Secured Wireless Communication Through Zigbee using Cryptography and Steganography

Prof. Mrs. S. Y. Kanawade
Department of Eletronics &Telecommunication Engineering
Savitribai Phule Pune University, Nashik

Vikas Nagare
Department of Eletronics &Telecommunication Engineering
Savitribai Phule Pune University, Nashik

Anupam Kumar
Department of Eletronics &Telecommunication Engineering
Savitribai Phule Pune University, Nashik

Swapnil Dhakane
Department of Eletronics &Telecommunication Engineering
Savitribai Phule Pune University, Nashik

Abstract

Network security and protection of data have been of great concern and a subject of research over the years. There are many different forms of steganography mechanisms like LSB, Masking and filtering and Transform techniques. All of them have respective strong and weak points. The Least Significant Bit (LSB) embedding Technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file . This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format. In a network The success of the algorithm depends on hiding technique used to store information into the image.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. The main purpose of implementing such an algorithm using Zigbee is to provide security on low and medium cost devices. The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography and steganography can be combined.
Keywords: ZigBee, steganography,Cryptography, LSB, Micro-Controller

I. INTRODUCTION

The rise of the Internet is one of the most important factors of information technology, So security has been the major aspect for communication and for that we need a secured system which gives the assured security of data to us. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret,it may also be necessary to keep the existence of the message secret.The technique used to implement this,is called steganography.It is the art and science of invisible communication.This is accomplished through hiding information in other information,thus hiding the existence of the communicated information.Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeps in the contents of a message secret,steganography focuses on keeping the existence of a message secret.The LSB algorithms used for image steganography to illustrate the security potential of steganography for business and personal use.After the overview it briefly reflects on the introduction to embedded system used in this project.

II. RELATED WORK

A popular way to protect data is to encrypt the data while sending and decrypt it while receiving to regain the original message.Before transmitting,the data is converted into unreadable format and then the data is encypted and decrypted in the receiver end to get the original message.Least significant bit (LSB) insertion is a common,simple approach to embedding information in a cover image using steganography.The least significant bit in other words,the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message.

III. PROPOSED WORK

For security, only encryption may not be enough, hence proposed project include combination of both cryptography and Steganography. The encrypted data hide into the image and then image is transmitted in the network. There is some weakness in hiding information in images; that is adversary could easily detect the confidential message, by noticing the noise and clarity of the image's pixels, also by observing the difference between the embedded image and the original one if it is known to him. In the proposed project, we are using an Iris images instead of images that contain faces or natural scenes, because the only feature or data of a person that hackers cannot hack is their biometric features.

IV. BLOCK DIAGRAM

A. Dataflow:

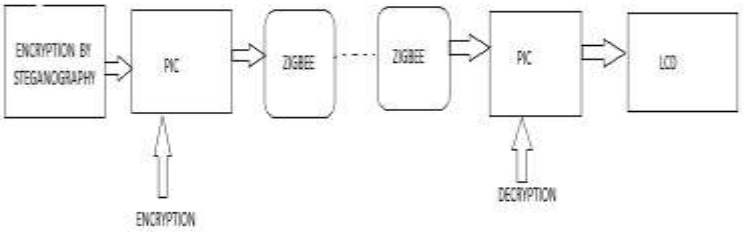

Fig. 1: Block Diagram

B. Transmitter:

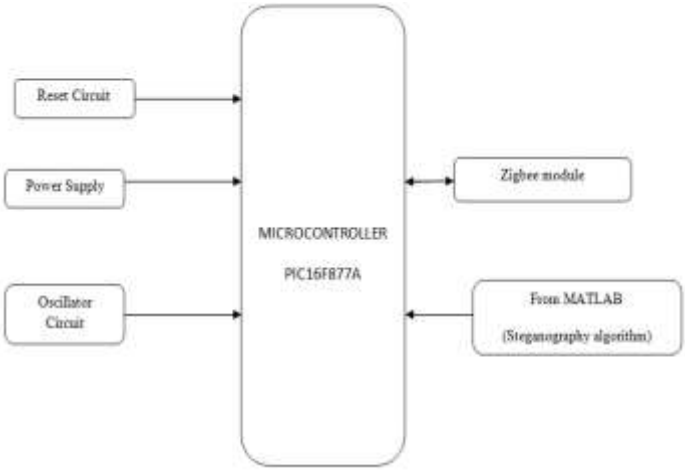

Fig. 2: Transmitter Circuit Diagram

C. Receiver:

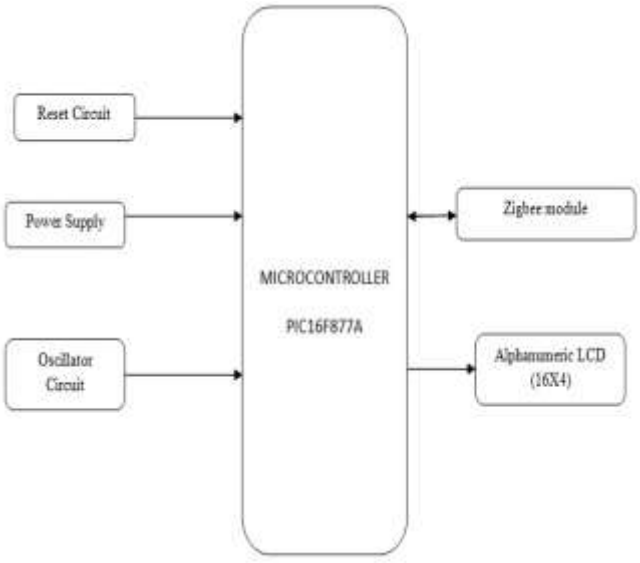

Fig. 1: Receiver Circuit Diagram

D. Discription

System is mainly comprised of Zigbee S2 module, Alphanumeric LCD and USB to TTL module with Microchip PIC16F877A microcontroller as brain of the system. Three basic circuits which any kind of microcontroller needs are reset circuit, oscillator circuit and power supply are also included in system. System is loaded with support of 16x2 alphanumeric LCD which provides provision of displaying encrypted and decrypted messages on it.

V. ALGORITHM

Input: Embed the message.
Output: Message is embedded safely in an image and reconstructed properly.
Begin
1) Message.
2) Encrypting message.
3) Implementing LSB based steganography
4) Embedding data.
5) Stego image.
6) Extraction of embedded message.
7) Encrypted message generation.
8) Decryption.
9) Original Message.

End

VI. LITERATURE SURVEY

In Steganography Secure Data Communication Using Zigbee,RF Module is used with serial communucation used steganography algorithms on an Zigbee platform. 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.

VII. CONCLUSION

Steganography is powerful and effective for communication of secret data. For the image steganography various methods have been proposed. A method that hides the secret messages in the image using Matlab. Matlab is not only a programming language, but a programming environment as well. It is provide more security for secret communications. Thus the capacity of the hiding process to hide secret messages is also high in the proposed.

REFRENCES

[1] P.Rohitha1, P.Ranjeet Kumar, Prof.N.Adinarayana and Prof.T.Venkat Narayana Rao"WIRELESS NETWORKING THROUGH ZIGBEE Technology Advanced Research in Science and Software Engineering", Volume 2, Issue 7, July 2012.
[2] Nisha Ashok Somani, Yask Patel,"ZIGBEE: A LOW POWER WIRELESS TECHNOLOGY FOR INDUSTRIAL APPLICATIONS", International Journal of Control Theory and Computer Modelling (IJCTCM) Vol.2, No.3, May 2012.
[3] S.Kanagamalliga, Dr. S. Vasuki, A. Vishnu Priya, V. Viji " EMBEDDED BASED SECURITY MONITORING AND CONTROL SYSTEM", International Journal of Information Sciences and Techniques (IJIST) Vol.4, No.3, May 2014.
[4] Mr.Nitin B.Naik, Mrs.Archana Nitin Naik,"STEGANOGRAPHIC SECURE DATA COMMUNICATION USING ZIGBEE", International Journal of Research in Science And Technology http://www.ijrst.com (IJRST) 2015, Vol. No. 5, Issue No. II, Apr-Jun.
[5] Prodanov.W.M. Valle & R.Buzas. A Control Area Network bus transceiver behavioral model for network design simulation IEEE. Transaction on Industrial Electronics, 56(9):p3762-3722, 2009.