LI-FI IN DEFENSE AND SECURITY

Remya Remesh[1], Sariga Raj[2]
[1,2]Division of IT, School of Engineering, Cochin University of Science & Technology

Abstract
Now days the solid state devices are revolutionizing the electronics sector. LEDs are the perfect example for solid state devices. We can replace incandescent and fluorescent lamps with LEDs. They are cost effective, energy efficient and low heat generating devices. Also the life span of LEDs is very large compared to other lamps. The color of light produced by the LEDs is better than that of incandescent and fluorescent lamps. Also they have the ability to be switched in different intensities of light at a very fast rate. This property of LEDs is being utilized in Visible Light Communication Technology. The paper describes the existing applications of visible light and how it can be implemented in defense and security. Currently fiber optic technologies are used in defense. If Visible Light Communication is used, we can replace the wired cables. The paper speaks about the characteristics and difficulties of Visible Light Communication in defense and security.

Index Terms: **Index Terms – Li-Fi, Secure data transmission, Sender Identification, Steganography, VLC Technology**.

I. INTRODUCTION

The visible light spectrum is one among the electromagnetic spectrum which has a bandwidth ranging from 400nm to 700nm. With every year, the number of electronic devices is increasing. This will result in the congestion of wireless networks. Since the visible light spectrum is very much larger than the radio spectrum it can be used for communication. Going towards the right side of electromagnetic spectrum, the wavelength of the signals reduces. A signal with reduced wavelength has a limited coverage area. As the spreading increases the rate of error increases. Hence the VLC technology is designed for short range applications that require high speed of data transmission.

The signal coverage of this technology is limited to a small geographical area. The data in VLC technology is transmitted using an LED bulb. The fast switching of LED light enable data transfer from sender to the receiver. The switching of LEDs is invisible to naked eyes. This property stands the LED out from other kind of lamps. This character enables data encoding at the sender side and decoding at the receiver side. This is how we can use LEDs for both illumination and communication. The RF spectrum is now facing the issue of bandwidth scarcity.

Since visible light spectrum is license free and available this can be used as a perfect replacement for RF waves at least for short range applications. Also we can introduce MAC techniques and multiple access schemes into the VLC technology. This will favor the identification of sender using VLC technology.

II. VISIBLE LIGHT COMMUNICATION

This section deals with the data transmission in VLC. VLC uses white LEDs to transmit data. The detected light intensity is converted into electrical signal using photo detector. The photo detectors in VLC use direct detection technique. Fig. 1 represents the components of VLC.

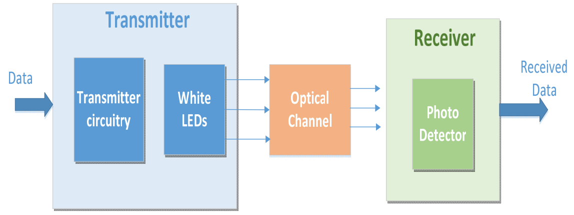


Fig. 1 Components of VLC

A. Transmitter

The data is transmitted using LED lamps. A simple on-off keying modulation is done prior to the transmission. This is achieved from the flickering property of LEDs. In on-off keying the emitted light is considered to contain binary 0s and 1s.

White LEDs can be used as a modulator in the transmitter circuit. The advantages of white LED include: more life span, high brightness and low power consumption. LEDs provide brightness along with data communication. Hence it is effective for indoor communication.

There are two kinds of LEDs providing white Light: RGB LEDs and Phosphor based LEDs. RGB LEDs produce three colors, Red Green and Blue, and produce white light as a combination of these three lights. The prototype developed uses phosphor LEDs, since it is cheaper and less complex than RGB LEDs

B. Receiver

The receiver consists of a photodiode and circuit for demodulating the received signal. A comparator circuit can be used to regenerate the 1's and 0's.

From the optical channel, the optical signal enters into the VLC receiver. The VLC receiver used here is a photo detector. Photodiodes can be used as a photo detector. Photo diode will convert the received optical signal to electrical signal. There are mainly two types of photodiodes: Avalanche Photo Diode (APD) and Positive Intrinsic Negative (PIN) photo diode. Solar cells can also be used as a detector, since this is a green technology.

III. PROPERTIES OF VLC

VLC has both advantages and disadvantages when compared to RF communication. Li-Fi technology is basically a short range communication technology. It needs line of sight communication between sender and receiver to achieve high data rate transmission.

The maximum possible data rate is limited and the data rate can be improved by using high speed switching LEDs. When using light as the medium for communication, there may be a chance of multipath dispersion and interference.

Still VLC has a lot of advantages over RF communication technology like, hazardless to the environment on which the technology is implemented, immune to electromagnetic interference, immune to radio frequency interference. VLC is also eco-friendly and secure. So this can be used in hospitals, petrol pumps, and refineries etc, where the use of radio waves is restricted.

IV. PROPOSED SYSTEM

The purpose of this system is to transmit an image from a sender PC to a receiver PC and identify the sender. Fig 2 shows the block diagram of the proposed system. .

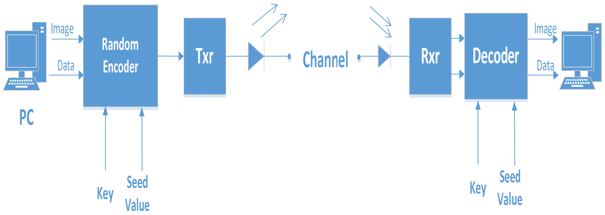


Fig. 2 Proposed System

A text file is encoded in an image and this image file is getting transmitted through visible light. Steganography techniques are used in this VLC system to provide more security to the system. If more than one person is sitting under the coverage of the same LED lamp, then anyone of them can access the data sent through Li-Fi. In order to provide authenticity to the transmitted data steganography is used. At the receiver side the encoded data is decoded from the image. Along with the image, the MAC address of the sender is also sent via light. This address is decoded at the receiver side. Hence we can identify the sender.

A. The Role of VLC In Defense And Security

Ensuring protection against demolition and crime is the fundamental and prime duty of the Defense and Security Corps. National Security is the main aim of the corporation. Loss or Leakage of confidential data is a severe threat to the national security. So Defense and security make use of Intranet services for information storage and transfer. Even if they use private networks, there are security issues like data breaching and data leakage. Beyond traditional email, many more techniques are used for the security like voice over IP, instant messaging etc. There also the chances of confidential data being hacked or leaked are high. A lot of confidential data are being leaked or spilled every year. Since VLC technology is implemented in defense and security, the crimes and demolition of data during data transfer can be eliminated.

Normally the data from intranet is modulated and sent to the receiver. When VLC technology is used amplitude modulation techniques cannot be used as direct detection is used at the receiver end.

Dimming: For the transmission of data from sender to the receiver different levels of illumination is required for the LED. Depending on the application the LED blinking can be changed to different levels. This dimming should not be perceptible by the human eye.

Flickering: While the modulation of data is done the light intensity is changed. The continuous flow of 0s and 1s is considered as the flickering of light.

B. Conference Halls with Li-Fi

C. 2 Conference Halls with Li-Fi

VLC is the most secure way of communication since the signals won’t penetrate through walls. If we are using RF waves inside the conference room, it will get radiated out. So a hacker can easily get that information. VLC needs LOS communication links. Therefore the signals emitted inside a room provide a significant amount of data security and privacy as shown in Fig. 3. Since VLC needs a LOS communication link between sender and receiver, any intervening obstacles can be identified easily. Thus it is preferred in military and national security corporations. Visible light communication will revolutionize the conference halls of defense. We can send information from a PC to anywhere and any system, remotely without using wired connections and with at most privacy and security.

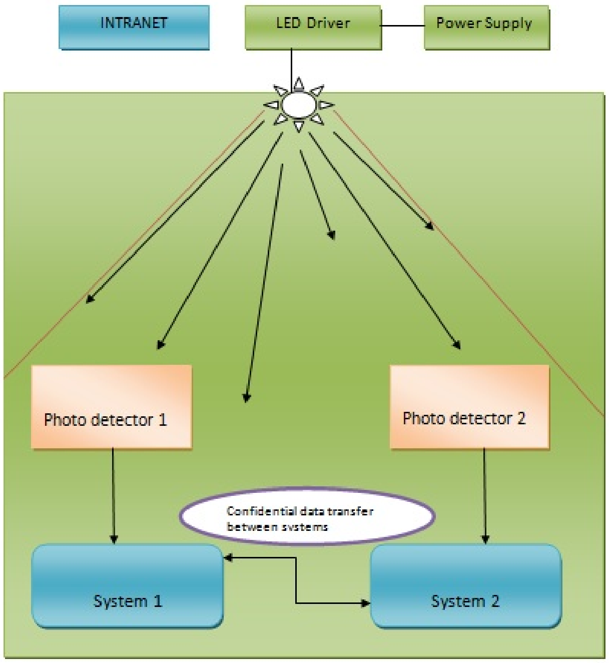


Fig.3 Li-Fi in Conference Hall

This is what actually needs in a highly confidential area like defense. Also the Corps can choose the data reception only from the authorized senders only.

V. WORKING

There are mainly eight phases in the working of the system. They include:

- Extracting the MAC address from sender
- Encoding data into an image
- Converting the encoded image into integers
- Data transmission using LED
- Data reception using photodiodes
- Image reconstruction
- Decoding the data from image
- Retrieving the MAC address at the receiver

A. Extracting the MAC address from sender

Sender identification in this system is done using the MAC address of the sending device. Since the MAC address is a unique one, there will not be any intruders. The MAC address is extracted from the sender PC using the tool MATLAB. This 15 digit MAC address is transmitted along with the encoded image.

B. Encoding data into an image

In LSB encoding, the data is encrypted into each and every pixel's least significant bits. Then the image with data encoded can be detected very easily.In order to overcome that issue, here the method proposed is an encoding technique called random encoding. In this method the LSBs of only randomly selected pixels are changed. The selection of pixels is based on a seed value. This will make the image look unchanged. Here data in three layers of an image, ie. Red, blue and green layers of an RGB image are encoded using a key.

This method is used just to show that an end to end protection of the data is needed in VLC just like in Radio Wave Communication Systems.

C. Converting the encoded image into integers

Each pixel from the image is selected and converted it into integers. And this integer value is transmitted using LED as light.

D. Data transmission using LEDs

The integer values corresponding to each pixel in the form of bit streams are fed to the LED as electrical signals. Based on the intensity of the input (value of each pixel), the LED will modulate the input signal. As the data transmission begins, we can see the flickering of light (slight variations in the visible light) emitting from the LED.

The dimension of the image is also transmitted along with the encrypted message. This will ease the process of reconstructing the image at the receiver side.

E. Data reception using photo diodes

The transmitted data via optical light is received using photo diodes. The photo diode will demodulate the light and convert the optical signal to electrical signals. This electrical signal carries the integer values of each pixel. The output of the photo diode is actually a bit stream of the pixel.

F. Image reconstruction

From the pixel values and the dimension of the image, the encrypted image is reconstructed. We will get it correctly, if and only if there is no dispersion and interference from outside light.

G. Decoding the data from image

From the reconstructed image the data is decoded using the seed value and the private key of the receiver.

H. Retrieving the MAC address

At the receiver side, the transmitted MAC address is also decoded and displayed.

VI. IMPLEMENTATION

Both the transmitter and the receiver are connected to a PC. VLC needs serial communication for LI-Fi. But most of the PCs don't have a serial port. So here, the system uses a USB to TTL converter at both ends.

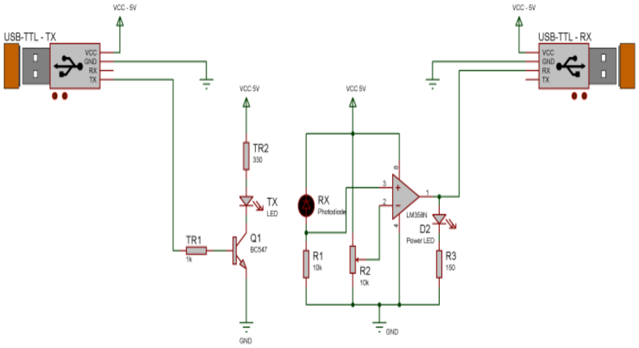


Fig. 4 Hardware Setup

Transmitter circuit

Transistor as a switch circuit is used as the transmitter circuit along with light emitting diode. The transistor used here is 2N2222. We use this circuit to step up 5V to 12V. This 12 V supply is fed to the LED.

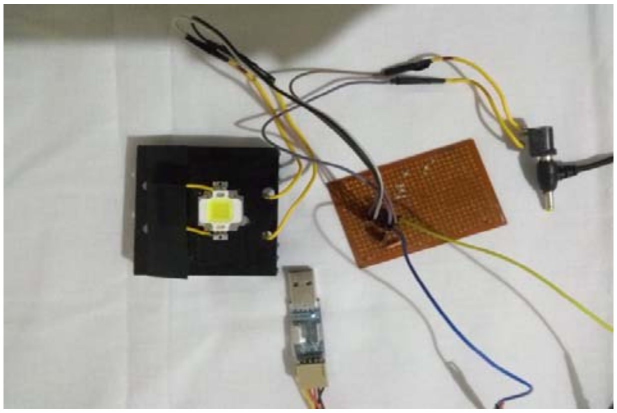


Fig. 5 Transmitter

Receiver circuit

A line follower circuit is used along with the photo diode. The line follower circuit consists of a comparator. This is to convert the received light into bits. It will distinguish the output of photodiode into binary 1 or 0 based on a threshold value.

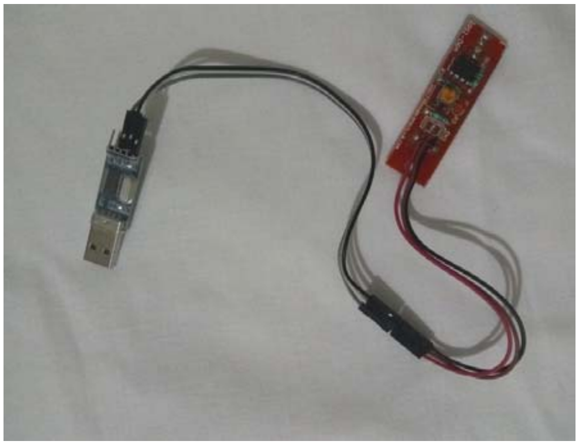


Fig. 6 Receiver

A. Steganography

There may be a number of receivers at the receiver side, when we transmit a data through wireless communication. So the communication should be secret. Only the sender and receiver should know about the data transmitted over the network.

Steganography is the process of embedding a secret message into a normal message [4]. Steganography has a lot of advantages over cryptography. In cryptography, the secret message is present in the external information and that can be seen by human. But in the case of steganography, the secret message is made invisible to the human eye, by embedding the message into digit image or sound signal etc. in this paper we use digital image to encode the secret information [5].

Random Encoding:

It is a variation of LSB encoding, but an advanced version of LSB encoding. In LSB encoding [6], the data is encrypted into each and every pixel’s least significant bits. Then the image with data encoded can be detected very easily.

In order to overcome that issue, here the method proposed is an encoding technique called random encoding. In this method the LSBs of only randomly selected pixels are changed. The selection of pixels is based on a seed value. This will make the image look unchanged. Here data in three layers of an image, ie. Red, blue and green layers of an RGB image are encoded using a key.

This method is used just to show that an end to end protection of the data is needed in VLC just like in Radio Wave Communication Systems.

B. Sender Identification

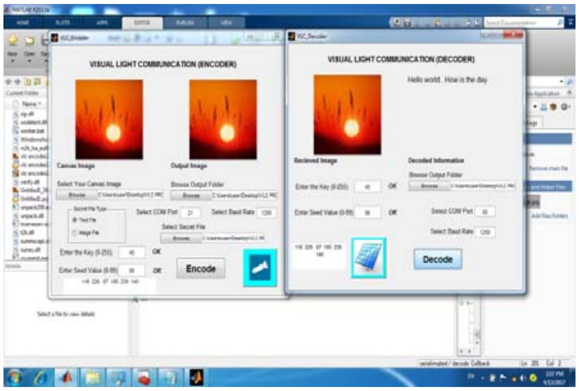
The sender identification in the system is done by retrieving the MAC address. As far as a device is concerned, its MAC address is unique to that system. This MAC address is extracted from the sender device using MATLAB tool and the same is sent to the receiver using visible light.

VII. TEST AND RESULTS

The work is done on MATLAB software. Two GUIs are created, one for transmitter and the other for receiver. For testing, a canvas image is loaded at the encoder side. Encoding should be done before transmission. So a secret text file is also loaded. After setting the baud rate and COM port to which the transmitter circuit is connected, stego key and seed value for encoding should be entered. In order to identify the sender of the information, the MAC address of the sender PC is captured from the sending device.Prior to transmission, encode the text file into the image file. It is possible to encode an image file within an image file. Then also the procedure is same. Before the transmission begins, set the receiver ready for reception.

At the decoder side, set the same baud rate and seed value. Also set the COM port to which the receiver circuit is connected. In order to decode the data, enter the key. After setting these data click on the receiver button. Then click on the transmitter button.

Now the flickering of the LED light is visible to the human eye. This is due to the transmission of the data from one system to the other. This flickering effect can be eliminated by using high speed switching LEDs and increasing the baud rate. When the LED stops blinking it is clear that the complete information is transmitted successfully. Now the secret message is ready to decode. Also the MAC address will be displayed on the screen automatically.



Hello world . How is the day

Fig. 7 Test Result

VIII. CONCLUSION AND FUTURE SCOPE

The possibilities of VLC Technology are numerous and it can be explored further. If this technology can be put into practical use, we can use every bulb as a source of information, ie., something like a Wi-Fi hotspot to transmit wireless data using light.

VLC technology can be implemented successfully only with fast switching LEDs. If low speed switching LEDs are used, there will be interference even with the sunlight. This problem can be solved by using high speed switching LEDs. Baud rate possible for this circuitry is limited to certain Kbps. Beyond that limit the photo diode will not detect the incoming signals. Transmission of black and white images is not possible since we use random encoding in 3 layers. The baud rate of transmitter and receiver should be the same.

There will be interference if another LED light is present inside the same room. So the data transmission may not be successful. To overcome this issue we can incorporate multiple access techniques like TDMA. In addition to sender identification, we may include the location of the sender also.

REFERENCES

[1] H. Haas and C. Chen, “What is Li-Fi?” in Proc. 41st Europ. Conf. on Optical Commun. (ECOC), Sept 2015, invited.

[2] S.Singh ,G.Kakamanshadi, S. Gupta, “Visible Light Communication An Emerging Wireless Communication Technology” Proceedings of 2015 RAECS UIET Panjab University Chandigarh 21-22nd December 2015

[3] P.Cherntanomwong,W. Chantharasena “Indoor localization System Using Visible LightCommunication” 2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE), Chiang Mai, Thailand

[4] Bhavana.S,L.Sudha” Text Steganography Using Lsb Insertion Method Along With Chaos Theory”

[5] M. S. Sutaone, M.V. Khandare” Image Based Steganography Using LSB Insertion Technique”

[6] M. Juneja, P. Singh Sandhu “Designing of Robust Image Steganography Technique Based on LSB Insertionand Encryption” 2009 International Conference on Advances in Recent Technologies in Communication and Computing

[7] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, “LED Based Indoor Visible Light Communications: State of the Art,” Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1–1, 2015.

[8] F.Khan,S.R.Jan,M.Tahir,S.Khan “Applications, Limitations, and Improvements in Visible Light communication Systems” 2015 International Conference on Connected Vehicles and Expo (ICCVE)

[9] A.Sewaiwar, P.P.Han, and Y.H.Chung ” 3-Gbit/s Indoor Visible Light Communications Using OpticalDiversity Schemes” IEEE Photonics Journal Volume 7, Number 6, December 2015

[10]C.Liao, Y.Chang, C.Ho, and M.Wu “Light-Emitting Diodes for Visible Light Communication” IEEE journal 2015

[11]IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: “Short-Range Wireless Optical Communication Using Visible Light”, IEEE Standard 802.15.7, 2011.

[12]P.H. Pathak, X.Feng, P.Hu, And P.Mohapatra ”Visible Light Communication, Networking, Andsensing: A Survey, Potential Andchallenges” IEEE Communications Surveys & Tutorials, Vol. 17, No.4,Fourthquarter2015

[13]F. Demers, H. Yanikomeroglu, and M. St-Hilaire, “A survey of opportunities for free space optics in next generation cellular

networks," in *Proc.9th CNSR*, May 2011, pp. 210–216.

[14]T. Komine and M. Nakagawa, "Fundamental analysis for visiblelight communication system using LED lights," *IEEE Trans. Consum.Electron.*, vol. 50, no. 1, pp. 100–107, Feb. 2004.

[15]M. V. Bhalerao, S. S. Sonavane, V. Kumar, "A Survey of Wireless Communication Using Visible Light", *International Journal of Advances in Engineering & Technology*, Vol-5, Issue-2, pp: 188-197, January 2013.

[16]K Kanthikumar, D.Koteswara Rao, Dr. A. Yesu Babu And Dr. P. Premchand, "An alternative communication technology: based on white LED's in visible light communication", *IJECT*, Vol: 2, Issue: 1, pp: 168-172, 2011.

[17]Ravi Kumar, Kavita Choudhary, Nishant Dubey, **"**An Introduction of Image Steganographic Techniques and Comparison", International Journal of Electronics and Computer Science Engineering

[18]DeepeshRawat,VijayaBhandari,"SteganographyTechnique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications,Vol.67, No.1, April 2013, pp.22-25.