# Zigbee based Image Transfer using Steganography

**K. Bhuvaneshwari**
M.Tech Student
RITM, Lucknow, India

*Abstract*— In There has been an abundance in media communication thanks to the advancements in the semiconductor technology and telecommunication services worldwide. We indulge into some type of image and video transfer almost on a daily basis. The security of the digital images over communication media, hence becomes one of the important aspects. Cryptography provides a solution to this problem. However, cryptography requires more processing power and memory. Lightweight cryptography another version of cryptography was suggested in constrained environments such as RFID tags, sensors, contactless smart cars and healthcare devices. It had the disadvantage that the sensitive information is in unreadable format, attackers may still be able to uncover or decrypt it with sufficient time or processing power. As an alternative, steganography, which hides the secret message i.e. image inside the cover image can be used as an alternative security mechanism for transferring the data in a secure manner. Several image steganography techniques have been used on low processing power devices, such as embedded devices and mobile phones for hiding the data. As well as, is a method to make confidential information and messages undetectable and prevent hackers from detecting them, thus preferable over cryptography based techniques. In this research work, a steganography based method to transfer images securely across a Zigbee transceiver complying IEEE 805.14 WPAN standards has been implemented. The steganography technique used for this research work is a modified Least Significant Bit technique.

***Key words:*** Steganography, Zigbee, Transceiver, Cryptography, Communication

## I. Introduction

In recent years, digital images can be captured easily with scanners, digital cameras and camcorders, and transmitted easily over the Internet. Associated with the widespread circulation of images are issues of copyright infringement, authentication and privacy. One possible solution is to embed some invisible information into the images where the embedded information can be extracted for different purposes. Data Hiding or Steganography offers an essential alternative to image integrity and authenticity problem. It is a kind of data hiding technique that provides another way of security protection for digital image data. Unlike utilizing a particular cipher algorithm to protect secret data from illicit access, the purpose of steganography is to embed secret data in preselected meaningful images, called cover images, without creating visually perceptible changes to keep an invader unaware of the existence of the secret. Cover media can be a text, or an image or an audio or video etc. It is an art of hiding information in ways a message is hidden in cover media so that will not arouse an unintended observer. Observers are unfamiliar that a covert message is being connected. Only the sender and receiver of the message notice it.

The basic components of any digital communication system are the transmitter, the channel or medium of transmission, and the receiver, and nowadays there are many digital communication technologies for different applications. The available technologies include the Bluetooth, the wireless USB (UWB), the WIFI, the WIMAX, the Infrared IrDA, the ZigBee, and the cellular technology. Wireless fidelity (Wi-Fi) over IEEE 802.11a/b/g are used for ranges up to 100 meters with a signal rate of 54Mbps, this reasonable speed allows to use these standards for broadband connection from browsing the internet to high definition video delivery. As for the ZigBee standard which is the standards that will be used in this research work.

In this research work, steganography based security approach is considered while image transfer over Wireless Personal Area Network. Zigbee communication will be used for implementation of the communication network, along with providing security using the steganography approach. The major research objectives is to implement a secured steganography based image transfer technique with the designed WPAN network module.

## II. Literature Review

Several Steganography is the art of hiding information imperceptibly in a cover medium. The word “Steganography” is of Greek origin and means “covered or hidden writing”. The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio files, video files etc. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. A message in cipher text might arouse suspicion on the part of the recipient while an ”invisible” message created with steganographic methods will not. Anyone engaging in secret communication can always apply a cryptographic algorithm to the data before embedding it to achieve additional security. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered [4]. According to, “Steganography’s niche in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection. In order to resolve the information disclosure among the devices, several techniques have been suggested.

The techniques based on cryptography generally, contains a pair of algorithms, which converts plaintext (secret messages) into cipher text (encryption) in the sender side and converts it back to plaintext (decryption) in the recipient side [5]. Nevertheless, due to the constraint of conventional cryptography in devices, which demands more processing and memory, lightweight cryptography is used [6]. Lightweight cryptography is a method that specialized in constrained environments such as RFID tags, sensors, contactless smart cars and healthcare devices. In software implementation, lightweight applications are preferred with smaller code and RAM size, which does not always exploit the security-efficiency trade-offs. The internet of things devices are not able to process strong and complex encryption schemes, therefore, lightweight encryption cryptography methods can be used. Although the sensitive information is in unreadable format, attackers may still be able to uncover or decrypt it with sufficient time or processing power. In addition, the encryption does not hide the existence of information or messages from the sight of the attackers [8]. As a result, steganography approach can be used as an alternative security mechanism for transferring the data in a secure manner.

Steganography on the other hand, is a method to make confidential information and messages undetectable and prevent hackers from detecting them [9]. With steganography, attackers will not be aware of the information being transmitted through a channel. In addition, several researchers have used image steganography on low processing power devices, such as embedded devices and mobile phones for hiding the data. The shift from cryptography to steganography is due to that concealing the image existence as stego-images enable to embed the secret message to cover images. Steganography conceptually implies that the message to be transmitted is not visible to the informal eye.

## III. Digital Communication Using Zigbee

An LR-WPAN is a Low Rate Wireless personal Area network that is simple, low-cost and allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol. [20]

Two different device types can exist in an IEEE 802.15.4 network:

- Full-function device (FFD) which has the routing capabilities.
- Reduced-function device (RFD) which does not have any routing capabilities, it just tries to connect to the nearest relevant FFD.

The full-function device (FFD) can operate in three modes

- Personal area network (PAN) coordinator
- Coordinator
- End Device.

ZigBee Protocol is built on top of the IEEE 802.15.4 standard. ZigBee provides routing and multi-hop functions to the packet-based IEEE 802.15.4 standard protocol. It is designed for very low-cost, very low-power consumption, two-way, wireless communications standard. Solutions that use the ZigBee standard are embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, and games [21].

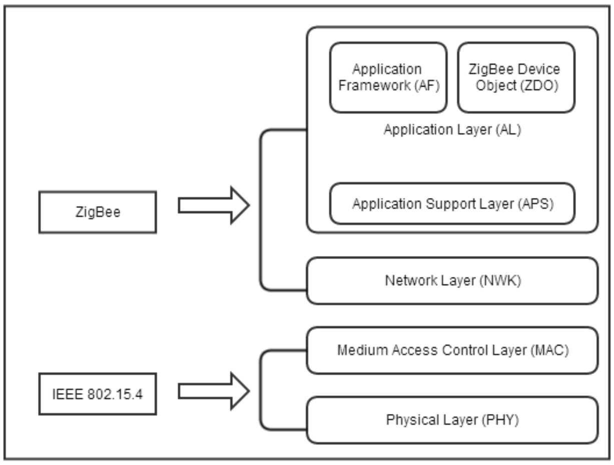

ZigBee
IEEE 802.15.4
Application Framework (AF)
ZigBee Device Object (ZDO)
Application Layer (AL)
Application Support Layer (APS)
Network Layer (NWK)
Medium Access Control Layer (MAC)
Physical Layer (PHY)

Fig. 1: Zigbee Architecture

The ZigBee stack architecture is made up of a set of layers. Each layer performs a specific set of functions and services for the layer above. These layers are the Physical Layer (PHY), Medium Access Layer (MAC), the Network Layer (NWK), and Application Layer (AL), which in turn consists of the Application Support Layer (APS), Application Framework (AF), and ZigBee Device Object (ZDO) as shown in Figure 1.

## IV. System Implementation

The steganography technique has been used to provide security over the communication system created using the Zigbee module. The outcome of the project is a wireless communication system that’s capable of sending images from one end to other. To provide security to images being transferred, the steganography method is used. Image steganography added advantage and has been employed in this research work. The stego image or the hidden image is added at the transmitter stage to form the transmitter message i.e. image. After recovering the image at the receiver end, suitable recovery algorithm is applied to obtain the cover image and the hidden stego image separately. The stego image is converted into a numeric key. The bits of this numeric key is added to the Least Significant Bit of the cover image. This results into an embedded image which resembles the original cover image but has the stego image hidden inside it. This image is then transferred through a standard Zigbee transmitter employing IEEE 805.14 communication standards. The connection between the coordinator and the PC will be through universal serial Bus (USB). This USB connection will be a serial-USB adapter as most commercial available components use this approach of communicating. For the coordinator and the PC to communicate properly a communication protocol will be designed to provide this function. At the receiver end, the Zigbee receiver module receives the image and sends to the software which applies the reverse process by calculating the liner index of the third dimension of the received image.

The transmitter part of the system has been explained with the help of the process flow diagram as shown in the Figure 2. As shown in the diagram, the image on which the steganography is to applied is selected from the image options available by browsing through the file folder. The image is then converted to grayscale format. Then the system asks to input the stego image which is again selected by browsing through the available images. The Least significant bits of the cover image are indexed using linear indexing method and the bits of stego image are embedded as explained in the below discussion. This forms the steganography image. The image is then transferred over the Zigbee transmitter module.

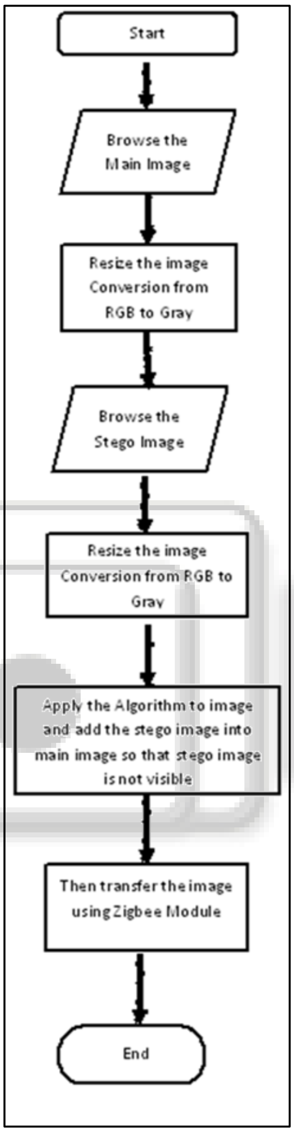

Start
Browse the Main Image
Resize the image Conversion from RGB to Gray
Browse the Stego Image
Resize the image Conversion from RGB to Gray
Apply the Algorithm to image and add the stego image into main image so that stego image is not visible
Then transfer the image using Zigbee Module
End

Fig. 2: Embedding Process

The embedding algorithm is as given below:

```
1)  img: the cover image
2)  img_logo: stego image to be hidden
3)  dim: Size of stego image
4)  if prod(size(img)) >= (prod(dim)*8+32)
    len=prod(dim)+4;      Stego image size
5)  im_w=img_logo(:);
6)  im=img(:);
7)  im=bitand(im,uint8(ones(length(im),1)*254));
8)  for j=1:bin=dec2bin(dim(j),15);
        for i=1:15
                index=(j-1)*15 +i;
                if(bin(i)=='1')
                if  length(varargin)==3
                             im(p(index))=bitset(im(p(index)),1);
    else
                         im(index)=bitset(im(index),1);
                         end
                        end
                        end
                   if length(varargin)==3
                  im(p(30+j))=bitset(im(p(30+j)),1);
        else
                  im(30+j)=bitset(im(30+j),1);
        end
             end
        end
```

The receiver process is initiated by triggering the receiver part of Zigbee module to accept the data transmitted from the transmitter side. The received image is stored in the database. The de-stego algorithm or the extraction algorithm is then applied to retrieve the hidden stego image from the received image. Thus, hidden image or stego image is retrieved is displayed separately. The flowchart in figure 3 shows the extraction process.

```
1)  im_w: received image
2)  Calculate linear index of pixels in the first two dimension
3)  Preallocate the image size matrix
4)  Check all the pixel positions
   while k<len,
          for j=1:8
         index=(k-1)*8 + j;
              if length(varargin)==2
              b=bitget(im_w(p(index-32)),1);
             else
               b=bitget(im_w(index),1);
               end

           if b==1
           im_log(k-4)=bitset(im_log(k-4),j);
           end
         end
     end
5)  Convert to unsigned integer form
6)  Reshape to form the image
```

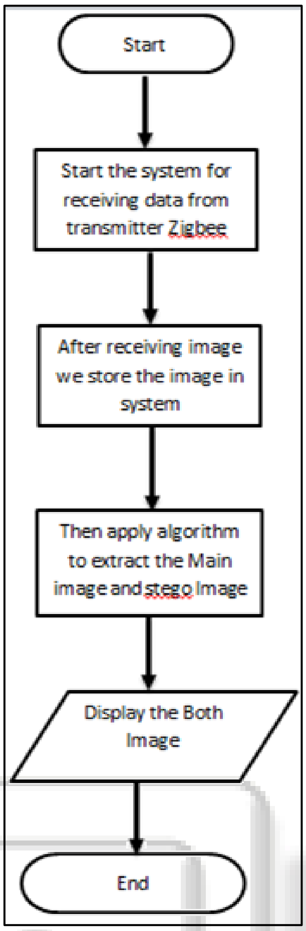
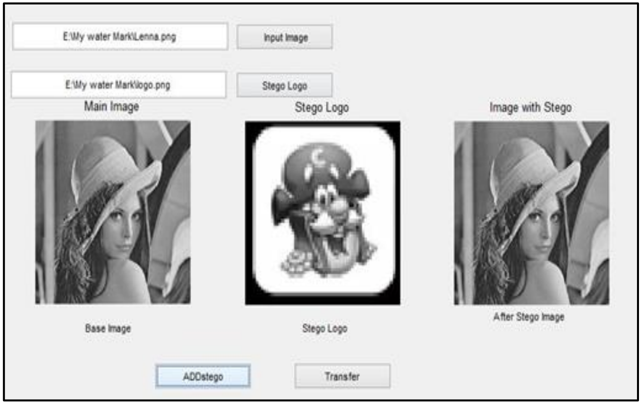

Start
Start the system for receiving data from transmitter Zigbee
After receiving image we store the image in system
Then apply algorithm to extract the Main image and stego Image
Display the Both Image
End

Fig. 3: Extraction Process

## V. Result & Analysis

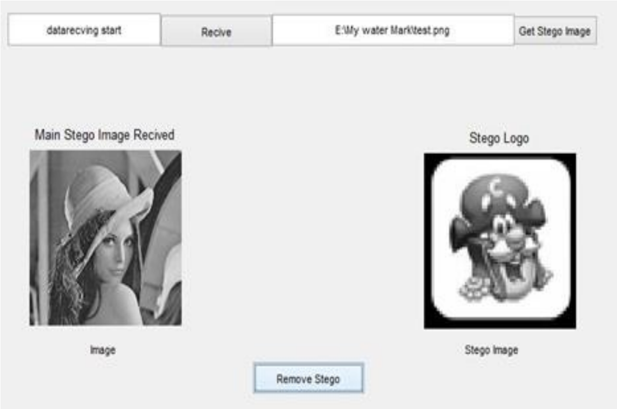
The algorithm has been implemented in MATLAB software tool. A GUI has been implemented to browse and select images from the hard disk. One tab selects the Original Image and the other the watermark image. The the third window shows the final stego image. The results with lena image as cover image are shown in Figure 4 below:


E:\My water Mark\Lenna.png

E:\My water Mark\logo.png

Fig. 4: Cover Image with Stego Image

At the receiver side the images received and the extraction algorithm has been implemented to extract the hidden stego logo from the received image. The GUI at the receiver side is as shown below.


datarecving start

E:\My water Mark\test.png

Fig. 5: Extracted Stego Logo

The stego image is retrieved by clicking on the remove stego pushbutton and the retrieved image is displayed along with the original image.

## VI. Conclusion

The Steganography provides an efficient means of secure data communication especially for image data. A number of steganography methods exist like text, audio and image steganography. In this research work, an image based steganography method has been implemented. The stego image or the hidden image is added at the transmitter stage to form the transmitter message i.e. image. After recovering the image at the receiver end, suitable recovery algorithm is applied to obtain the cover image and the hidden stego image separately. The stego image is converted into a numeric key. The bits of this numeric key is added to the Least Significant Bit of the cover image. This results into an embedded image which resembles the original cover image but has the stego image hidden inside it. This image is then transferred through a standard Zigbee transmitter employing IEEE 805.14 communication standards. The connection between the coordinator and the PC has been done through universal serial Bus (USB). At the receiver end the receiver Zigbee module receives the message and deciphers the hidden image from the received image.

## References

[1] S. Y. Kanawade, Vikas Nagare, Anupam Kumar, Swapnil Dhakane," Secured Wireless Communication Through Zigbee using Cryptography and Steganography.

[2] 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.

[3] 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.

[4] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.

[5] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade , “Image Steganography using Karhunen-Loève Transform and Least Bit Substitution”, International Journal of Computer Applications ,Volume 79 – No9, October 2013, (0975 – 8887).

[6] Privacy and Digital Protection paper, ACMA, June 2013.

[7] Pritam Kumari, Chetna Kumar, Preeyanshi and jaya Bhushan, “ Data Security Using Image steganography And Weighing Its Techniques”, International Journal Of Scientific & Technology Research, Volume 2 ,Issue 11,November 2013. ISSN 2277-8616.

[8] Namita Tiwari and Dr.Madhu Shandilya. Article:Evaluation of Various LSB based Methods of Image Steganography on GIF File Format. International Journal of Computer Applications 6(2):1–4, September 2010. Published By Foundation of Computer Science.

[9] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," Security & Privacy, IEEE, vol. 1, pp. 32-44, 2003.

[10] B. Lakhsmi and B. V. Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor," International Journal of Computer Trends and Technology (IJCTT), vol. 6, pp. 6-14, 2013.

[11] Rafael C. Gonzalez, Richard E. Woods,” Digital Image Processing,Third Edition”.

[12] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, “Comparison of different techniques for Steganography in images”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014.

[13] Kodituwakku, S. R., & Amarasinghe, U. S. (2007). Comparison of lossless data compression algorithms for text data. Indian journal of computer science and engineering, 1(4), 416-425.

[14] Rodrigues, J. M., Rios, J. R., & Puech, W. (2004). SSB-4 System of Steganography using bit 4. In 5th International Workshop on Image Analysis for Multimedia Interactive Services.

[15] Hetzl S.: Steghide (1) - Linux man page [online]. [cit. 2008-05-21]. Available from WWW: http://steghide.sourceforge.net/documentation/manpage.php

[16] Drew Gislason. “ZigBee Wireless Networking”. Newnes, 2004.

[17] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”. The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) , pp 46-51, Nov. 5-8, 2007, Taipei, Taiwan, pp 46-51.

[18] Seong Peng Lim, Gik Hong Yeap. “Centralised Smart Home Control System via XBee Transceivers”. IEEE Colloquium on Humanities, Science and Engineering Research (CHUSER 2011), pp 327-330, Dec. 5-6 2011, Penang.

[19] XBee Family Features Comparison, Digi International. http://www.digi.com/pdf/chart_xbee_rf_features.pdf

[20] IEEE.” Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, 2006.

[21] ZigBee Specification.” ZigBee Document 053474r17”. Sponsored by: ZigBee Alliance, Jan 17, 2008. http://www.zigbee.org/en/.

[22] Glify, http://www.gliffy.com/

[23] Pei, Zhongmin & Deng, Zhidong & Yang, Bo & Cheng, Xiaoliang. (2008). Application-oriented wireless sensor network communication protocols and hardware platforms: A survey. 1 - 6. 10.1109/ICIT.2008.4608532.