An Innovative way of Text Steganography with ASCII Values

[1]Arbind Tiwary, [2]Dr. A. K. Gupta, Dr. [3](Prof) Rajesh Kr. Tiwary

[1]Research Scholar, Department of Computer Application, Vinoba Bhave University, Hazaribag, India
[2]Associate Professor, Department of Physics, Vinoba Bhave University, Hazaribag, India
[3] Dean, Deparment of C.S.E., R.V.S. College of Engg.& Tech., Jamshedpur, India

Abstract: Steganography is the skill of obscuring 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, the execution of an innovative text steganography method is proposed. The methodology based on merging the 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, Image Processing, ASCII Value, Information Hiding

I. INTRODUCTION

secure data becomes one of the fundamental requirements of information technology and communication because of the advent of the World Wide Web and owing to the huge rise in digital networks. Information hiding is one of such prevailing techniques used in information protection. There are two broad-spectrum Cryptography and Steganography to hide information over the network. Cryptography was originally developed and used as a method for securing the confidentiality of information. Unluckily, it is occasionally 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 utterance Steganography is of Greek source and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "writing" [8]. Steganography is a 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. the largest part data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in a way that they both are used to protect secret information. If both the techniques: cryptography and steganography are used then the communication becomes double secured [9]. The main distinction 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 provisos of expansion, steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding procedure is worried with conceal a secret message within a cover work and is the most carefully constructed procedure of two. The extraction procedure is usually a much simple procedure as it is simply an inverse of the embedding procedure, where the secret message is discovered at the end. When it comes to security, algorithmic efficiency plays a vital role. To evaluate the effectiveness of the steganography algorithm

Various evaluation parameters are identified and listed below [7].

- Security: The steganography algorithm is thought to be secure if it ensures non-delectability beside an attacker who knows the stegno-object but has no information available. The algorithm provides the highest level of security if there is no significant difference between the original image and the 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. making the same level of security, superior reliability of images implies better imperceptibility.
- Runtime Performance: instant complication plays a crucial role in steganography as it evaluates the applicability of the algorithm for embedding data into very large images and performance for low resource systems like mobile devices etc.

II. PREVIOUS STUDIES

Text Text steganography can be divided into three main categories. Initially, the layout based, which changes the formatting of the conceal text to hide data. Secondly, random and statistical generation to avoid assessment with a known plain text, steganographers often option to generating their own wrap text. Lastly, Linguistic methods particularly consider linguistic properties of generated and customized text; in this method, pre-selected synonyms of words are used [3-5]. Apart from this arrangement, 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 show this, assume the subsequent 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 image with the dimension of a printed period but contain full-page information. Further, the microdots were then expressed in a letter or on an envelope and being so tiny, they could be sent barely discernible [10].

A set of studies cover text steganography such as:

Shirali-Shahreza, M.H. and M. Shirali-Shahreza [5] agreement with the concern of text steganography, their representation focuses on the letters that have points on them (example the English language had two letters P and O. In Arabic language have 15 major letters out of its 28 alphabet letters). The Point steganography conceals information in the points of the letters exclusively in the point's location within the pointed letters. Subsequent to changing the message into bits, if the bit is one the point in the wrap text is shifted up, otherwise, the concerned cover-text character point location remains unchanged.

Gutub A. and M. Fattani. A in [6], "this gets benefited from Shirali-Shahreza [5] obtainable a new scheme to conceal information in any letters (Unicode system) as an alternative of pointed ones only". This model uses the pointed letters with conservatory after the letters to hold secret bit 'one' and the un-pointed Letters with extension to hold secret bit 'zero'.

In [8] Authors proposed a novel approach on hiding information in the manipulation of white spaces between words and paragraph. The proposed technique was capable to offer more capacity for hiding more bits of data into a cover-text. The main negative aspect of this method was that it requires a great deal of space to encode a few bits. But by integrating with inter-paragraph in conceal the secret bits can efficiently utilize most of the white spaces in a text document. Therefore, they used inter-word and inter-paragraph spacing for concealing information.

III. PROPOSED MODEL

In this paper, a new way of text steganography is showed. This comes within reach of uses the RGB values of a pixel to store an individual character. to begin with, it takes the first character of a message and divides its corresponding ASCII value into three segments. For example, if the character is 'D' then its corresponding ASCII value is '68' and after dividing this value into three parts, three numbers are generated that is '0', '6', and '8'.

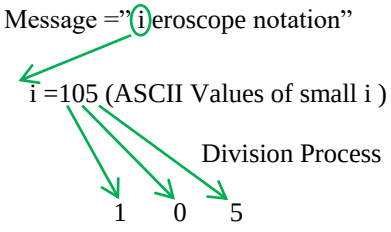

Figure 1: Division of ASCII value

Now there are three numbers that are called as data values for a single character and there are three dissimilar rooms accessible for these values in a pixel that is RGB (Red, Green, and Blue) values. in conclusion, merge these data values with RGB values in such a mode that there is no alter in original image. The combining process is elucidated below:

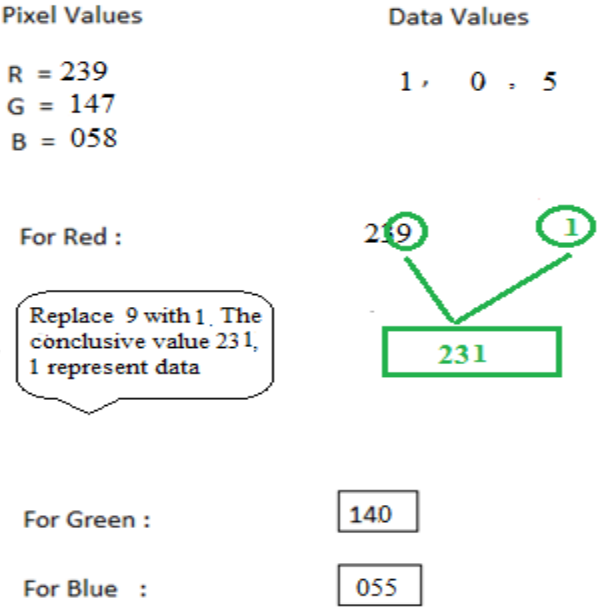

Figure 2: Combining Process

In joining procedure, the last digit of RGB values is changed with data values and this complete procedure continue working till the last character of the message. From an effectiveness point of view, in the worst case, dissimilarity in intensity would be 9 pixels and that is totally insignificant to be detectable by the human eye. One significant point is to be noted that greatest value of RGB, always lies in 240s because above that i.e. in 250s there would be extraordinary cases if data values are greater than equal to 6 and this method does not control such cases. For example: 258, 259 etc. But there is no dissimilarity in a concentration of pixels. It always lies within the range of 9 and this provides additional trustworthiness to presented model. The proposed method completely depends on the value of pixels so it is not applicable to lossy formats like (JPG, JPEG, etc).

Embedding Algorithm

- The message is encrypted in string form, first read it.
- Start a loop to the end of message length and read characters from the string.
- Convert the character into ASCII value.
- Affect the division process on the ASCII value to get three different numbers.
- Combine these data values with RGB values as per the combining process.
- amend the consequential values according to special cases.
- Repeat the process until the loop ends.
- Add an endpoint in the image to detect the end of the message.
- Algorithm results in Stego image with data embedded in it.

Extracting Algorithm

- Stego image to be read.
- obtain the values of red, green and blue from a pixel.
- pull out the last digits of red, green and blue.
- unite the results together to form one number.
- This value expressed the ASCII value of character.
- Obtain character from this value.
- Repeat the process till endpoint.
- Algorithm outcome into the embedded text from Stego image.

IV. EXPERIMENTAL RESULTS

To exhibit the functioning of projected text steganography method, it has been implemented on diverse images. All of the experiment images are of the same size that is 512x512. In a message, all of 255 ASCII characters are used. disparate other algorithms and techniques, which limit to certain characters, this technique gives the facility to embed almost any letter define in the English language. The superiority of the images and efficiency of the algorithm have been calculated using PSNR (Peak Signal to noise ratio). PSNR is general merriment used in steganography technique in order to test the quality of stego images. The upper of the PSNR, the more quality the stego image will have. Below mentioned are some examples of practical implementation of this technique. On the left-hand side, there are original images i.e. a, c, e and on the right-hand side these are stego images i.e. b, d, f. additional 10 kb of text is embedded in all the stego images. Clearly, it can be seen that there is a very insignificant difference between original and stego images.

Fig (a)

Fig (b)

Fig (c)

Fig (d)

Fig (e) Fig (f)

therefore it is convincing evidence that this method doesn't influence the image and provide protection and utmost payload capacity. Moreover, the outcome of PSNR ratio for different images are showed in table (1). With regards to outcome, the values of PSNR are very decent. In broad, 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	50.63	10 KB
Image 2	51.11	10 KB
Image 3	51.48	10 KB

V. CONCLUSION

The major intention of this paper is to take advantage of the payload capacity in text steganography. An innovative technique has been projected to obscure text inside images by using pixel values and ASCII values. Merging and dividing processes are the heart of this method and works extraordinarily well. due to the significance of pixel values, this method can only be used on lossless formats. disparate some other methods this projected model can embed all the 255 ASCII characters. In conclusion, it can be said that this move meets the needs of steganography and can be used professionally.

VI. REFERENCES

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

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

[3] Chandramouli R., Kharrazi M., and Memon N., “Image Steganography and Steganalysis: Concepts and Practice”, International Workshop onDigital Watermarking (IWDW), Seoul, pp. 35-49, October 2003.

[4] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Methos", International Journal of ComputerApplications (IJCA), June 2013.

[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.

[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.