"Wireless Image Transmission Using Visible Light Implementing Steganography"

Suraj Sonmale[1], Suash Sinha[2], Kshitija Sawant[3], Pratik Thite[4], Prof. S. R. Wategaonkar[5]
[1, 2, 3, 4, 5] Dept of Electronics and Telecommunication
[1, 2, 3, 4, 5] Bharati Vidyapeeth College of Engineering,
Belpada, Navi Mumbai

Abstract- *Future electric lights will be comprised of white LEDS (light-emitting diode). An indoor visible data transmission system utilizing white led lights is proposed. In the system, these devices are used not only for illuminating rooms but also for an optical wireless communication system. However it remains necessary to investigate the properties of white led's when they are used as optical transmitters. Based on numerical analyses and computer simulations it can be used for indoor optical transmission. Secured transmission is possible using steganography and password prompt for exchange.*

I. INTRODUCTION

Data transmission using optical wireless has been identified as a technology that can be utilized for communications in critical environments, such as aircrafts or hospitals, where radio frequency (RF)based transmissions are usually prohibited or refrained to avoid interference with critical systems. Moreover, a huge amount of unregulated bandwidth is available at infra-red and visible light frequencies. Researchers around the world are fine-tuning technologies that use standard lighting equipment to cheaply transmit high-speed data streams wirelessly, even while the equipment appears to be producing nothing more than normal illumination.

Generally, the technologies rapidly and subtly fluctuate the intensity of light-emitting diodes, or LEDs, in a way that is imperceptible to the human eye. The idea of using light to send information, a field now known as visible light communications, has been around for well over a century. In fact, Alexander Graham Bell sent a wireless phone message in 1880 using his invention known as the Photo phone. But academic and commercial interest in visible light communication has accelerated in recent years.

The increasing popularity of LED lights, which can be more finely controlled than traditional bulbs, makes light-based technology more practical and economical. Also, the exponentially growing demand of wireless communication devices has taxed radio spectrum, resulting in a need to find alternatives. In addition, commercially available light emitting diodes (LEDs) and photodiodes(PDs) can be utilized for data transmission and reception. In addition, transmissions can be stopped simply by blocking the light, and thus can be stopped by walls, so there is less risk of data leaking out of a house or office. And researchers say they believe that signals can piggyback on lights that are already in use – street lamps, car headlights or room lighting. Use of MATLAB has made it possible to provide the feature of steganography.

II. LITERATURE REVIEW

Visible light communication is a fascinating and emerging communication technology employing visible light with spectrum between 400 THz and 790 THz for both illumination and data communication. Signal is transmitted with LED by their intensity modulation. Several modulation techniques could be adopted e.g. on/off keying (OOK) which is the main output for the system. The VLC uses LEDs to send data by flashing light at undetectable speed to human eyes. Its applications can be found in office broadband communications, secured communications, hybrid energy and communications, and smart home. Every kind of light source can theoretically be used as transmitting device for VLC or LI-FI. However, some are better suited than others. For instance, incandescent lights quickly break down when switched on and off frequently. These are thus not recommended as VLC transmitters. More promising alternatives are LEDs. VLC transmitters are usually also used for providing illumination of the rooms in which they are used. The simplest form of LEDs are those which consist of a bluish to ultraviolet LED surrounded by phosphorus which is then stimulated by the actual LED and emits white light. This leads to data rates up to 40 m bit/s. RGB LEDs do not rely on phosphorus any more to generate white light. They come with three distinct LEDs (a red, a blue and a green one) which, when lighting up at the same time, emit light that humans perceive as white, because there is no delay by stimulating phosphorus. Data rates of up to 100 MB its/s can be achieved using RGB LEDs. In recent year the development of resonant cavity LEDs (RCLEDs) has advanced considerably. These are similar to RGB LEDs in that they are comprised of three distinct LEDs, but in addition they are fitted with Bragg mirrors which enhance the spectral clarity to such a degree that emitted light can be modulated at very high frequencies. In early 2010, Siemens has shown that data transmission at a rate of 500MBBit/s is possible with this approach. The most common choice of receivers is photodiodes which turn light into electrical pulses. The signal retrieved in this way can be demodulated into actual data.

III. RESULT OF STUDY

a) Capacity: The radio waves used by Wi-Fi to transmit data are limited as well as expensive. With the development of 3G and 4G technologies, the amount of available spectrum is running out.

b) Efficiency: There are 1.4 million cellular radio masts worldwide. These masts consume massive amounts of energy, most of which is used for cooling the station rather than transmission of radio waves. In fact, the efficiency of such stations is only 5%.

c) Availability: Radio waves cannot be used in all environments, particularly in airplanes, chemical and power plants and in hospitals.

d) Security: Radio waves can penetrate through walls.

BLOCK DIAGRAM:

This framework will be valuable when there are just two hubs, who needs to exchange computerized image safely through the medium of visible light. In this framework hub one will give private report , which he need to send to hub two and a high determination mystery image. The framework will take this as info and will perform diverse preparing on them. On the other hand, the private record is encoded and after that it will be compacted to limit its size. At the same time, Binary transformation and division of mystery image will take place. At that point, the framework install compacted record into one of the arbitrary piece of image. Presently, the framework is having a computerized image, which is prepared for the steganography stage. After the fruitful steganography a mystery security key is given to hub one, so another hub can recognize it. Finally, for the security reason framework randomize the information parcels to be send in the system and exchange them one by one. At receiver side, hub two give his mystery get to key and after that reverse processing will be carried on the mystery image. After the effective turn around preparing hub two will get his secret archive.

a) Image: In this task information transmission is done by means of visible light. The information is to be transmitted is an image.

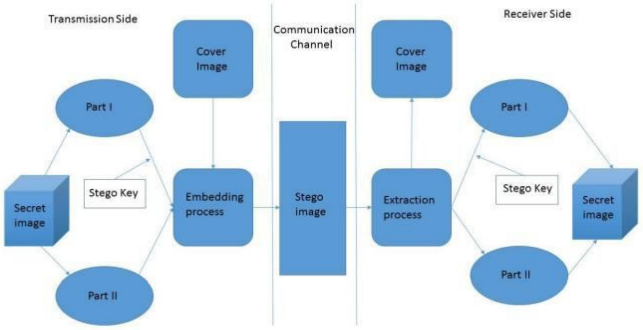
b) Image handling: The image to be transmitted should be prepared. Image preparing here is done in PC programming 'MATLAB'. In MATLAB the quantity ofpixels of that specific image is ascertained in the primary stage. The second stage predominantly comprises of changing over every pixel into its identical twofold code. This code is then exchanged over to the microcontroller by means of serial port.

c) LED flipping: The changed over double codes are transmitted over to recipient taking obvious light as its medium with the assistance of LEDs. These LEDs are flipped as per the paired codes that the microcontroller gets through the serial port.

d) Photo identification by phototransistor: On the receiving side we have a phototransistor which distinguishes the light occurrence on it. The simple voltage produced at the yield of this identifier is then given to the microcontroller/Arm/Arduino.

e) Microcontroller/Arm/Arduino: At the contribution of the microcontroller the simple voltage is changed over into double arrangement. This is finished with the assistance of the edge level which is predefined.

f) Analog to Digital Convertor (ADC) and Digital to Analog Convertor (DAC).



ALGORITHM:

Image preparing: The twofold code got through the serial port is then handled in MATLAB where the exchanged image is reverse processed utilizing the parallel codes received from the microcontroller.

Compression Stage: In the event that the report is expansive in its size, at that point it will require greater investment to install in the image and recovery of information from image will likewise require additional time. In this way, if the framework pack this encoded information the general framework will work quicker. Pressure will likewise in a roundabout way secure the archive's data. Image pressure might be lossy or lossless. Lossless pressure is favored for chronicled purposes and regularly for therapeutic imaging, specialized illustrations, cut craftsmanship, or funnies. Lossy pressure strategies, particularly when utilized at low piece rates and are particularly reasonable for common images. Lossless image pressure is best reasonable for our proposed framework.

Binary Conversion Stage: The secret image provided by the user will be converted to binary form with the application of MATLAB, so that proposed system will be able to perform different processing on the digital form of image.

Dividation Stage: After the twofold change the mystery image will be isolated into number of a balance of for the security reason. Simply after this stage the mystery image is prepared to movement in the system.

Something else, any bundle sniffer can get the image in the system. Along these lines, when the image is in the isolated shape gatecrasher won't have the capacity to get every one of the parts. Furthermore, without every one of the parts everything else will be pointless for him.

Reconciliation Stage: This procedure happens at the goal side when a collector hub needs to recover his private record from the mystery image. Every one of the parts assemble at the goal side will be in irregular request. The goal framework will mastermind them in appropriate request and after that coordinate every one of the parts to reproduce finish mystery image.

Implanting Stage: Implanting of packed report to specific parts of image will happens at this stage. In the wake of implanting a total advanced image will be given to the steganography stage.

Steganography Stage: In this stage, steganography will be perform on singular piece of mystery image utilizing LSB algorithm. We can likewise utilize other steganography calculations like, KNCG (kekre's Median Codebook Generation) calculation, BlindHide, HideSeek, Filter First, Battle Steg and so forth.

Transmission Stage: When every one of the parts of mystery image will be prepared to-s-end in the system from Source side then they won't be end in their genuine request. The framework initially organized them in irregular request and after that after that parcel by-bundle every one of the-parts will be discharged to the goal side through the noticeable light transmission.

VI. CONCLUSION

VLC appears to be an important potential component in expanding useable bandwidth, protecting sensitive electrical equipment and data, creating more biologically friendly communications technology. The new transmission technology is suitable for hospitals, for example, because radio transmissions are not allowed there. Despite this fact, high data rates must be transmitted without losses and unzipped, according to the experts. If part of the communication occurs via the light in the surgical room, this would make it possible to control wireless surgical robots or transmit x-ray images. In airplanes, each passenger could view his own entertainment program on display, saving aircraft manufacturers miles of cables. Another possible venue for the application of this technology is production facilities like petrochemical plants, where radio transmissions very often interfere with the process. In addition, transmissions can be atopped simply by blocking the light, and thus can be stopped by walls, so there is less risk of data leaking out of house or office.

REFERENCES

[1] 2007 Nature Photonics-Dominic O’Brien, Gareth Parry & Paul Stavrinou.

[2] Lopez-Hernandez-Fj, Poves-E, Perez-Jimenez-R and Rabadan-J: ‘Lowcost diffuse wireless optical communication system based on white LED’. Proc. 2006 IEEE Tenth International Symposium on Consumer Electronics. St. Petersburg, Russia. 28 June 1 July 2006. pp.

[3] P. Amirshahi and M. Kavehrad, (2006). Broadband Access over Medium & Low Voltage Power-lines and use of White LEDs for Indoor Communications. In IEEE CCNC 2006 proceedings.

[4] Amirshahi P. and Kavehrad M.2006. Broadband access over medium and low voltage power-lines and use of white light emitting diodes for indoor communications. In IEEE Consumer Communications & Networking Conference, Las Vegas, Nevada. Citeseer.

[5] J. Carruthers and J. Kahn, “Multiple-Subcarrier Modulation for Nondirected Wireless Infrared Communication,” IEEE Journal on Selected Areas in Communication, vol. 14, pp. 538–546, April 1996.