International Journal of Computers & Technology
Volume 4 No. 3, March-April, 2013, ISSN 2277-3061

Steganography: Securing Message in wireless network

A H M Kamal
Department of Computer Science and Engineering
Jatiya Kabi Kazi Nazrul Islam University, Bangladesh

Abstract

Steganography is the process of hiding a secret message with in a cover medium. However eavesdropper may guess the embedding algorithm like least significant bit (LSB) replacement of Chan et al, 2004; Wang et al, 2001; Wu et al, 2005, LSB matching of Mielikainen, 2006, addition and/or subtraction of Andead wastfield, 2001; F. Huang et al in 2011, Exploiting Modification Direction by Zhang and Wang, 2006, Binary Space Partition by Tsai and Wang, 2007, modulus function of Chin et al, 2011 and thus can apply the respective extraction method to detect the secret message. So challenges lies in the methodologies of embedding message. Capacity, security and robustness are the services to be demanded by users. Again the true-positive rate of secret message detection by eavesdropper should be lessened by applying firm technique. Thirdly operating domain should be less sensitive to the noise, margin level of losses or alteration of data while communicating through unguided medium like wireless network, sensor network and cellular network. This paper will briefly discuss the steganographic methods and their experimental results explained in the survey paper of Niels Provos and Peter Honeyman to hide and seek message. Finally the proposed results and the directions for future works are addressed.

Keyword: embedding, steganography, message hiding, LSB replacement, Stego, capacity.

1. Introduction

Steganography is an old technique that has existed since antiquity. Herodotus, a Greek historian who lived in the 5th century B.C., relates how the Greeks sent and received warnings of enemy movements using a message underneath the wax of a writing tablet. Others can be found in the use of secret ink to hide information on a white paper or the use of micro-dot by intelligence agencies in World War 2.

If cryptography is to encrypt and render a data unreadable, steganography is the way to hide the existence of this data. In this paper, we show that it is possible to secure a wireless sensor network, to use steganographic techniques to hide the existence of data in the 802.15.4 protocol. This protocol is widely used in wireless sensor networks. This protocol specifies the Physical and MAC layers of communication, because it provides an energy-efficient solution for communication between wireless sensors. Zigbee [3], [4], [5] the most used protocol in wireless sensor networks, uses this 802.15.4 protocol for the communication layer.

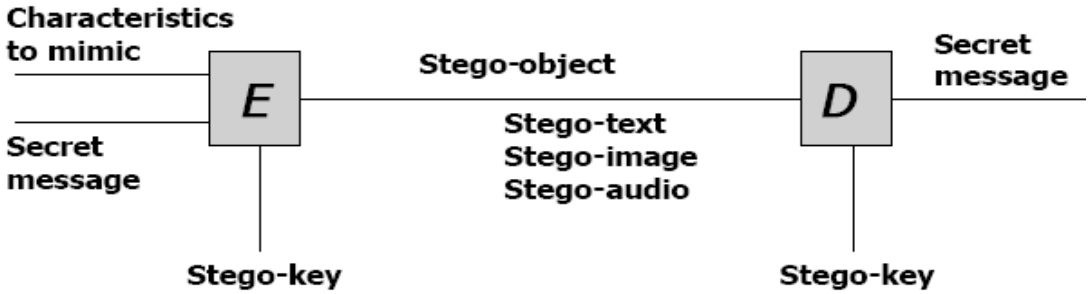


Figure 1: Embedding and detection process in steganography

The level of security of hidden message relies on the encoding method. So embedding method is the key component in steganography which will ensure the data secrecy. Here a description on steganographic methods and some proposals are outlined gradually. Section 2 is to provide a review of the literatures on the target area. Following section will give an idea of different types of steganography. Problem domains are described in section 4. All the algorithms in embedding message are described in section 5. Section 6 is the outline of experimental result. Finally in section 7 we have given our proposal and direction for future work. Section 8 is just to conclude the writing.

2. Literature Review

Steganography bears the principle of embedding of messages (text, audio or video) in another media or support [1], [6], [7]. In paper [3] it was shown that by hiding data in the MAC layer of the 802.15.4 protocol a good latency in hiding can be achieved and thus a security will be stronger. Paper [8] and [9] also discussed on hiding data and creating steganographic channel possibilities using noise in the physical layer of the 802.15.4 protocol.

Paper [10] and [11] researched on several techniques in steganography to hide pictures in other pictures and in this way watermarking was introduced [11]. Several steganographic techniques aim to use specificities of communication protocols to hide data and use communication layer fields as the cover object [3]. This use of steganographic data in communication layer fields provides the creation of a hidden channel in the network [3]. Only devices that know in which fields the data is hidden can read data or write data. They can invisibly exchange data in the network if the network does not know the steganographic technique [3]. [12], [13] and [14] show different possibilities for hiding data by using specific characteristics of protocol to create a hidden channel (steganographic channel). Recent techniques consist of using the reserved field of the protocol. Thus, [12] uses the reserved field in the TCP packet header of the TCP/IP protocol

International Journal of Computers & Technology
Volume 4 No. 3, March-April, 2013, ISSN 2277-3061

3. Types of Steganography

Though steganography is a recent decade's research area in communication a variety is already seen. Varieties come based on the cover medium. Those are text, image, audio, video and protocol steganography. All of those use redundant bits to replace by message bits while embedding. So text steganography is not a famous one; rather it is less likely used as a cover medium as it contains less redundant information.

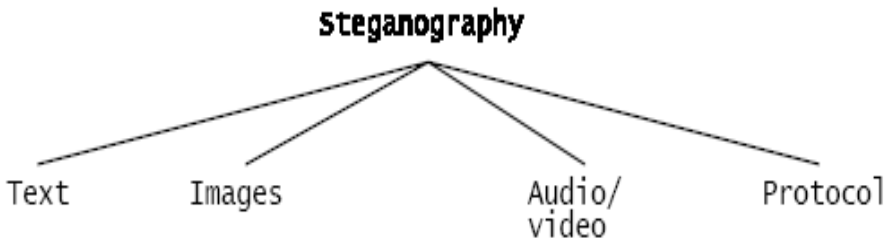


Figure 2: Types of Steganography

Likewise audio and video steganography are less used method for their large size and complex algorithm for compression and coding. Again in protocol steganography, messages are embedded in network layer. So it may increase the network congestion. So image embedding is a famous technique in the area of steganography because it contains larger amount of redundant bits and changes in least significant bit is unrealizable to human eye.

4. Problem Domain

The principle objective of that article is to provide information security and henceforth we choose the latest research topic – image steganography. The major aspects those influence the problem domain of steganography are service related and implementation related.

4.1 Service Related Issues

Service related issues are capacity, security and robustness. Capacity means how much information can be hided in the cover medium. This obviously desired to increase the capacity to embed large amount of information. In steganography cover medium is used to hold and hide secret message. Unfortunately a fractional part of the cover medium can be utilized to maintain the message hiding property of steganography. Currently most of the proposal suppors to use LSB of each byte of cover medium to embed message bits which results in yielding the maximum amount of capacity upto 1/8th of the size of cover medium. Again security refers to the inability of eavesdroppers to realize the existence of hidden message and to detect it. Eavesdropper usually measures the probability of steganographic contents being in received information. Steganographic contents are hided inside into the cover medium to generate the stego medium. The stego is communicated over a channel through guided or unguided medium. There are lots of reasons of changing the bit's value of transferred contents while passing through a medium. How much the system can withstand before destroying information due to modification is referred to robustness.

4.2 Implementation related issues

Another challenging issue is to choose the media to embed the message. It is already said that message can be embedded with text, images, audio, video and protocol. But at what location to start embedding is an issue to take into consideration. Another issue is the file format of each media. Each media has different formats, jpeg, bmp, gif for images, mp3, wav for audio, avi, dat for video. Some of those support compressed format while other are not. So as to different steganographic algorithm are needed for different formats. A third issue in implementation to be considered is to make it enough firms so that eavesdropper can't detect the secret message. A statistical analysis can lead to a guess of hidden message even to retrieve it.

5. Message embedding domain

It is delineated that images are famous for embedding message. In images message hiding are performed in two domains – image domain, transformed domain. Following is an explanation of those two.

5.1 image domain

In image domain messages are embedded directly to color values. For jpeg format each pixel value consists of three bytes. LSB of each byte can be considered for embedding information. So each pixel can contain three bits of hidden information. To understand the method of embedding, consider a grid of image of 3 pixels of 24 bits. Also consider their binary values are as follows.

```
(00101101   00011100   11011100)
(10100110   11000100   00001100)
(11010010   10101101   01100011)
```

Again consider a message portion is 200 whose binary is 11001000. Then gets the LSB of each byte from grid and replace those with the bits of message sequentially to generate the following stego image which will be transferred through a medium.

International Journal of Computers & Technology
Volume 4 No. 3, March-April, 2013, ISSN 2277-3061

```
(0010110|    0001110|    1101110|)
(1010011|    1100010|    0000110|)
(1101001|    1010110|    01100011)
```

This is easy to implement. However eavesdropper can find the hidden message if he/she has a guess about the message or has a pattern of it. Besides that any changes in the stego images an destroy the original messages. That is why it is not famous for steganography.

5.2 Transform domain

It is a better choice for steganography. It tolerates a margin level of data altering or losses. Transform domain can be the Fourier transform, Laplace transform, discrete cosine transform (DCT) or similar one. Among those DCT is widely used. The basic idea of calculating DCT is as follows.

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \csc\frac{(2x+1)u\pi}{16}\csc\frac{(2y+1)v\pi}{16}\right] \quad \text{(i)}$$

Where

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases}$$

Based on that DCT three well known method of steganography is explained in the following.

5.2.1 Sequential method

There at each step pointer in DCT and message bits progress sequentially. Implementation is known as Derek Upham's JSteg. Each time it calculates DCT from cover image, collect next LSB from message and replaces LSB of DCT with LSB of message. When the whole message is embedded the stego image is ready to be transferred.

5.2.2 Pseudo random method

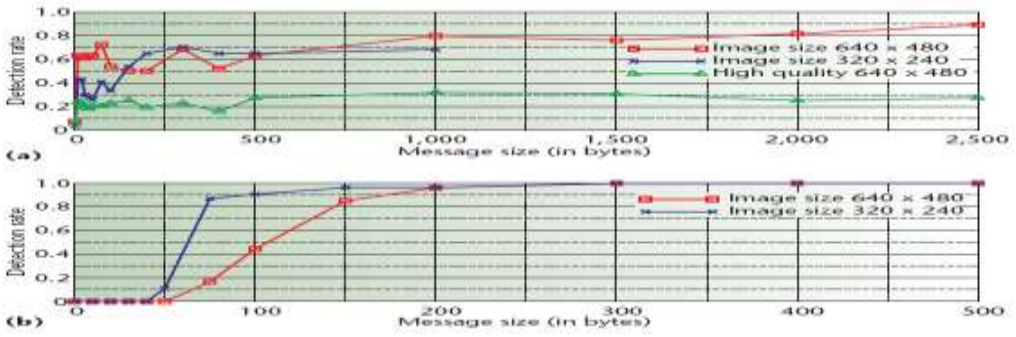
This is an implementation of Niels Provos which is known as OutGuess 0.1. Another implementation is done by Allan Latham which is known as JPHide. There a pseudo random number is generated to select the DCT. So message is embedded at random position in the images.

5.2.3 Subtraction method

In this method a block of code is embedded rather than bit. This was proposed by Andreas Westfield and known as F5. There the absolute value of DCT is decreased rather than replacing LSB.

6. Experimental result

An experiment was done to detect the secret message embedded by above three methods. The result shows that JPHide, in upper grapgh a, is independent of message length. The reason lies behind the pseudo random selection of DCT. On the other hand JSteg is detectable if the message size is greater than 50 bytes. However, in other saying, it is a well performing one if the message length is less than 50 bytes as the detection rate less than 10%.



International Journal of Computers & Technology
Volume 4 No. 3, March-April, 2013, ISSN 2277-3061

Figure 3: Detection rate versus message size

7. Our Proposal and result analysis

Based on the discussion in section 5 and 6 a modified and efficient proposal is presented here to minimize the memory utilization as well as to increase the embedding security.

7.1 Proposed method

In the calculation of DCT the proposals uses a temporary memory to store the 8x8 grids of images which can be seen in equation (i). Our proposal minimizes the use of temporary memory by working at image frame directly.

```
P=0;
For (k=0;k<h/8;k++)
{
For (i=k; i<k+8;i++){
For (j=P; j<(P+8);j++){
```

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x\epsilon i}\sum_{y\epsilon j} f(x,y) * cos\frac{(2x+1)u\pi}{16} cos\frac{(2y+1)v\pi}{16}\right]$$

```
}
}
P=P+8;
If (P>w*3) P=0
}
```

Here h means image height and w means image width. P is a variable to from grid to grid. This implementation improves the memory utilization.

The authors in the article defined an equation to find the true positive rate – the probability that a detected image must contain steganographic content. The equation is as follows.

$$P(S|D) = \frac{P(S).P(D|S)}{P(S).P(D|S) + P(\neg S).P(D|\neg S)} \quad \text{(ii)}$$

In this equation it is not considered that an eavesdropper may not detect an image which must contains steganographic contents. As a result if value of P(S|D) may be enough high to encourage the eavesdropper to look into more details to find secret message. We have modified the equation as follows.

$$P(S|D) = \frac{P(S).P(D|S)}{P(S).P(D|S) + P(\neg S).P(D|\neg S) + P(S)P(\neg D|S)} \quad \text{(iii)}$$

Usually the probability of success rate of detecting message by eavesdropper is less than 0.5. So the value of P(S|D) in (iii) will be less than in (ii). As a result eavesdropper will lose intension to seek more details. So it will improve the security issues in steganography. Again the targeted user will detect the secret message successfully as he/she has the necessary key and algorithms in hand. So then $P(\neg D|S)=0$.

7.2 Result analysis

In our experiment it was found that it is dominating the other in memory requirement as well as in security issues. The memory requirement is wxh/8x8 times less than the others. Again the improvement of security in our experiment shows that it is hardly detectable even if the message size is near to 100 bytes. In the cellular communication or sensor network it can be a good solution in improving security of teganography.

International Journal of Computers & Technology
Volume 4 No. 3, March-April, 2013, ISSN 2277-3061

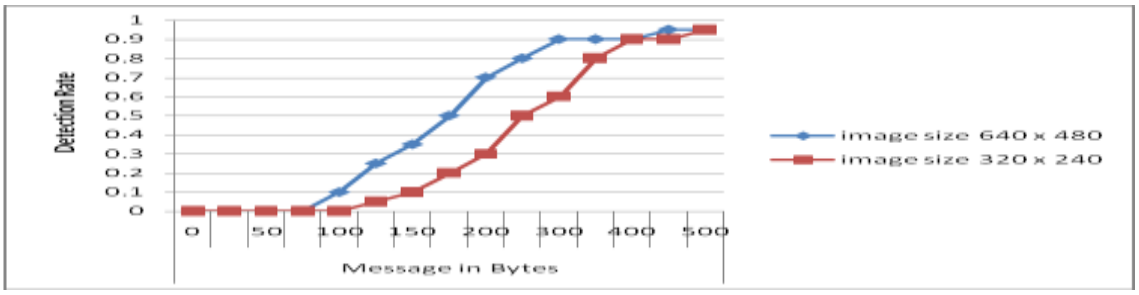


Figure 4: Detection Rate at proposed method

Finally the cellular network has bandwidth limitation. Its channel is erroneous. So there is a scope to work for new embedding method to perform well in cellular network, sensor network.

8. Conclusion

This is a brief study on image steganography. Here all the algorithms are analyzed and a modified method is proposed to improve memory utilization and security of image steganography. In addition to those a new research scope is outlined where one can further devote time.

References

1. Hide and Seek: An Introduction to Steganography, NIELS PROVOS AND PETER HONEYMAN, University of Michigan, IEEE COMPUTER SOCIETY, 1540- 7993/03, 2003 IEEE.
2. Security in Wireless Sensor Networks: Issues and Challenges, Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, ISBN 89-5519-129-4, ICACT 2006
3. Steganography in MAC Layers of 802.15.4 Protocol for securing Wireless Sensor Networks, David Martins and Hervé Guyennet, IEEE
4. Public Key Cryptography in Sensor Networks- Revisited*, Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, ANI-0112889.
5. Energy-Aware Security Management Utilizing Adaptive Security Mechanisms for Wireless Sensor Networks, Mikael Fernandus Simalango, Amikelive.com – Technical Paper Series
6. Security Attacks and Challenges in Wireless Sensor Networks, Al-Sakib Khan Pathan and Choong Seon Hong, Encyclopedia on Ad Hoc and Ubiquitous Computing, chapter – 16.
7. R. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, pp. 474–481, 1998.
8. L. S. Mehta A.M. and P. K., "Steganography in 802.15.4 wireless communication," in *Advanced Networks and Telecommunication Systems, 2008. ANTS '08. 2nd International Symposium on*, (Mumbai), pp. 1–3, 2008.
9. T. Kho, "Steganography in the 802.15.4 physical layer," tech. rep., 2007.
10. S. Katzenbeisser and F. A. Petitcolas, eds., *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA, USA: Artech House, Inc., 2000.
11. I. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.
12. T. G. Handel and M. T. Sandford, II, "Hiding data in the osi network model," in *Proceedings of the First International Workshop on Information Hiding*, (London, UK), pp. 23–38, Springer-Verlag, 1996.
13. Z. Trabelsi, H. El Sayed, L. Frikha, and T. Rabie, "A novel covert channel based on the ip header record route option," *Int. J. Adv. Media Commun.*, vol. 1, no. 4, pp. 328–350, 2007.
14. S. J. Murdoch and S. Lewis, "Embedding covert channels into tcp/ip," in *Information Hiding: 7th International Workshop, volume 3727 of LNCS*, pp. 247–261, 2005.