A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency

Ms. Neha Shrivastava[1], Assistant Prof. Mr. Toran Verma[2]

Abstract— **Data Security is one among the foremost necessary challenges being faced by every kind of organizations. Several companies have explored that however vital is that the information to urge success in their business or operations and extremely few have managed to adopt effective measures to create their information secure, avoiding unauthorized access, preventing intrusions, stopping secret information revelation, etc**.

In this proposed technique, the sender is hiding the data which is to sent to the receiver in the form of images. The image is a mixture of the text which is derived from the two techniques of the text steganography which has been derived earlier. The two techniques used are Reflection Symmetry and the Vedic Numeric method. The sender sends the data into partitioned form or we can say the data which is sent by the sender is partitioned into 2 parts and separate-separate part is sent to the two techniques. We are doing this as if the whole text is sent to one technique or vedic technique it will consume more memory. So, the text after being processed by the two techniques is joined to form a whole text and then the text is converted into image by the various methods or algorithms ex.LSB, matrix multiplication. Thus , the text is converted into image that is sent to the receiver.

The advantage of the proposed technique is that, since we are hiding the data without changing the structure of the file and by creating the summery of a publicly available text like newspaper article, therefore it will draw less attention to the unintended recipients and hence more security is added to the proposed steganographic system.

Index Terms— ***steganography;unauthorized;intrusions***

I. INTRODUCTION

Image processing is a methodology to convert an image into digital kind and perform some operations on that, so as to urge enhanced image or to extract some helpful information from it. It's a kind of signal dispensation during which input is image like video frame or photograph and output could also be image or characteristics related to that image. Typically Image process system includes treating images as dimensional signals whereas applying already set signal process strategies to them. It is among speedily growing technologies nowadays, with its applications in varied aspects of a business. Image process forms core analysis space among engineering and applied science disciplines too. Image process primarily includes the subsequent 3 steps:

1. Importing the image with optical scanner or by photography.

2. Analyzing and manipulating the image which incorporates information compression and image improvement and recognizing patterns that aren't to human eyes like satellite pictures.

3. Output is that the last stage within which result are often altered image or report that's supported image analysis.

A. Steganography

Steganography means that lined or hidden writing. The principle of steganography is secret communication to cover a message from Associate in Nursing mediator. This differs from cryptography, the art of secret writing, that is meant to create a message indecipherable by Associate in Nursing inadvertent receiver however doesn't hide the existence of the key communication.
Although steganography and cryptography are different and distinct, these two can be treated as twin sisters of secret communications.

B. Text steganography

Text steganography uses text as a cover media for hiding message. Message can be hidden by shifting word and line [4, 8], in the open spaces [5], in word sequence [6]. Properties of a sentence such as number of words, number of characters, number of vowels, position of a vowel in a word are also used to hide secret message. The advantage of preferring text steganography over other steganographic technique is its smaller memory requirement and simpler communication [14]. But due to lack of large scale redundancy of information in text file, in compared to other medias , text steganography seems to be most difficult kind of steganography [12].

Manuscript received March 2015
*Ms. **Neha Shrivastava**, Computer Science & Engineering, RCET Bhilai Bhilai, India, 7828344313*
***Assistant Prof Toran Verma**, Information technology,,RCET Bhilai, India, 9770404044*

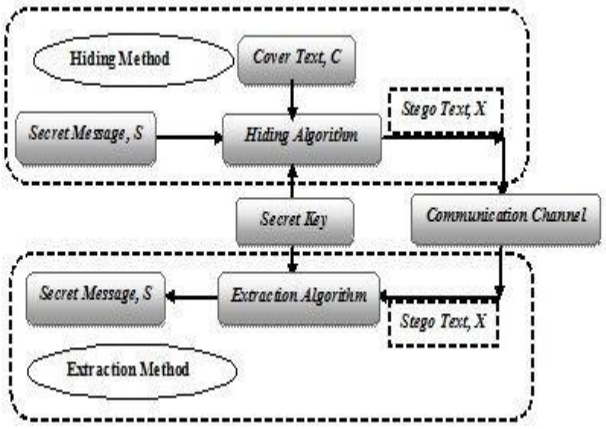


Fig1: General Model for Text Steganography

If a steganography methodology causes somebody to suspect that there is secret info during a carrier medium, then the tactic has failing [10].The first written proof concerning steganography being employed to send messages is that the Heredotous[17] story concerning slaves and their smooth shaven heads. The modern illustration of steganography are often given in terms of the prisoner's downside[13]. Specifically within the general model for Steganography, illustrated in Fig1.Let Nick want to send a secret message S to Ricky. In order to do so, Nick embeds S into a cover-object C to get the stego-object Ć. The stego-object Ć is then sent through the public channel. During a pure Steganography framework, the technique for embedding the message is unknown to Wendy and shared as a secret between Nick and Ricky. However, it's typically not thought of pretty much as good follow to rely on the secrecy of the formula itself in camera key Steganography Nick and Ricky share a secret key that is used to engraft the message.

C. Image Steganography

Image steganography has been a colossal space of analysis for several years currently. It's a method that hides the key image behind the duvet image in such the way that the presence of the key image is fastened and also the cover image seems to be constant In such the way, the digital information will be embedded and transferred to the destination with minimum risk of detect- ability. The construct of undetectability has raised the requirement of steganography all told dimensions like commerce, national security services, and banking and alternatives personalcommunication-areas.
Alternative information activity strategies like cryptography, watermarking and digital signature differs from the steganography construct as steganography permits the communication to be hidden and conjointly, provides higher quality of the key image .
Below fig: explains the various effects of steganography and water-marking and also how the stego-image is produced with the help of combination of cover image and secret image and how secret image is formed with the help of stego- image and various operations performed on it.

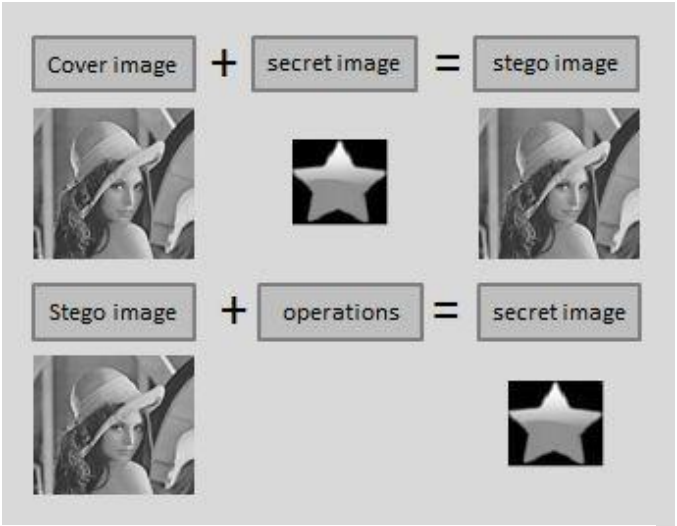


Fig2: Formation of stego-image and secret-image.

II. BACKGROUND

Related Works on Text Steganography

A. Syntactical Steganography

Considering the syntactic structures of a text, the syntactical steganography approach build syntactically correct sentences by using the Context Free Grammars (CFG). CFG based Mimicry[11] comes under this category of NICETEXT[16] uses the cover text as a source of syntactic patterns and by running the cover text through a part-of-speech tagger; this algorithm obtains a set of "sentence frames," e.g. [(noun) (verb) (prep) (det) (noun)] for 'I saw in the Hall'. Then by using the dictionary, a large list of (type, word) pairs where the type may be based on the part-of-speech tagger or its synonyms, the system randomly generate sequence of words to form a sentence.
Though, NICETEXT produces syntactically correct sentences, the output text is almost always set of ungrammatical and semantically anomalous sentences. Using this disadvantage of NICETEXT steganalysis algorithms have been developed to detect the presence of hidden information in the cover file generated by NICETEXT.

B. Lexical Steganography

In lexical Steganography,Wayner, has proposed that lexical units of natural language text such as words are used to hide secret bits. During this approach a word may well be replaced by its word and therefore the selection of word to be chosen from the list of synonyms would depend on secret bits. as an example take into account a sentence – Diana may be a sensible woman. If sensible represent 00 then in line with the input bits 01, 10, eleven we will replace the word good by nice, pleasant and kind respectively to hide the bits.

A. Ontological Technique

In this methodology, to imbed information, rather than implicitly departure linguistics intact by replacement solely

substitutable words an exact mode which means is employ-ed to judge equivalence between texts. This methodology is additionally having identical disadvantage like NICETEXT that generally it should turn out semantically incorrect texts.

D. Other Steganography Approaches

In Text Steganography by concealing information in specific Character of Words approach [20], specific characters from some explicit words area unit hand-picked to cover the data. For instance, the primary character of each various word hides the key message. Text Steganography by Line Shifting methodology [15,18] is another helpful approach wherever lines area unit shifted vertically to some extent. For instance, lines area unit shifted vertically to degree say α or – α. For α, the data is one and for – α, the data is zero. This methodology is suitable for written text. Information is hidden by making Spam Texts [2] in a very HTML file. This approach uses the pliability of HTML concerning case-sensitiveness. By Word Shifting method- ology [3] info is hidden within the text by shifting words horizontally and by dynamic the gap between the words. Feature committal to writing methodology changes the feature or structure of the text to cover information. For instance, happiness or shortening finish portion of some characters, or by vertical displacement of points of characters like 'i', 'j' etc. during this this methodology an oversized volume of knowledge is hidden within the text. By adding Open areas methodology the data is hidden by adding additional white areas within the text.
Besides of these, some algorithms for text steganography through Indian Languages are planned by victimization feature committal to writing technique and dynamic programming technique Some a lot of approaches in text steganography space has additionally been developed, that scans the letters in English alphabets and analyses their shapes for activity secret knowledge Some approaches are there that checks the properties of sentences and counting on that hides secret knowledge.

By victimization the properties of a sentence and therefore the presence of redundant feature code in a position characters in Indian Languages, a message is hidden into AN innocent cover file containing Indian texts. Victim-ization the existence of too several points in Persian and Arabic phases, data is hidden within the Persian and Arabic texts Hindi letters and its diacritics and numerical code square measure utilized in for activity message into Hindi text. Generating a random sequence of characters or words, specific data typically will hidden in sequence however it often ends up in senseless words sentence that is at risk of raise suspicion. In technique some specific characters from bound words, placed in bound sequence in sentence ,square measure used as spot for secret message however the strategy is time overwhelming and takes plenty of mental power. By inserting punctuation signs in specific places, information is hidden but information hiding capacity of the method is low. Using synonym of certain words in a sentence, information can be hidden By altering the features of a text information is hidden in text.

III. RECENT WORKS IN IMAGE STEGANOGRAPHY FOR IMPROVING FREQUENCY

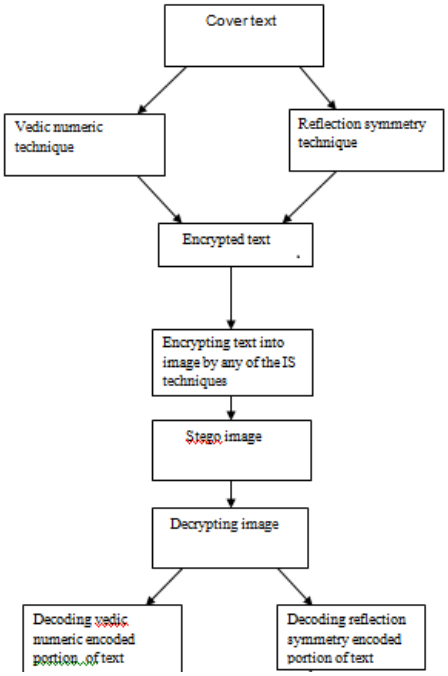
The novel approach for text steganography proposed by[1] generating the summery of a text file that contains English language text. The projected methodology takes as input a publically obtainable text and therefore the secret message. The secret message is hidden by following the reflection symmetry properties of the characters of English alphabets on the axis of reflection. As an output of the system, outline is generated from the chosen input text which outline is our cover text, to be sent to the receiving finish. At the receiving finish reckoning on an equivalent properties of a people alphabets, several secret bits from the quilt text are extracted tourge back thefirst message.
The purpose of steganography is covert communication to cover the existence of a message from the prying eyes. Digital. However, mistreatment text because the target medium is comparatively troublesome as compared to the opposite target media, owing to the shortage of accessible redundant data during a computer file. This paper presents associate degree approach for text steganography through a method that uses reflection symmetry of a people alphabets.
To cover secret information bits, the projected methodology checks the vertical and horizontal reflection symmetry properties of the characters gift in every sentence of the text and, if followed, it selects the sentence to get an outline of the text, referred to as cover text or stego text. Equally at the extraction finish, the receiver checks for the reflection symmetry properties followed by the characters gift within the sentences of the stego text and places the corresponding bits to urge the key message from the outline generated by the concealment method.
The projected methodology exhibits satisfactory experiment-al result with the quilt text chosen from totally different daily newspapers.

A text based steganography technique [19] has proposed that different approach to the English text based steganography with Indian root. In the propose methodology, no properties of a sentence are used rather characteristics of land language is employed. This provides flexibility and freedom from the purpose read of the sentence construction however it will increase machine complexness.
This paper presents a text primarily based steganography technique supported the religious text Numeric Code. Frequency of the letters in English alphabet in conjunction with religious text Numeric Code are used for the steganography technique. No separate importance is given for vowels and consonants.

IV. PROPOSED METHODOLOGY

Many ideas come from different papers which works on the text steganography. This paper describes a method in which the sender has to convert text into images and then the encrypted file is sent to the receiver and the receiver has to decrypt that in order to extract the secret message or the data which is hided. In this paper we will combine the two techniques of Reflection symmetry and the Vedic Numeric Method and by using these two we are getting the data to be converted into image.

Figure 3.1 shows the diagrammatic view of proposed methodology.



In the Reflection symmetry method, the process of generating the summary is dependent on the reflection symmetry property of English alphabets and according to that, they are grouped into different sets, where each set represents a pair of bits.In this we are classifying on the basis of groups which are based on Bisection of the letters along Horizontal Axis of Symmetry and Bisection of the letters along Vertical Axis of Symmetry and also groups based on both horizontal and vertical axis of symmetry.

In the vedic numeric method, Some of the outstanding characteristics, inflexion, fixed word order and use of periphrases, of the English language are used for the steganography technique.

Inflexion means that it can indicate the relationship of the words into a sentence with a minimum change of shape. In fixed order, the place of each word in a sentence decides it relationship with the others. Periphrases are the different ways to express something. Sri Bharati Krishna Tirthaji in [9] described a particular code called Vedic Numerical Code used in deciphering Sanskrit text. The coding is based on the tongue position. For applying the Vedic code to the English alphabet, frequency of letters in English vocabulary [7] is used as the basis of assigning numbers to the letters in the English alphabet. No discrimination is made for assigning coding number to vowels and consonants as compared to [21].In the fig. shown above, we are taking a cover text which is undergoing or we can say we are dividing that text into two equal parts, half of the text we are sending to the vedic numeric method and half we are sending to the reflection symmetry technique. After the text is processed by both the techniques then an encrypted text is formed. The encrypted text is then converted into image by any of the algorithms or IS techniques.

The encrypted text is then hided under an image which we call as stego-image and send it to the receiver. The receiver then decrypts the image and decode half of the portion of the text by vedic numeric method and half of the portion by reflection symmetry method. By decoding,the receiver finds the desired text. By using these two methods, data will be very secure and also it provides memory consumption.

In this proposed technique, the sender is hiding the data which is sent to the receiver in the form of images. The image is a mixture of the text which is derived from the two techniques of the text steganography which has been derived earlier. The two techniques used are Reflection Symmetry and the Vedic Numeric method. The sender sends the data into partitioned form or we can say the data which is sent by the sender is partitioned into 2 parts and separate-separate part is sent to the two techniques. We are doing this as if the whole text is sent to one technique or vedic technique it will consume more memory. So, the text after being processed by the two techniques is joined to form a whole text and then the text is converted into image by the various methods or algorithms ex. LSB, matrix multiplication. Thus the text is converted into image that is sent to the receiver.

V. CONCLUSION

By using the hybrid approach that involves the combination of Vedic Numeric approach and Reflection Symmetry approach we are able to cover out the disadvantages that incur in following both the methods separately for a simple text to be hidden. Moreover, it provides better security and creates less chances of attenuation of the image to be sent to the receiver in the transmission channel.

1. It also reduces the memory consumption while performing the above two techniques separately.

2. The proposed text steganography technique can provide a two layer of authentication and security system in physical and online banking as well as online shopping.

The advantage of the proposed technique is that, since we are hiding the data without changing the structure of the file and by creating the summery of a publicly available text like newspaper article, therefore it will draw less attention to the unintended recipients and hence more security is added to the proposed steganographic system. Also, as there is no restriction to the size of the text file, we can hide a large volume of data using the proposed algorithm. In case of mobile banking, transaction can be made via SMS securely using the proposed techniques.

REFERENCES

[1] Anandaprova Majumdera,*, Suvamoy Changderba Department of Computer Science &Engineering, Dr. B. C. Roy Engineering College, Durgapur, India Department of Computer Applications, National Institute of Technology, Durgapur, India International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA) 2013

[2] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report 2004-13

[3] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), 2003, pp. 775–779.

[4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images", Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, 1995.

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, 1996.

[6] K. Bennet, "Linguistic Steganography Survey, Analysis, and Robustness Concerns for Hiding information in Text", Purdue University, Cerias Tech Report 2004—2013.

[7] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension", Motilal Bansari Publishers, 1992.

[8] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", Proceedings of IEEE INFOCOM'94,vol.3, pp. 1278-1287,Toronto, June 1994.

[9] Kalavathi Alla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography", Proceding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.

[10] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-Jun 2001.

[11] P. Wayner, "Mimic functions", Cryptologia XVI, pp. 193–214, July 1992.

[12] J.T. Brassil, S. Low, N.F. Maxemchuk, and L.O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, vol.13, Issue. 8, pp. 1495-1504, October 1995.

[13] G. Simmons, "The prisoners problem and the subliminal channel," CRYPTO, pp.51–67, 1983.

[14] J.C. Judge, "Steganography: Past, Present, Future", SANS Institute, November 30, 2001.

[15] S.H. Low, N.F. Maxemchuk, J.T. Brassil, and L.O'Gorman, "Document marking and identification using both line and word shifting", Proceedings of the Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '95), 2-6 Apri,1995,vol.2, pp. 853 – 860.

[16] M. T. Chapman, "Hiding the hidden: A software system for concealing ciphertext as innocuous text", Master's thesis, University of Wisconsin-Milwaukee, May 1997.

[17] Herodotus. The Histories. Penguin Books, London, 1996. Translated by Aubrey de Sélincourt

[18] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", Proceedings of SPIE – Volume 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp. 685-695.

[19] A Text based Steganography Technique with Indian Root Souvik Roya,*, P.Venkateswaranba Jadavpur University, India bJadavpur University, IndiaInternational Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013

[20] T.Moerland,"Steganography and Steganalysis", May 15, 2003, www.liacs.nl/home/tmoerlan/privtech.pdf.

[21]http://oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english.

About Authors:

Ms.Neha Shrivastava received the B.E. degree from Chhattigarh Swami Vivekanand Technical University, Bhilai (C.G.) India in Computer Science & Engineering with Honors in the year 2013. She is currently pursuing M.Tech. Degree in Computer Science Engineering with specialization in Computer Science & Engineering from CSVTU Bhilai (C.G.), India. Her research area includes Image Processing.

Mr. Toran Verma is currently Assistant professor in Department of Information Technology RCET, Bhilai (C.G.) India. He completed his B.E.,M.Tech and Ph.D. in Computer Science and Engineering Branch. His research area includes Neural Network, computer Network, Image processing etc. She has published many Research Papers in various reputed National & International Journals, Conferences, and Seminars.

