A Review for Text Steganography Techniques for WSN

Reetika Sodhi
Department of Electronics and
Communication Engineering
Gharuan, Mohali, Punjab,
India-140413

ABSTRACT
In today's digitised era almost all data is transferred digitally which is very easy and advantageous but it also has some shortcomings i.e. the security of this data is very important. So different techniques such as steganography and cryptography are used to ensure security of data being sent over a medium. In steganography, the secret data is concealed within an object known as cover media which can be an image, audio/video, text so that the existence of any hidden data is not known to the third party or anyone who is not the intended receiver of that data. So in this paper discussion on some text steganography techniques is done with their merits and demerits.

Keywords
WSN, Steganography, Cryptography.

1. INTRODUCTION
As the internet has transformed our lives in numerous constructive means, but cyber safekeeping is a major problem faced these days. Security over web is a universal label for concealing data for communication on internet. So there is a need to protect the data transmitted over the web, and steganography is one of the many techniques to hide the personal and trustworthy data.

This word "steganography" is coined from Greek term "stegano" meaning "covered" and "graphy" means "writing"[13].

Steganography deals with hiding data inside an object referred to as cover object which can be an image, audio/video, or text. The data is concealed by such an approach that the attacker is not aware of if any data is hidden or not. Cryptography is also a data hiding technique but the main difference in cryptography and steganography is that steganography deals in making the existence of hidden data invisible while in cryptography the third person knows that data is hidden but it is in encrypted form.

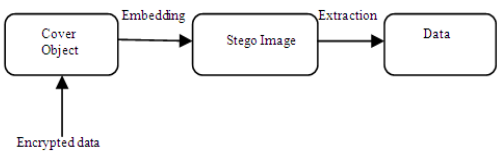

Fig 1: Steganography process

A latest and different evolving technique which consist of an enormous amount of tiny nodes or devices used for observing changes, making procedure to sort it out and then transmitting information to interact with the actual world is termed as wireless sensor networks i.e. nodes which are wirelessly connected to each other in an environment[10].

The information in WSN are transmitted through RF(radio frequency) connection so the errors may get generated due to many factors such as intervention, alterations etc. [2].

These nodes communicate and transfer information between them. Sensors used by these nodes are of many kinds which are used for observing and examining the changes in temperature, passage of traffic, detection of specific entity, speed with which a body is moving its direction ,pressure conditions etc. are seismic, thermal, infrared, acoustic and radar.

So providing security to data which is transferring between these nodes is concern in wireless nodes and all steganography and cryptography algorithms cannot be used directly for wireless sensor nodes because WSN are resource limited due to restrained power supply, battery life, area of network [11].

The restrictions and limitations of WSN such as limited power, limited processing requirement, low battery life and challenging distribution of nodes makes it tougher as compared to the traditional network systems, but the ability to design safety solutions into these networks from beginning as they are in their initial research phase. Moreover, the size, physical qualities of location can be used. Eventually, the distinctive attributes of wireless sensor nature permit the new and innovative securities which are not accessible in traditional systems [5]. The review paper is arranged in a particular pattern as described: Section II indicates different types of cover objects to be used for embedding secret data. Section III describes basic requirements for security algorithms. Section IV presents related work for text steganography techniques. Section V defines parameters for quality evaluation. In Section VI conclusion is attained.

2. DIFFERENT TYPES OF COVER OBJECT
In steganography the message is hided in wrapping object caller "cover object" which can be either text, image, audio/video or protocol [1].In text a successive chain of numerals is transmitted which is known as key and it describes the subsequent position of secret message (e.g. letters)in the cover text. The image is defined as the arrangement of numbers which characterises different strength of light at distinct pixels .The changes in values of pixels is resultant from RGB (red, green, blue) which are considered to be primary colours. Every primary colour signifies 1 byte. Usually size of images in which data is to be stored is either 8 or 24 bit, large size is generally not been used as it will draw attentiveness of intruder while the file is being transmitted [5]. Audio files make use of masking method which takes advantage of the human hearing system properties.

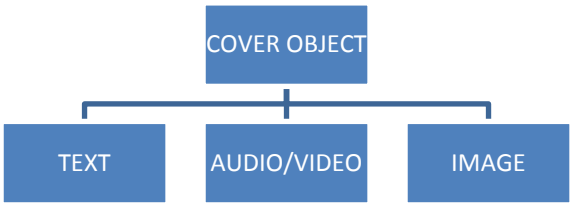

Fig 2: Types of cover object

Another cover object can be protocol in which confidential information can be hided in the network based protocols like TCP/IP datagram header; padding bits; fields that are reserved or not used can be chosen for hiding data.

3. BASIC REQUIREMENTS FOR SECURITY ALGORITHMS

To communicate data between a wireless networks one should make sure that data must be delivered with secrecy i.e. no intruder can manipulate the data between the transmitting node and receiving node. So there are certain requirements which are discussed below as:

3.1 Confidentiality

It is a significant matter in securing data in networks. Confidentiality defines that the data is not seen or accessed by any attacker or intruder [2].

E.g. in a particular network if some nodes are distributed in a particular area to destroy or fetch information from the original nodes then confidentiality here means that the malicious nodes cannot retrieve information from the original nodes.

3.2 Authenticity

It defines that the data must not be manipulated by the third party i.e. the secret data must remain original when received at receiver. Secret keys and passwords which are only known to user are used to maintain authentication of data.

3.3 Integrity

It depends on the truthfulness of sources from which data is derived. It defines that data must not be altered by any activity such as malicious node or any data hacking process and it also signifies that data must be received from a reliable source [2].

3.4 Non-repudiation

It means that the data must be received only by the person or parties who are intended to receive it and not to any other receiver.

3.5 Embedding Capacity

Capacity defines how much data is made to concealed in a cover image that can be send over a communication channel i.e. on how many locations the message can be hided so steganography algorithm must have high embedding capacity.

3.6 Robustness

It is defined as the degree of manipulations in cover media e.g. crop, rotation etc. that the steganogram can tolerate without variation or change in secret message and it should not provide any clue to make it statistical significant [11].

3.7 Hiddenness

Steganography itself implies that the existence of hidden message in cover image is made secret i.e. the unintentional person is not able to sense out where the data is been concealed. So invisibility is the main and initial prerequisite for any steganography technique and must be accomplished.

4. RELATED WORK

There a large number of algorithms for text steganography. In text steganography the cover object is a text or data in which another text or data is concealed in the string of numbers by controlling or changing the numbers or ith letter of a word. There are different methods to hide data by using text as cover media such as semantic method, linguistic method, abbreviation method, word spelling method etc. Here are some algorithms used for text steganography.

P.Uddin et.al. proposed a method for text steganography which uses DES as the algorithm to first encrypt the data to be transmitted for hiding in cover media which is text in this case. The cover text is constructed using characters of English language of count 224 starting from 0 to 223[3]. The embedding procedure first calculates the frequency with which particular number appears and then checks the corresponding number in the cover media and calculates the ASCII out of it. Then an alphanumeric puzzle is generated consisting of some operators in which the first column of table denotes the text for hiding the secret data and later column denotes the position. The cover text used in algorithm is smaller as compared to other text steganography algorithms and this algorithm ensures greater security of data hiding and it is difficult for any third party to extract the message as it is very complex and time consuming [3].

M.Garg proposed an algorithm for text based steganography which uses html labels for inserting the covert message or data [6]. This method offers more embedding capacity and hence is more efficient in terms of capacity of hiding the data and this technique hides data in such a way that the characteristics or points in the cover media are not visible to anyone which makes an html document away from the attention of the attacker or any unintended person but if the relation is once detected by attacker then the secret data can be extracted depending on the values of primary and secondary features [6].

T.P. Nagarhalli proposes a steganography algorithm for text used for hiding secret information by making use of adjectives in the English language. It provides security to the data from the third party or an attacker in such a way that the attacker is unable to detect the message. The database for the secret message corresponding to the adjectives or their group is made available to the intentional recipient and the sender [4].

The technique is simple to implement and consist of database or table for all adjectives to be used and the periodic updating of the database is required which is a tiresome work [4].The demerit of this technique lies in the fact that if the third person or the one who wants to fetch the secret information looks at the data i.e. the group of special words which are used to shroud data (cover object) then he/she may get to know that something wrong with the data is going on as sometimes the sentences used are meaningless. So looking at group of meaningless words there may originate doubt about secret transmissions.

P.Singh et.al. proposed a technique for text based steganography which utilizes null or void spaces for hiding the covert information[7]. In this method single spacing in between the words are denoted by “0” and double spacing are

denoted as "1".The shortcoming of this technique is that it takes more memory or space for encrypting few bits. Hence if data with more bits are to be hided then it requires more spacing which may attract an intruder towards it. Some software for text editing purpose may erase additional spaces which may result in damaging the hidden message [7].This technique cannot be used for being applied over WSN considering any scenario because it demands higher memory requirements which is not feasible for WSN. Secondly, if on hiding the data the spaces causes the meaning of data to change then it may result in overall changed data which may provide hint to attacker.

5. PARAMETERS FOR QUALITY EVALUATION

5.1 PSNR (peak signal to noise ratio)

It is defined as highest value of a quantity (in terms of power) of wave divided by the power of altering noise which may affect the signal. Due to the reason that signal has broad span so the value of peak signal to noise ratio is defined in series of the logarithmic decibel scale. If a steganography technique can improve a signal corrupted by noise and is matched with the initial signal then is said to be a good algorithm or technique [12].

Mathematical expression of PSNR is shown below:

$$PSNR = 10\ log_{10}\frac{MAX_f}{\sqrt{MSE}}$$

5.2 MSE (mean square error)

It is the comparison between the initial values to the values corrupted by noise [12].

Error=difference in of initial values by corrupted values.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|$$

Where f=matrix of initial values

g=matrix of values corrupted by noise

m=no. of rows and i=index

n=no. of columns

MAXf is the maximum signal value which occurs in initial value matrix.

5.3 Energy consumption

The energy consumed in one round of the communication from nodes of sensor network to the sink can be calculated to make an analysis that whether the technique can be used for wireless sensor network or not because the wireless sensor network are energy restraint networks.

Table 1. Comparison of Different Algorithms

S.No.	*Algorithm*	*Secure*	*Can be used for WSN*
1	Developing an efficient solution to information hiding through text steganography along with cryptography.	Highly secure	Yes as the cover image is of small size.
2	A novel text steganography technique based on html documents.	Secure	May not be feasible to use for WSN as more processing is required for searching attributes.
3	A New Approach to Text Steganography Using Adjectives	Secure (If database leaked then the secret message will be known to the attacker)	Cannot be used as the database is too large which will consume large memory so cannot be used for WSN.
4	A Novel Approach of Text Steganography based on null spaces	Not much Secure	Cannot be used as it requires large memory for null spaces.

6. CONCLUSIONS

This paper gives an overview of different text steganography techniques and a table showing comparison of different techniques that whether the techniques be used for wireless sensor networks or not considering the constraints of wireless sensor networks. In future, an advanced technique can be developed for security over wireless sensor networks having high security and high undetectability. Applying the steganography algorithms over wireless sensor networks and analysing the parameters like MSE, PSNR and energy left for each communication round is an open research issue as all the algorithms for steganography cannot be applied directly over wireless networks.

7. REFERENCES

[1] Amirtharajan, R., and Rayappan, J.B.B.2012. An intelligent chaotic embedding approach to enhance stego-image Quality.

[2] Mehta,A.M., Lanzisera,S., and Pister, K.S.J. 2009.Steganography in 802.15.4 Wireless Communication.

[3] Uddin, M. P. , Saha,M.,Ferdousi,S.J., Afjal,M.I., and Marjan, M.A. 2014.Developing an efficient solution to information hiding through text steganography along with cryptography.

[4] Nagarhalli, T.P. 2015. A New Approach to Text Steganography Using Adjectives.

[5] Perrig,A., Stankovic,J., *and* Wagner,D.2004.Security in wireless sensor networks..

[6] Garg,M.2011. A Novel Text Steganography Technique Based on Html Documents.

[7] Singh,P.,Chaudhary,R.,and Agarwal,A.2012.A Novel Approach of Text Steganography based on null spaces.

[8] Kumar,K.A.,Pabboju,S.,andDesai,N.M.S.2014.Advanvce d text steganography algorithms: An overview

[9] Jassim,F.A.2013.A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method.

[10] Sharma,G.,Bala,S.,and Verma,A.K.2012. Security frameworks for wireless sensor networks-review.

[11] Modi,R.P.,Nimbalkar,M.V.,andPathak,G.R.2011. Dynamic cryptographic techniques for wireless sensor networks.

[12] Peak Signal-to-Noise Ratio as an Image Quality Metric.2013.[Online].*Available: www.ni.com,*

[13] Introduction to Steganography.[Online].Available: Revised. 2009.

[14] Gupta, S.,and Gupta, D.2011. TextSteganography:Review Study & Comparative Analysis.

[15] Kaur,A.,Kaur,R., and Kumar,N.2015. A Review on Image Steganography Techniques.