreza [5] proposes a new method to hide information in any letters (Unicode system) instead of pointed ones only". This model uses the pointed letters with extension after the letters to hold secret bit 'one' and the un-pointed Letters with extension to hold secret bit 'zero'.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Shirali-Shahreza, M.H. and M. Shirali-Shahreza [5] deal with the issue of text steganography, their model focuses on the letters that have points on them (example English language had two letters I and J. while Arabic language has 15 pointed letters out of its 28 alphabet letters). Point steganography hides information in the points of the letters specifically in the point's location within the pointed letters. After converting the message into bits, if the bit is one the point in the cover text is shifted up, otherwise, the concerned cover-text character point location remains unchanged

In [8] 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 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.

III. PROPOSED MODEL

In this paper, a new method of text steganography is presented. This approach uses the RGB values of a pixel to store an individual character. Initially, it takes first character of message and divides its corresponding ASCII value into three segments. For example if character is 'A' then its corresponding ASCII value is '65' and after dividing this value into three parts, three numbers are generated that is '0', '6', and '5'.

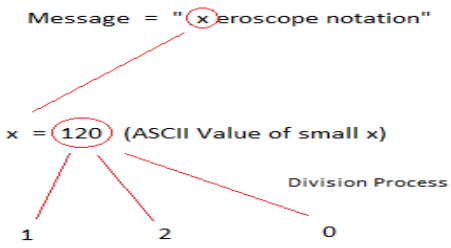

Figure 1: Division of ASCII value

Now there are three numbers that are called as data values for a single character and there are three different rooms available for these values in a pixel that is RGB (Red, Green, and Blue) values. Finally, combine these data values with RGB values in such a way that there is no change in original image. The combining process is elucidated below:

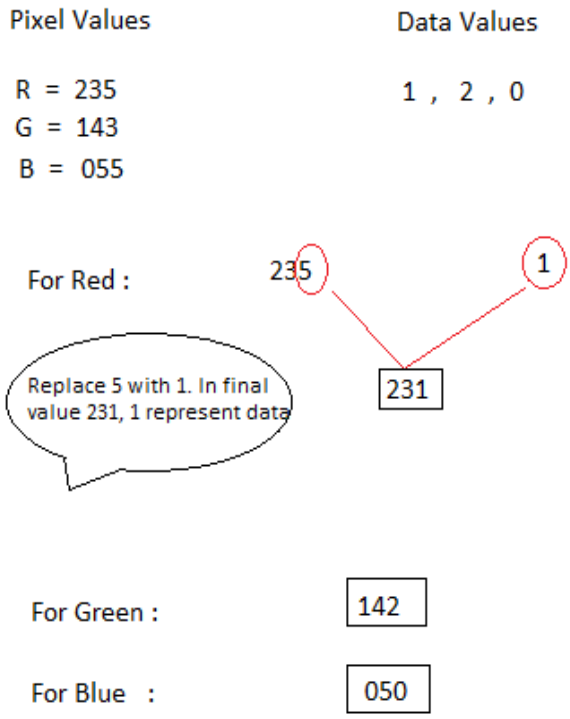

Figure 2: Combining Process

In combining process, last digit of RGB values is replaced with data values and this entire procedure continue working till the last character of message. From efficiency point of view, in worst case, difference in intensity would be 9 pixels and that is totally insignificant to be detectable by human eye. One important point is to be noted that maximum value of RGB, always lies in 240s because above that i.e. in 250s there would be exceptional cases if data values are greater than equal to 6 and this technique does not handle such cases. For example: 258, 259 etc. But there is no difference in intensity of pixels. It always lies within the range of 9 and this provides extra credibility to presented model. The proposed technique totally depends on the value of pixels so it is not applicable on loosy formats like (JPG, JPEG, etc).

Embedding Algorithm

- Read the message to be encrypted in string form.
- Start a loop to the end of message length and read characters from string.
- Convert the character into ASCII value.
- Apply division process on the ASCII value to get three different numbers.
- Combine these data values with RGB values as per combining process.
- Modify the resultant values according to exceptional cases.
- Repeat the process till the loop ends.
- Add end point in image to detect the end of message.
- Algorithm results into Stego image with data embedded in it.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Extracting Algorithm

- Read the Stego image.
- Get the values of red, green and blue from pixel.
- Extract the last digits of red, green and blue.
- Combine the results together to form one number.
- This value represents the ASCII value of character.
- Get character from this value.
- Repeat the process till end point.
- Algorithm results into embedded text from Stego image.

IV. EXPERIMENTAL RESULTS

To demonstrate the working of proposed text steganography technique, it has been implemented on different images. All of the test images are of same size that is 512x512. For a message, all of 255 ASCII characters are used. Unlike other algorithms and techniques, which restrict to certain characters, this method gives the ability to embed almost any letter defined in English language. The quality of the images and effectiveness of the algorithm have been measured using PSNR (Peak signal to noise ratio). PSNR is a standard measurement used in steganography technique in order to test the quality of stego images. The higher the PSNR, the more quality the stego image will have. Below mentioned are some examples of practical implementation of this technique. On left hand side, there are original images i.e. a, c, e and on right hand side these are stego images i.e. b, d, f. More than 10 kb of text is embedded in all the stego images. Clearly, it can be seen that there is very insignificant difference between original and stego images.

Fig (a)

Fig (b)

Fig (c)

Fig (d)

Fig (e)

Fig (f)

Hence it is cogent evidence that this technique doesn't affect the image and provide security and maximum payload capacity. Moreover, the results of PSNR ratio for different images are presented in table (1). With regards to results, the values of PSNR are very decent. In general, payload size of 10 KB with PSNR value 44.0 is very excellent.

Table 1: PSNR (db) for Test Images

Images	PSNR	Payload Size
Image 1	51.62	10 KB
Image 2	51.12	10 KB
Image 3	51.58	10 KB

V. CONCLUSION

The main purpose of this paper is to maximize the payload capacity in text steganography. A new technique has been proposed to conceal text inside images by using pixel values and ASCII values. Combining and dividing processes are the heart of this technique and works exceptionally well. Owing to the importance of pixel values this technique can only be used on lossless formats. Unlike some other methods this proposed model can embed all the 255 ASCII characters. In the end, it can be said that this approach meets the needs of steganography and can be used efficiently.

ACKNOWLEDGMENT

The paper is written under the guidance of my mentor, Roshan Srivastava, who provided insight and expertise that greatly assisted the research. I would like to thank everyone who helped me and motivated me by which the work is made possible.

REFERENCES

[1] Chandramouli R., Kharrazi M., and Memon N., "Image Steganography and Steganalysis: Concepts and Practice", International Workshop on Digital Watermarking (IWDW), Seoul, pp. 35-49, October 2003.

[2] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Methos", Internationl Journal of Computer Applications (IJCA), June 2013.

[3] Isbell, R., 2002, Steganography: hidden menace or hidden saviour. Steganography White Paper.

[4] Agarwal, M., 20135(1) TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON. International Journal of Network Security & Its Applications.

[5] Shirali-Shahreza, M.H. and M. Shirali-Shahreza, 2006, A new approach to Persian/Arabic text steganography. in Computer and Information Science, 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

[6] Gutub, A. and M. Fattani, 2007, A novel Arabic text steganography method using letter points and extensions. in WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria.

[7] Ratnakirti Roy and Suvamoy Changder, "Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach" International Journal of Security and its Applications (IJSIA), vol. 10, no. 4, pp. 179-196,2016.

[8] L. Y. Por, B. Delina, Information Hiding: A New Approach In Text Steganography, 7th WSEAS int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, April 6-8, 2008.

[9] Swain G. and Lanka S. K., "A Quick review of Network Security and Steganography", International Journal of Electronics and Computer Science Engineering, vol. 1, no. 2, pp.426-435, 2012.

[10] Dhanarasi G. and Prasad A. M., "Image Steganography Using Block Complexity Analysis", International Journal of Engineering Science and Technology (IJEST), vol. 4, no.07, pp. 3439- 3445, 2012.

[11] Wang H and Wang S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47, no. 10, 2004.

[12] Manish Trehan and Sumit Mittu, "Steganography and Cryptography Approaches Combined Using Medical Digital Images" International Journal of Engineering Research and Technology, vol. 4, no. 6, 2015.