DOI: 10.21917/ijct.2015.0165

INTERFACING VISIBLE LIGHT COMMUNICATION WITH GSM NETWORKS TO PREVENT THE THEFT OF THE VEHICLE

P. Prabu[1], N. G. Bhuvaneswari Amma[2] and G.Annapoorani[3]

[1,2] *Department of Computer Science Engineering, Indian Institute of Information Technology - Srirangam, India*

E-mail: [1]prabususti@gmail.com, [2]ngbhuvaneswariamma@gmail.com,

[3]*Department of Information Technology, Anna University, BIT Campus, India*

E-mail: pooranikrish@gmail.com

Abstract

Visible Light Communication (VLC) by means of white Light Emitting Diode (LED) is an alternate and most promising technology for existing Radio Frequency (RF) communication. We proposed one of the important applications of VLC to prevent the theft of the vehicle. Every year approximately 36,000 vehicles worth Rs.115 crores are stolen in India. In critical road condition, only 15,000 are traced and many spare parts of vehicle are found missing. Even the existing technologies have some disadvantages related to the problem stated. In our paper, we dealt with the data communication through LED. One of the optical wireless communication having short range is called as VLC whose visible light spectrum starts from 380 nm and ends at 780 nm and it has an incomparable data rate of 10GB/s whereas the speed is 1MB/s on Bluetooth and for Infra Red (IR) the speed is 4MB/s. We try to achieve the communication through VLC between 1) car - car to prevent the accident and 2) car - tollgate and received signal from tollgate is transmitted to Global System for Mobile communication (GSM) network using microcontroller to prevent the theft of vehicle. To enhance the security of VLC, Advanced Encryption Standard (AES) algorithm is used and the result is illustrated with the help of LabVIEW.

Keywords:

Visible Light, White LED, AES, GSM, Bluetooth

1. INTRODUCTION

Recently developed Visible Light Communication technology seeking to create an ultra-high speed, highly secured, biologically and friendly communication networks that allow the creation and expansion of continuous computing applications using light characterized by very large bandwidth high-frequency pulses instead of radio waves and microwaves [1]. VLC is the short-range optical wireless communication [11], [13], [20] using the visible light spectrum from 380 to 780 nm. With ~300THz of bandwidth [16] available for VLC, gigabit data rate-per second could be achieved over short distances [2], [8].

This widespread of bandwidth removes one of the major difficulties faced by communication techniques. Some of the noted advantages of VLC over RF and IR based systems are:

1. Higher security than existing RF communication system.
2. Unlike in IR [7] communication system, no restriction on transmission power.
3. No regulations in the use of the visible electromagnetic spectrum.
4. The key advantage of VLC is the duality in the use of the visible light. The same light is used for both communication and illumination applications such as domestic light bulbs, traffic lights [4] and LED TVs.

The main reasons for using LED in VLC are high usage of bandwidth, non-expensive and very simple transmitter and receiver circuit, eco-friendly and long life expectancy.

An interesting fact is that VLC systems can transmit data more securely over very short distances rather than other communication devices whose signals can be easily detected outside the rooms and buildings they originate in [2], [14], [17]. So, VLC using white LED [5] is a secure way of communication as encryption and decryption is possible in this technique [3], [9], [12]. The Fig.1 shows the VLC technology in which white LEDs are used.

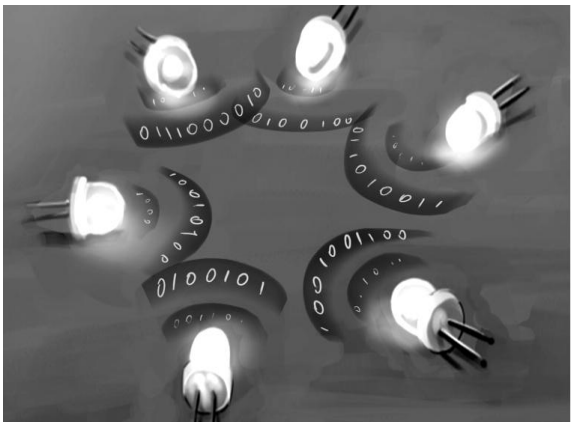

Fig.1. VLC Technology

2. EXISTING METHODS

Existing technique for theft prevention are Audiovox car alarm, CCTV camera system and Theft preventer alarm. The operation of each technique is explained below: Audiovox car alarm [21] is a multi-tone self-contained automotive alarm can scare any thief away with its siren and it has the drawbacks such as it can tend to cause havoc at night as its multi-tone siren will chase your neighbours away as well, unlike auto pagers that will alert silently. CCTV camera system [21] sounds straight forward that in which signal is sent from camera to monitor and recorder by means of a secure link rather than being broadcast. The secure link could be cable, microwave or even infra-red and it has the following drawbacks such as they are very costly, and they do not always work and manipulate with people's privacy. Theft preventer alarm [19] uses a 555 timer IC which can be used as an alarm system to prevent the theft of the vehicle. The alarm goes ON when a thin wire, usually as thin as a hair is broken and it has following disadvantages such as battery dependence, stopping the alarm by operating manually.

3. PROPOSED SYSTEM ARCHITECTURE

The Fig.2 shows the proposed architecture and it contains five parts namely transmitter module, receiver module, microcontroller, GSM network and mobile phone. VLC system permits point to point communication which avoids problems arises due to interference.

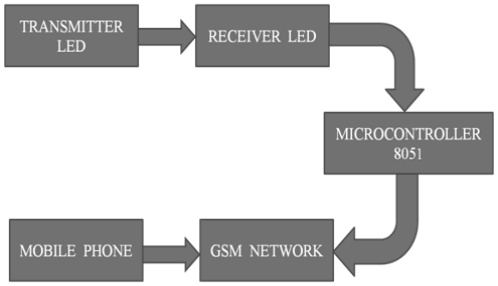

Fig.2. Proposed Architecture

In our work, LED transmitter sends the location of the car to the receiver in the vehicle. The receiver LED is connected with 8051 microcontroller and it receives the data and sends the message to the mobile phone through GSM networks. Thereby, exact location of the car can be found out and theft is prevented. Another noticeable point is that with the help of VLC using LED, we can prevent the car accidents by data communication between two cars thereby resulting automatic break to the car. The information about the particular location including city name, area name are transmitted from toll gate to car through LED and those retrieved information is allowed to arrive at the GSM network by means of 8051 micro controller. So, that the location where the car is located currently is made to receive immediately by the car owner's mobile phone via Short Message Service (SMS).

3.1 TRANSMITTER MODULE

In the transmitter module, the transmitter LED is used to send the data and design of it should be comfortable than other optical light sources. Various kinds of modulation technique are adopted to modulate the LED [10]. LED blinks are harmful to human eyes while transmission so when the same LED is used for illumination it will be safe and comfortable for human eyes. There may be a chance for the receiver occupant to block the incoming light beam, so more than two LED lamps in the transmitter side can be modulated simultaneously from different directions to cover a larger recipient area. In case where the receiver loses connection with the one of the transmitter, it can be able to receive same data from another transmitter at the same time. The Fig.3 explains the VLC transmitter circuit.

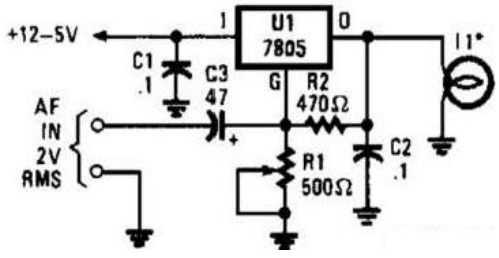

Fig.3. Visible Light Communication Transmitter

A 7805 voltage regulator is connected in a variable-voltage configuration, and an audio signal is given to the common input, to modulate the output voltage in the visible-light transmitter. The modulated output voltage is used to transmit intelligence via an LED/incandescent lamp [15].

3.2 RECEIVER MODULE

A receiver module is generally composed of PIN detectors/photodiode/Receiver LED and signal conditioning circuit which is the most important part of the receiver part. The signal from output detector/diode/LED is usually very weak with a lot of noise and there may be the chances for receiving data getting corrupted. So the receiver's PIN photo detector/diode/LED is connected to a trans-impedance amplifier which transforms the receiving current signal into a voltage signal. A high pass filter is applied next in order to filter out various types of noises present in the signal. At Last, the signal is finally amplified by an amplifier and reshaping is done by comparator.

In visible-light receiver, in order to increase range amplitude-modulated light signals takes the help of phototransistor Q1 which is mounted in a parabolic reflector. Phototransistor can be any NPN transistor. The amplifier Q3 is driven by emitter follower Q2. The output of the amplifier Q3 is given to volume control R7 and audio amplifier U1. For receiver, minimum of 9-V and maximum of 12-V supply is recommended. The Fig.4 explains the VLC receiver circuit.

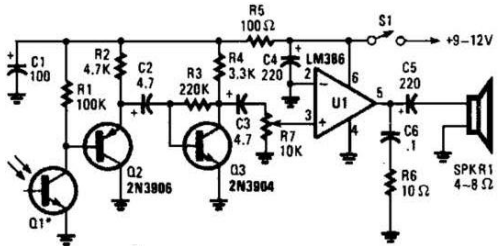

Fig.4. Visible Light Communication Receiver

3.3 8051 MICROCONTROLLER

AN Intel product is the 8051 microcontroller which is MCS-51 families 1st microcontroller. The market share of 8051 family and its enhanced members is calculated to be approximately 40%, compared to other microcontroller families. And it has special features such as microcontroller has on chip peripheral devices. 8051 microcontroller other special features are as follows:

1. 12 MHz clock. Processor instruction cycle time 1 µs.
2. An 8-bit ALU.
3. Harvard memory architecture – having separate external program memory and data memory.
4. 8-bit internal data bus width and 16-bit internal address bus – Harvard memory architecture
5. Follows CISC (Complex Instruction Set Computer) architecture.

The Fig.5 shows how to interface the LED with microcontroller. As in the figure anode is connected to Vcc with the help of resistor R1 and the cathode is connected to the

Microcontroller pin. The relationship between port pin and LED is that when the Port Pin goes HIGH, the LED gets OFF and when the Port Pin goes LOW, the LED gets ON.

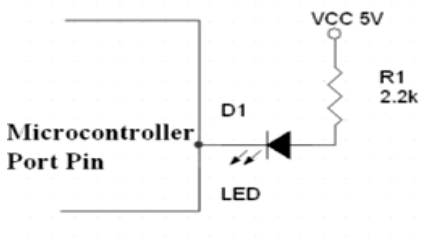

Fig.5. Interfacing microcontroller with LED

The microcontroller used here to interface LED is ATmega32.

The interesting features of this controller are as follows:

1. High-performance, Low-power 8-bit Microcontroller
2. Advanced RISC Architecture.
3. High Endurance Non-volatile Memory segments.
4. JTAG (IEEE std. 1149.1 Compliant) Interface

3.4 GSM NETWORK

A standard set named Global System for Mobile Communications (GSM), developed to describe protocols for (2G) second generation digital cellular networks used by mobile phones. GSM can be considered as that of a digital mobile telephony system. The function of GSM is to digitize the data and then compresses data, at last send it to a channel with two other user data streams, each in its own particular time slot. It operates at two frequencies either at 900 MHz or 1800 MHz frequency band.

The GSM module can communicate with mobile phones with the help of microcontroller through UART. To communicate over either UART or USART, we need three basic signals namely, RXD (receive), TXD (transmit) and GND (common ground). GSM modem interfacing with microcontroller can be used for applications such as SMS control of industrial equipment's. The SMS sending with the help of GSM modem when it is interfaced with microcontroller or PC is very much simple when it is compared with that of sending SMS by UART. With the help of modem, Text message may be sent by interfacing three signals of the serial interface of modem with microcontroller i.e., with TxD, RxD and GND. In this scheme RTS and CTS signals of serial port interface of GSM Modem are connected with each other. The serial port transmit signal of microcontroller is connected with transmit signal (TxD) of the serial interface of GSM Modem on the other hand receive signal of microcontroller serial port is connected with receive signal (RxD) of GSM Modem serial interface. The text mode SMS messages can contain maximum of 140 characters at the maximum. It depends upon the how much amount of information that can be collected from GPS Engine that is needed at the base station for tracking vehicle or person.

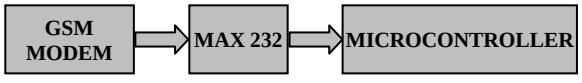

Fig.6. Interfacing GSM modem with microcontroller

LabVIEW GSM tool box is a mandatory tool for systems programmers, developers and integrators in LabVIEW environment. It helps us to quickly use various modem features such as GSM-GPRS serials modems and standard AT modems in easy and intuitive way with the help of low level and high level functions. Icons are organized in such a way that it has to be linked in cascade mode to initialize, open and manage communication and data exchange through a serial modem.

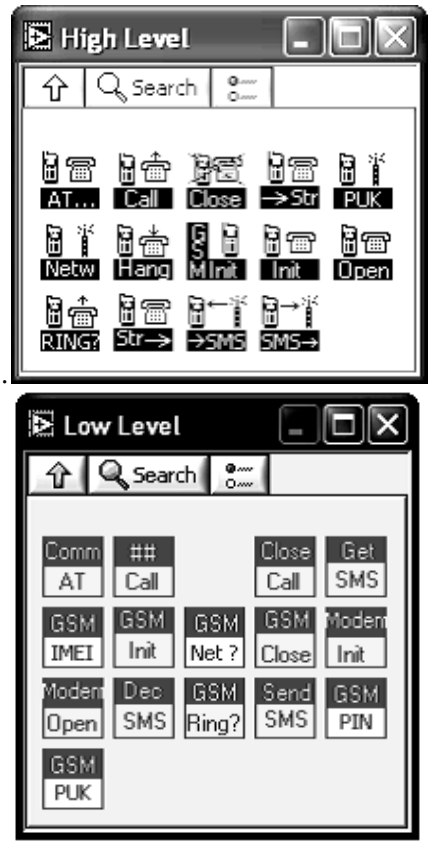

Fig.7. GSM tool box in LabVIEW

4. SECURITY IN VLC

VLC is more secure than the existing RF communication systems because it uses visible light to transfer digital data from transmitter to receiver. As light intensity is very high eavesdropping is not possible, because when intruder wants to hack a data the intensity of two lights get collapsed and data get lost and it cannot be recovered by intruder. Unlike in RF communication system, multipath propagation and interference is not possible in VLC because direct line to sight communication is enhanced in VLC.

One more advantageous point is LED transmission is broader in fashion unlike narrow transmission in LASER so with the MIMO configuration of LED fastest data communication is achieved in VLC [6]

Security can be done by simple digital addition, subtraction, multiplication, division, logical AND, logical exclusive OR, logical OR or two or more combination of original plain text and key. The transmission of signals in visible light communication is done by blinking the light signals. One of the visible light communication fascinating features is ability to the see the

transmission of signal area. Visible light communication can very easily create a small network; let us take an example of partition or per a room basis [3], [18]. For intruders/malicious users trying to connect to such small network, it is necessary to enter in the service provided area. Thus the administrator can easily manage all users in the network. For the enhanced security of VLC, we proposed AES in our work in LabVIEW. A switch is connected in serial mode with LED which is in serial with FOR loop execution of AES algorithm. Whenever the switch gets on LED turns on and transmits the data following AES algorithm.

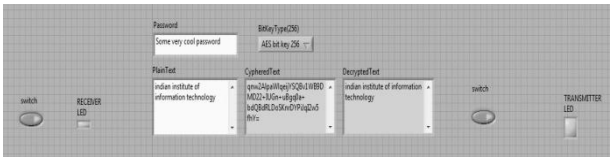

Fig.8. AES algorithm implementation in LabVIEW

AES is a symmetric key block cipher. That implies that same key is used for both encryption and decryption part of algorithm. However, AES is quite different from DES by many criteria. The algorithm follows word block size of 128 bits and key size of 128 bits and not just like that of 64 and 56 bits of DES block and key size. The block and key size can be chosen independently from 128, 160, 192, 224, 256 bits and not necessarily be the same size. However, the AES standard follows a predefined rule and it states that the algorithm can accept a block size of 128 bits and we have choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name can be changed to AES-128, AES-192 or AES- 256 respectively. AES differs from DES in which it is not a feistel cipher. In a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are exchanged. In this algorithm, the entire data block is processed in parallel during each round using operations such as substitutions and permutations.

A number of AES parameters depend on the key size. For instance, if the key size used is 128 then the number of rounds is 10 whereas for 12 and 14 rounds, the key size is 192 and 256 bits respectively. At recent the most commonly used key size is 128 bit key.

Table.1. Key-block-round combination of AES

AES VERSIONS	KEY LENGTH	BLOCK SIZE	NUMBER OF ROUNDS
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Encryption and decryption in LabVIEW software can be done in different languages such as Latin and Cyrillic. Encrypted text is an ASCII text through which it can be transmitted via network without being corrupted on the wire. Another interesting and useful feature of this algorithm is that, encryption algorithm will produce new ciphered text each and every time and it will be correctly decrypted if and only if passwords are matched for the same plaintext and password. There is no major difference between 256 and 128 bit modes of operation, so to increase complexity it's better to use 256 key mode for security.

Table.2. Secret Key Algorithm Comparison

Sl. No	ALGORITHM	KEY LENGTH	COMMENTS
1.	DES	56 BITS	TOO WEAK TO USE
2.	TRIPLE DES	112 – 168 BITS	2nd BEST CHOICE
3.	AES	128 – 256 BITS	BEST CHOICE
4.	IDEA	128 BITS	PATENTED
5.	RC4	1 – 2048 BITS	SOME KEYS ARE WEAK
6.	RC5	128 – 256 BITS	PATENTED
7.	BLOWFISH	1 – 448 BITS	OLD AND SLOW

5. CONCLUSION

We analyzed the Performances of security of VLC by investigating AES algorithm. We proved that AES algorithm with 256 bit key size provides high security of VLC. Data that are transmitted over existing RF communication are always prone to security issues. This problem is addressed in our paper and we made a solution to this by providing AES algorithm and this makes VLC technology suitable for all kind of communication applications. In future, we will try to achieve the communication through VLC between cars to prevent the accident. Thus, VLC using white LED is a secure way of communication as encryption and decryption is possible in this technique.

REFERENCES

[1] P. Prabu, R. Manikandan and M. Pradeep, "Performance Enhancement of Data Communication through Visible Light Communication Using On Off Keying", *International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 2, No. 2, pp. 559-563, 2013.

[2] A. Suban, P. Prabu, R. Manikandan and M. Pradeep, "Mitigating Effect of Flickering & Dimming in Visible Light Communication Using MIMO", *International Journal of Electrical and Computing Engineering*, Vol. 1, No. 1, pp. 8-12, 2014.

[3] Kuniyoshi Okuda, Takuya Yamamoto, Tomoo Nakamura and Wataru Uemura, "The Key Providing System For WirelessLan Using Visible Light Communication", *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, Vol. 5, No. 3, pp 13-20, 2014.

[4] Mohsen Kavehrad, "Sustainable Energy Efficient Wireless Applications Using Light", *IEEE Communications Magazine*, Vol. 48, No. 12, pp. 66-73, 2010.

[5] P. Amirshahi and M. Kavehrad, "Broadband Access over Medium and Low Voltage Power-lines and use of White Light Emitting Diodes for Indoor Communications", *IEEE Consumer Communications and Networking Conference*, Vol. 2, pp. 897-901, 2006.

[6] D. O'brien, Hoa Minh, G. Faulkner, Kyungwoo Lee, Daekwang Jung, Yunje Oh and Eun Tae Won, "High Data Rate Multiple Input Multiple Output (MIMO) Optical Wireless Communications Using White LED Lighting", *IEEE Journal on Selected Areas in Communications*, Vol. 27, No. 9, pp. 1654-1662, 2009.

[7] J. M. Kahn and J. R. Barry, "Wireless Infrared Communications", *Proceedings of the IEEE*, Vol. 85, No. 2, pp. 265-298, 1997.

[8] G. Pang, T. Kwan, H.Liu, C.-H.Chan, "LED Wireless: A Novel use of LEDs to transmit audio and digital signals", *IEEE Industry Applications Magazine*, Vol. 8, No. 1, pp. 21-28, 2002.

[9] Jae Kyun Kwon, "Inverse Source Coding for Dimming in Visible Light Communications Using NRZ-OOK on Reliable Links", *IEEE Photonics Technology Letters*, Vol. 22, No. 19, pp. 1455-1457, 2010.

[10] Hidemitsu Sugiyama, Shinichiro Haruyama and Masao Nakagawa, "Experimental investigation of modulation method for visible-light communications", *IEITC Transactions on Communication*, Vol. 89-B, No. 12, pp. 3393-3400, 2006.

[11] Dominic O'Brien and Marcos Katz, "Short-Range Optical Wireless Communications", *Wireless World Research Forum (WWRF11)*, 2004.

[12] T. D. C. Little, P. Dib, K. Shah, N. Barraford, and B. Gallagher, "Using LED Lighting for Ubiquitous Indoor Wireless Networking", *IEEE International Conference on Wireless and Networking and Communication*, pp. 373-378, 2008.

[13] Dominic O'Brien, "Indoor optical wireless communications: recent developments and future challenges", *Proceedings of SPIE*, Vol. 7464, 2009.

[14] Grantham Pang, Chi-ho Chan, Hugh Liu, and Thomas Kwan, "Dual use of LEDs: Signalling and Communications in ITS", *Proceedings of the 5th World Congress on Intelligent Transport Systems*, 1998.

[15] M. G. Craford, "LEDs challenge the incandescents", *IEEE Circuits and Devices Magazine*, Vol. 8, No. 5, pp. 24-29, 1992.

[16] J. Grubor, S. Randel, K. D. Langer and J. Walewski, "Bandwidth Efficient Indoor Optical Wireless Communications with White Light Emitting Diodes", *6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, pp. 165–169, 2008.

[17] Yuichi Tanaka, Toshihiko Komine, Shinichiro Haruyama and Masao Nakagawa, "Indoor Visible Light Data Transmission System Utilizing White LED Lights", *IEICE Transactions on Communications*, Vol. E86-B, No. 8, pp. 2440–2454, 2003.

[18] T. Komine and M. Nakagawa, "A Study of Shadowing on Indoor Visible-Light Wireless Communication Utilizing Plural White LED Lightings", *1st International Symposium on Wireless Communication Systems*, pp. 36-40, 2004.

[19] http://www.circuittrue.com/theft-preventer-alarm-circuit-using-a-555-timer-ic/

[20] WG802.15 - Wireless Personal Area Network (WPAN) Working Group, "P802.15.7 - Standard for Short-Range Wireless Optical Communication using Visible Light", *IEEE Standard Association*, 2011.

[21] http://www.monitoryourassets.com/ip-vs-analog/