STEGANOGRAPHIC SECURE DATA COMMUNICATION USING ZIGBEE

MR.NITIN B.NAIK, MRS.ARCHANA NITIN NAIK
Vice-Principal, Sharad Institute of Technology ,Polytechnic,
Yadrav,Dist.Kolhapur(Maharashtra),India
HOD E&TC, Sharad Institute of Technology ,Polytechnic,
Yadrav,Dist.Kolhapur(Maharashtra),India

ABSTRACT

Steganography is a science dealing with writing hidden messages/pictures in a particular way that only the sender & the intended recipient are able to decipher so as to provide security in open environment like internet. Steganography attempts to hide the very existence of the message and make communication undetectable. Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices. This paper focuses on the implementation of a steganographic algorithm using wireless communication such as Zigbee. Furthermore, this article presents experimental results obtained from testing a steganographic algorithm using Zigbee devices. The main purpose of implementing such an algorithm using zigbee is to provide security on low and medium cost devices.

1. INTRODUCTION

Nowadays, an important aspect of the modern way of life is communication. Many devices present today have the ability to transmit various information between them using different ways of communication, like insecure public networks, different types of wireless networks and the most used: the Internet. In some cases it is needed to keep the information travelling through different kinds of channels secret. Mainly there are two ways of concealing information: cryptography and steganography. Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is an encrypted, secret information.[2] On the other hand steganography is able even to hide this aspect making sure that even the fact that there is secret information, is concealed. Steganography's main aspect is that it is embedding the secret message into another message [3]. Mainly, steganography can be used for concealing important information within computer files such as documents or image files in such a way that only so called authorized users know and can extract the information. The advantage over classic cryptography is that messages hidden using steganography techniques do not attract attention on themselves. Before continuing this discussion additional terminology needs to be added. In general, steganography terminology is analogous to more conventional radio and communication technologies.

2. RELATED WORK

Significant results have been obtained hiding information into text. The main goal was to discourage illegal document copying by making documents with line shift encoding, the lines of text being shifted up or down thereby encoding a serial number. [4] Steganography was also used to embed data into an audio signal by manipulating characteristics of the audio signal below the level of perceptibility. These techniques were useful in applications such as annotation, captioning and the automatic monitoring of radio advertisements. [5] Important steps have been made hiding information using digital watermarking using improved techniques based on the decorrelation property of the Karhunen- Loeve Transform [6] as well as a method of hiding messages in digital images based on YUV format and its derivatives [7]. These techniques were used especially against a current common issue like illicit copying and distribution of copyright material.

Studies and tests were made for elaborating different techniques and algorithms to embed large amount of data into a picture as well as the requirements needed. Other steps have been taken towards eliminating detection of steganography and counteracting attacks meant to extract the hidden information. New and more complex algorithm have been developed to avoid the detection of hidden data as well as embedding hidden information in preprocessed images and in images where compression was applied. [8] Other related work on the subject is about using steganography to insert a video or audio message in the cover in real time, using a secret key steganographic micro-architecture employing Field Programmable Gate Arrays .Furthermore, devices such as Field Programmable Gate Arrays (FPGA) also hosted steganalysis (the reverse process of steganography) algorithms.

3. HARDWARE USED FOR IMPLEMENTING STEGANOGRAPHY

This paper focuses on the steganographic technique used for hiding information in communication between various mobile or embedded devices. As shown above significant steps have been made in bringing steganography on dedicated devices using FPGAs/CPLDs. The major advantage of using a FPGA/CPLD for steganography is speed, a FPGA/CPLD being able to execute steganographic algorithms much faster than other devices. The disadvantage in using an FPGA/CPLD is cost, making them impossible to be used in mobile phones for example.

This paper tries to implement the steganographic algorithm using Zigbee.

The main focus of this paper is to bring steganographic algorithms like the LSB algorithm on mobile and embedded devices without significantly rising their price. One possible solution presented here is using microcontrollers for executing the steganographic algorithm.

It consists of Zgbee interface.Zigbee is an industrial consortium designed to build a standard data link communication layer for used in ultra-low power wireless application. The Zigbee alliance was formed because its members felt that existing standard technologies were not applicable to ultra-low power application scenarios.

The Zigbee data link layer is designed to operate on top of the IEEE 802.15.4 physical layer. IEEE 802.15.4 is a direct sequence spread spectrum physical layer including transmission bands at 868 MHz, 902-928 MHz and 2.4 GHz.

3.1 RF Module Operations

3.1. 1Serial Communications

The XBee ZNet 2.5 OEM RF Modules interface to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with any logic and voltage compatible UART; or through a level translator to any serial device (For example: Through a Digi proprietary RS-232 or USB interface board).

3.1.2 UART Data Flow Devices that have a UART interface can connect directly to the pins of the RF module as shown in the figure below.

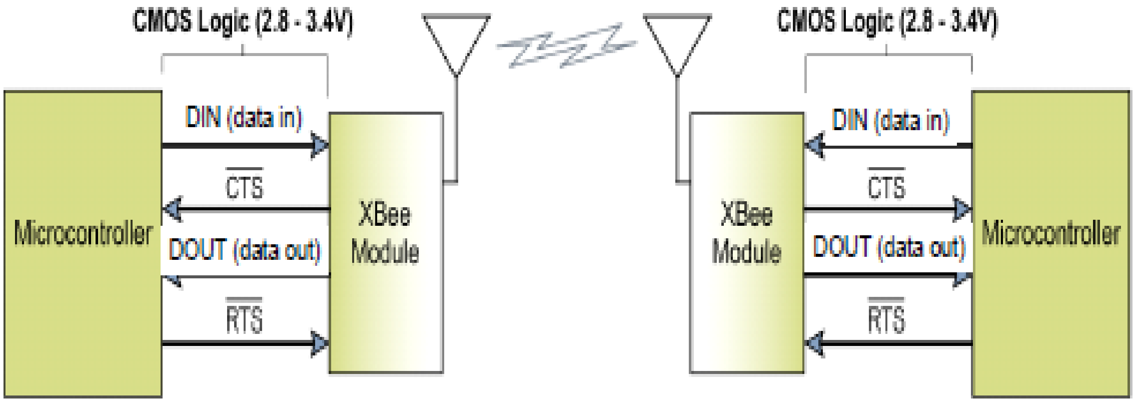

Fig 3.1System Data flow diagram in UART Interface environment

Data enters the module UART through the DIN (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted. Each data byte consists of a start bit (low), 8 data bits (least significant bit first) and a stop bit (high). The module UART performs tasks, such as timing and parity checking, that are needed for data communications. Serial communications depend on the two UARTs to be configured with compatible settings (baud rate, parity, start bits, stop bits, data bits).

4. IMPLEMENTATION DETAILS

The steganography algorithm can be implemented on PC using MATLAB based on how to decode an encrypted message within a carrier image. The image used in this work is 256*256 bitmap image.

Steganography algorithm implemented in MATLAB can perform the effective hiding of information in such a way that it is very difficult to a casual person to detect that image contains some information. It can't attract the attention of any user except the intended recipient.

This can hide or retrieve the data by using the various options present in the software these options can be:
1. Hide Message: -Hide the Text message into the Bitmap file.
2. Retrieve Message:-Retrieve the Text message from the Bitmap file.

The Data and Image are applied from PC and transferred to Zigbee, where the encryption process is performed on data. In encryption process the encryption algorithm is applied. This data and cover image are hide by steganography algorithm. This is called stego image. This stego image is then transmitted through channel via Zigbee. At receiver side the stego image is received via Zigbee receiver. The exactly reverse operations are performed at this stage. The decryption steganography algorithm are applied to stego image to extract the message from it. Then decrypted message is appeared in at the receiver end.

5. RESULTS

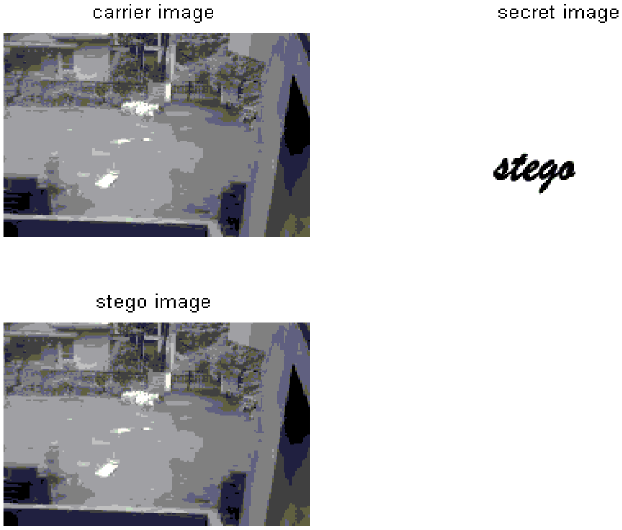

Fig. 5.1 Stego Image

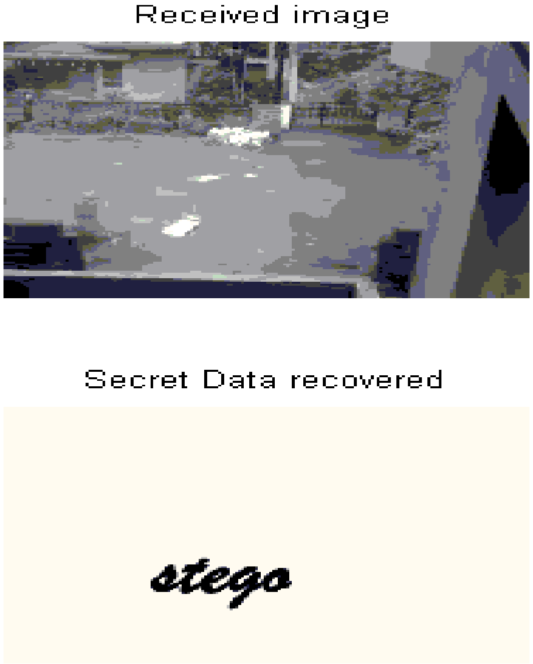

Fig. 5.2 Data Extraction

6. CONCLUSION

This paper presents a possible implementation of steganography algorithms on an Zigbee platform. The main benefit of this implementation is that it brings steganography on a level very common nowadays, the mobility. Using steganography on mobile devices may improve security on data transfers without additional significant cost. Furthermore, this work focuses on using Zigbee for executing the steganographic algorithms instead of using Field Programmable Gate Arrays. This way, when adding steganography capabilities on an embedded device the cost is not mainly influenced as it could be if a FPGA module is added to the device. Steganography may also help hiding secret information in communication lines, for example embedded modules with steganographic encrypting and decrypting capabilities connected between two systems. An embedded device with steganography implemented on it can be used in secret communication. The technique used in this work is LSB algorithm, processing the images on the pixel level.

7. REFERENCES

[1] Daniela Stanescu, Valentin Stangaciu, Ioana Ghergulescu, Mircea Stratulat “Steganography on embedded devices” 5th International Symposium on Applied Computational Intelligence and Informatics • *Timişoara, Romania*

[2] Neil F. Johnson, Sushil Jajodia, “Exploring Steganography: Seeing the Unseen”, *IEEE COMPUTER, vol. 31, 1998, pp. 26--34*

[3] József Lenti, “Steganographic methods”, *Department of Control Engineering and Information Technology, Budapest University of Technology and Economics, H-1521, Budapest, Hungary, June 2000, pp. 249-258*

[4] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, “Electronic marking and identification techniques to discourage document copying,” *Selected Areas in Communications, IEEE Journal on vol. 13, 1995, pp. 1495-1504.*

[5] D. Gruhl, W. Bender, A. Lu, “Echo hiding”, in *Information hiding: First International Workshop, Computer Science, Isaac Newton Institute, Cambridge, England, May 1996, pp. 295 – 315*

[6] D. Stanescu, M. Stratulat, B. Ciubotaru, D. Chiciudean, R. Cioarga, and D. Borca, “Digital Watermarking using Karhunen- Loeve transform,” *Applied Computational Intelligence and Informatics, 2007. SACI '07. 4th International Symposium on, 2007, pp. 187-190*

[7] Stanescu, D.; Stratulat, M.; Groza, V.; Ghergulescu, I.; Borca, D.“Steganography in YUV color space”, *Robotic and Sensors Environments, 2007. ROSE 2007. International Workshop on Volume , Issue , 12-13 Oct. 2007*

[8] Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy, “Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics”, *Communications and Multimedia*