Secure Visible Light Communication by Caser Cipher and Spiral Wheel Algorithm

Komal Kumari Agrawal 1, Vishal Shrivastava 2
1P.G. Student, 2Associate Professor
Department of Computer Science Engineering
Arya College of Engineering & I.T, Jaipur (Raj.), India

Abstract— *Due to growing congestion of the RF spectrum and its adverse health effects on humans as well as plants and animals, alternate way of communication are constantly sought. Light-Fidelity (Li-Fi) is a Visual Light Communication and has remained a prime research topic over past years. However security aspects related to data transmission are often neglected. The paper proposes a data security algorithm based on Caesar Cipher and novel Spiral wheel algorithm. The new Spiral Wheel encryption technique based on substitution of ASCII value of characters in reliable data transmission across Li-Fi system is successfully implemented on Li-Fi hardware, which is constructed on ArduinoUNO microcontroller .The results convey the reliability and efficiency of developed algorithm.*

Index Terms— *light fidelity , security, key, encryption, decryption.*

I. Introduction

THE term “Li-Fi” was coined by Professor Herald Hass in 2011[1].Li-Fi is a form of visible light communication which employs Light Emitting Diodes(LED) for data transmission[1].Li-Fi can solve RF congestion problem and is a promising technology for future, as it utilizes the infrared and visible light spectrum, which is approximately 2600 times larger than radio spectrum bandwidth. For past ten years the Compound Annual Growth Rate(CAGR) is sixty percent[2].If the present CAGR is sustained ,we will face short fall compared to todays allocated RF bandwidth[2].The Light Fidelity (Li-Fi) is a vitality productive innovation designed for indoor applications yet it might be converged with Wi-Fi. Researchers have effectively demonstrated the transmission speed of 224 gigabits per second[3]. Using light, we achieve not only illumination but alsodata transmission with the same energy can be achieved,Thus Li-Fi can be called as green energy because it does not inflicts health problems on humans and animals as well as protects the data without extra cost. As shown in Table 1,Li-Fi provides many advantages over Wi-Fi such as increase in quality, speed, maximum protection, etc. Although Li-Fi provides the strong security for accessing data from the outside of data center, there are some cyber security issues within the data center [4].Thus cybersecurity and privacy issues on Li-Fi systems should be considered.

The aim of our project is to develop a reliable data security algorithm for Li-Fi system by novel spiral wheel algorithm.The rest of the paper is organized as follows; Section II demonstrates the related work. Implementation details are summarized in Section III.Results are mentioned in Section IV.Section V and VI mentions conclusion and future scope respectively.

II. Related Work

Tasfia and Hira[5] proposed a modification in Caesar Cipher wheel algorithm. It is also used in Li-Fi for secure data exchange. In this algorithm, an array is used whose length is defined according to our requirement. A loop is created with iteration number to repeat the operation. The ASCII values of the plain text are taken and it uses any mathematical equation in which the ASCII value of the plain text letter and the array value are used according to the iteration number position. Thus, the cipher text is evaluated from the mathematical equation. Mishra [6]enhanced the security of Caesar Cipher algorithm i.e. transposition cipher. Goyal andKinger[7].In this paper, an encryption algorithm based on Caesar cipher has been enhanced which first checks alphabet index and if the alphabet index is even then increase the key value by one else decrease the key value by one when it is odd. Singh, and Garg[8] used American Standard Code for Information Interchange i.e. ASCIIvalue of the plain text and uses a random key of four characters to encrypt the data. The key used to encrypt the plain text is generated randomly by the system. To encrypt the plain text various transformations are applied using the randomly generated key.Lavanya1[9] proposes a new algorithm called RAND_ASC which construct the cipher depending on the ASCII values. It uses floating point numbers in a symmetric key to encrypt the data. The prime concept is to convert the plain text into a format of floating point numbers. Random numbers are generated which are coded with the cipher text, to make cryptanalysis arduous. The use of floating point numbers rejects the mapping of frequency of characters and hence brute force attack is impossible and the encrypted text is unreadable.Charru and etal [10] used using exclusive OR operation in symmetric key algorithm. Jain And etal[11] contributed in the area of classical cryptography by providing a modified and expanded version for Caesar cipher by complex key generation technique which generates two keys from a single key to provide enhanced security.The proposed algorithm uses a randomized approach for substitution which is then combined with double columnar transposition technique to increase the strength. On performing crypto analysis on the modified algorithm, it is found that it is impossible to break it by frequency analysis. Security provided by this algorithm can be enhanced further by using it with one or more different encryption algorithms or by using asymmetric key approach instead of symmetric key. Satyajeet and etal[12]presents a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. This system randomly generates a key for user having length equal to the length of the message or plaintext. In this algorithm the secret key is converted to another string and that string is used as a key to encrypt or decrypt the data and hence, it gives good result in less execution time. Verma and etal[13] presented a new approach named Coherent Caesar Cipher (CCC). Coherent Caesar Cipher (CCC) is found to be more consistent and reliable as compared to other existing Caesar cipher algorithms. Abraham and etal [14]presented Improved Caesar Cipher (ICC) which strengthens cipher text generated by Caesar cipher by removing spaces in plaintext and changing positions of character.The major strength of ICC is that it requires less computer resources when compared to other encryption algorithms. Thus, ICC would be ideal for devices with limited computing resources such as mobile devices and Personal Digital Assistance (PDA).Srikantaswamy and Phaneendra[15]proposed a hybrid version of classical and modern cipher properties which provides appreciable Security with high throughput and occupies minimum memory space. This method suggests the idea of converting a given plaintext characters into two ciphertext characters. It involves 100-bit key value. The modern DES algorithm involves 56-bit key value. Thus, this method exhibits more resistance against cryptanalytic attacks.Gupta and Vinod Kumar Sharma[16] proposed encryption technique in which the original data is encrypted many times with different encryption algorithms at each phase. The Multi-Phase Data Encryption is an ambivalent technique used for data and information security which plays an important role in modern Cryptography. It describes the enhanced complexity of data encryption due to multiple operations of single phase encryption techniques in cryptography. The advantage of multiple encryptions is that it provides better security because even if some component ciphers are broken or some of the secret keys are recognized, the confidentiality of original data can still be maintained by the multiple encryptions.Priyanka V and etal[17]focuses on the substitution of characters, numbers and special symbols with color blocks and it is based on PlayColor Cipher.Abdus[18] used improved version of ciphering with the combination of double phase encryption. To ripen this method of encryption, a simple technique of vertically selecting the text for ciphering is used. Other techniques related to encryption and steganography can be found in [20,21,22,23,24].

One of the drawbacks of substitution ciphers is that if the message is long enough, it may be vulnerable to Frequency Analysis i.e. The frequencies of letters are not masked; thus, it retains the frequency patterns of letters that are found in the original message.The major drawback of transposition cipher is to decipher it i.e. Transposition cipher can be broken by statistical methods. If the messages are short, some characters will not appear thus it is possible to say which words do not exist in the text.

III. METHOLDOLOGY

Cryptography is an important protocol for network security. It protects information from undesirable disclosure or malicious users by converting it into an imperceptible form (Cipher) while storing and transmitting it. It is an important building block of information systems. It describes the aspects of information security that are related to the study of mathematical techniques such as data integrity, confidentiality and authentication of data.In the proposed methodology an implementation of a new encryption technique based on substitution of ASCII value of characters in reliable data transmission across Li-Fi system, as both privacy and prevention from unwanted access along with high data rate can be achievable from Li-Fi if light contains encrypted message. The proposed encryption algorithm primarily follows Caesar Cipher and it is further modified by applying unique spiral wheel algorithm. Encryption of data, transmission, reception and conversion to original message are implemented successfully using laser, phototransistor, microcontroller (Arduino UNO) and associated devices.

3.1 Spiral Wheel Algorithm

Spiral wheel algorithm is an enhanced version of Caesar Cipher algorithm. In spiral wheel algorithm, the data during transmission is encrypted by rotating the bits of data in spiral form. While in decryption, there are two cases depending on the number of characters. In the first case, if number of characters in the string are even then from the encrypted string characters are selected (N/2)-1 times next to adjacent character and the last character is selected by taking the adjacent character from left to right and then again the characters are selected (N/2)-1 times next to adjacent character from right to left. In the second case, if number of characters are odd then characters are selected next to adjacent character till Nth character and then from right to left it will first select the adjacent character and again the next to adjacent character.

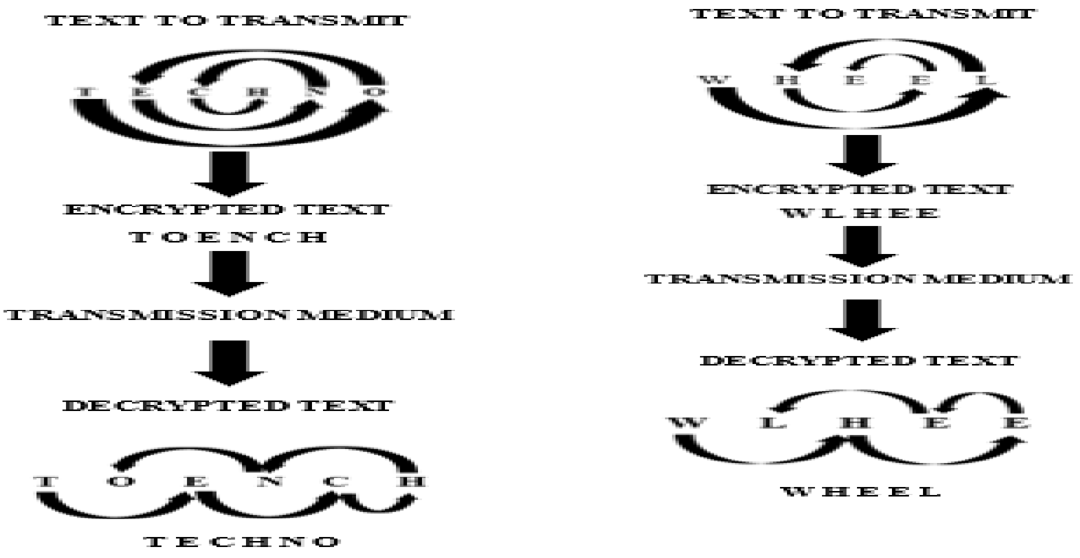


Fig 1. Spiral wheel algorithm

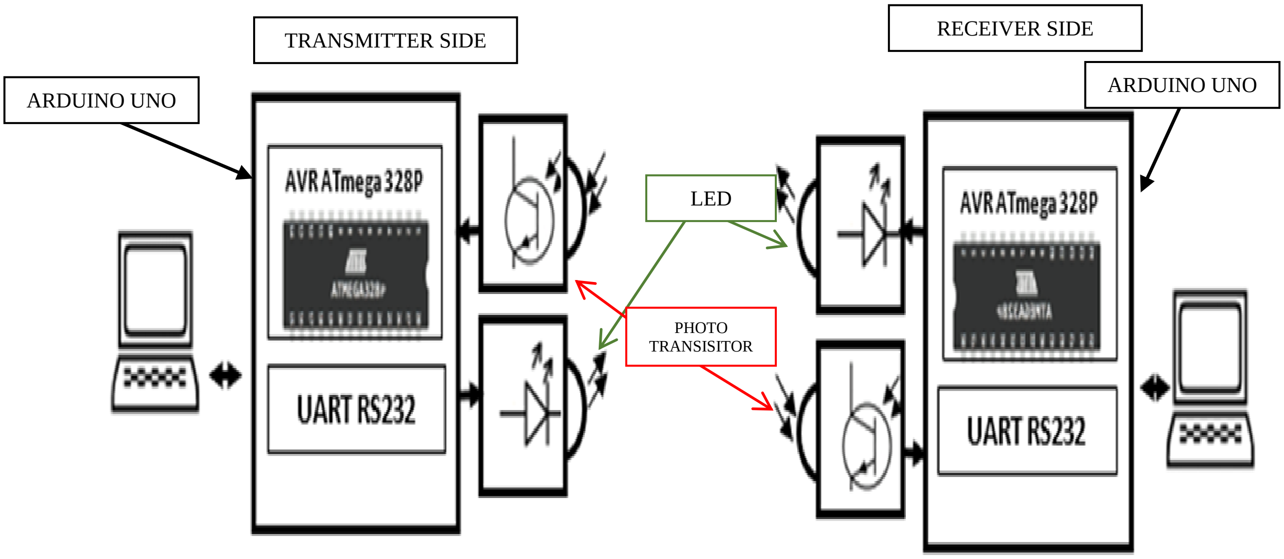


Fig 2. Block diagram of Li-Fi system

.

The encryption and decryption process involved is expressed mathematically by following equations.Ustr, EnUstr, DrUstr represents user string, encrypted string and decrypted string respectively, len is length of string and c represents center of string. Equation(1) returns alternate characters in user string. Equation (2) denotes calculation of centroid for even and odd length string.Equation (3) returns modified string after spiral wheel rotation.The encrypted string is shown in equation (4).Equation (5)and (6) shows the spiral wheel decryption process.Equation (7) represents the final decrypted string which is equal to user string.

$$\mathrm{Ustr[i]} = \sum_{i=0}^{len} \mathrm{Ustr[i+2]}$$

(1)

$$\mathrm{C}=\begin{cases} \frac{\mathrm{len}+1}{2} & \mathrm{len}=2\mathrm{n}+1 \\ (\mathrm{len}/2)+1 & \mathrm{len}=2\mathrm{n} \end{cases}$$

(2)

Encryption

$$\mathrm{Ustr[i]}=\sum_{0}^{len} Ustr[len-i]$$

(3)

EnUstr[i]=

$$\sum_{\mathrm{i=0}}^{\mathrm{i<len}} [\mathrm{Ustr}_{\mathrm{len}}\ , \mathrm{Ustr}_{\mathrm{len-len+1,}} \mathrm{Ustr}_{\mathrm{len-1,}} \mathrm{Ustr}_{\mathrm{len-len+2,}} \mathrm{Ustr}_{\mathrm{len}\frac{1}{2},}]$$

(4)

Decryption

$$\mathrm{DrUstr[i]}_1 = \sum_{\mathrm{i=len}}^{\mathrm{c}} \mathrm{EnUstr[i+2]} \qquad (5)$$

$$\mathrm{DrUstr[i]}_2 = \sum_{\mathrm{i=c}}^{0} \begin{cases} EnUstr[i-1], i = len \\ EnUstr[i-2], otherwise \end{cases} \qquad (6)$$

$$\mathrm{DrUstr=DrUstr}_1 + \mathrm{DrUstr}_2\mathrm{= Ustr} \qquad (7)$$

3.2 Implementation of LI-FI

The implementation of LI-FI is realized with help of Arduino microcontroller (Fig 7).The block diagram is shown in fig 2. The transmitter section consists of LED which acts as a communication source. Li-Fi is implemented using the Light of White LED bulbs at transmitter. These kinds of devices generally used for illumination by applying constant current on it. when the LED is ON, then it transmits digital string 1 and when it is OFF then it transmits the string 0. And the rate of encoded data depends on the flicker of LED. The input can be any type of data. When a constant current is applied to a LED, certain amount of energy (photons) gets released, that we perceive as visible light. If the input current to the LED is varied slightly, the intensity of the light output also varies. This flickering of LED is regulated by voltage regulator and level shifter. Since LEDs are nothing but the semiconductor devices, the current and the optical output (the light produced by LEDs) is modulated at very high speeds, which is then detected by a photo detector. Here, modulation technique is developed for intensity modulation and direct detection(IM/DD) of optical wireless communication. For optical wireless links, the intensity modulation is used in which the desired signal is modulated onto the instantaneous power. Also, a direct detection in which a photo detector produces a current to receive the instantaneous power, it detects only the intensity of optical signal. The photo detector at receiver side sense light and converts into the respected pulses which is then amplified and processed to achieve the original data stream. The distance achieved by system depends only on the potential of the light source.

3.3 Hardware and software flow control at Transmitter

Algorithm for hardware flow control at transmitter:

Step1: Connect comport.
Step2: Set parity bit and start bit as 1.
Step 3: Set stop bit =0.
Step4: Set hardware flow control=0.
Step5: Start USB to serial communication.
Step6: User data is converted to binary by Arduino.
Step7: LED driver Arduino pin
Step8: LED Pulse Data send to photo transistor of other Arduino.

Software flow algorithm for Transmitter
Step1: Enter string for encryption.
Step2: Start the Caesar cipher Engine to encrypt the data.
Step3: Assign the private key.
Step4: Apply the spiral wheel.
Step5: Check string is Even or Odd.
Step6: Calculate the String length.
Step7: Apply spiral user for encryption of Caesar cipher string.
Step8: Apply spiral private key.
Step9: Convert the data into binary.
Step10: Converted data and send to the RS-232-bit stream.
Step11: Go to RS-232- setting.
Step12: set parity and hardware flow control.
Step13: set the start, stop, bits/sec+ and baud settings.
Step14: Send the data to Li-Fi driver circuit.

3.4 Hardware and software flow control at receiver

Algorithm for hardware flow control at receiver:
Step1. Data received at phototransistor.
Step2. Data is converted from serial to binary by Arduino.
Step3. Start USB to serial communication.
Step4. Set harder ware flow control.
Step5. Set start bit equal to one.
Step6. Set stop bit equal to zero.
Step7. Go to the setting and set parity bit equal to one.
Step8. User encrypted data.
Step9. To application software.

Software flow algorithm for Receiver
Step1: Receive the data at Li-Fi driver circuit.
Step2: Set the start, stop, bits/sec and baud settings.
Step3: Go to RS-232- setting.
Step4: Received asRS-232-bit stream.
Step5: Convert binary data into string.
Step6: Apply spiral private key.
Step7: Apply spiral user for encryption of Caesar cipher string.
Step8: Calculate the String length.
Step9: Check string is Even or Odd.
Step10: Apply the spiral wheel.
Step11: Assign the private key.
Step12: Start the Caesar cipher Engine to decrypt the data.

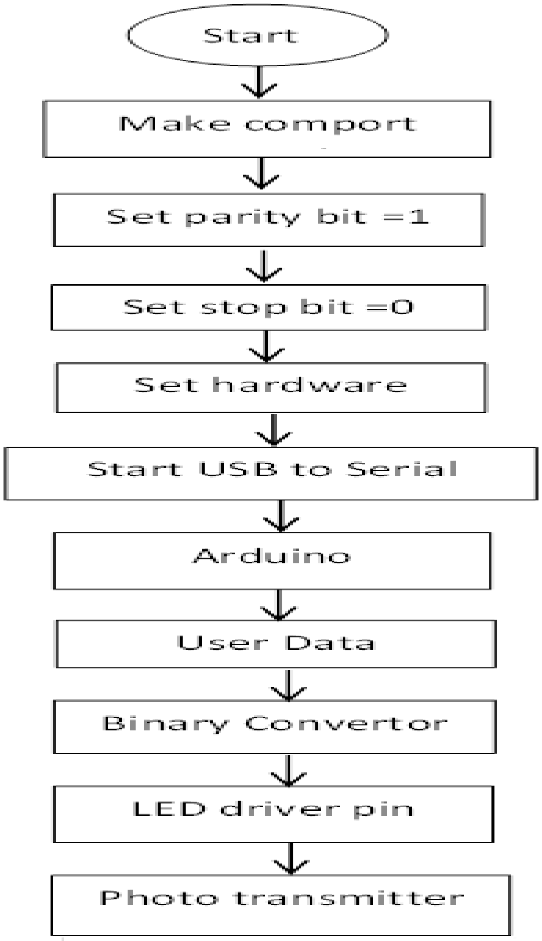


Fig 3.Hardware flow control at transmitter

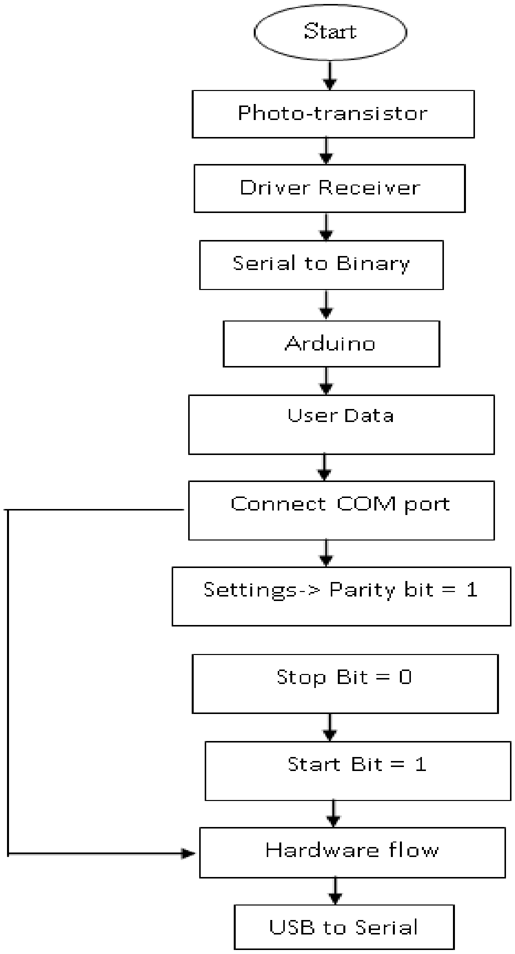


Fig 4.Software flow control at receiver

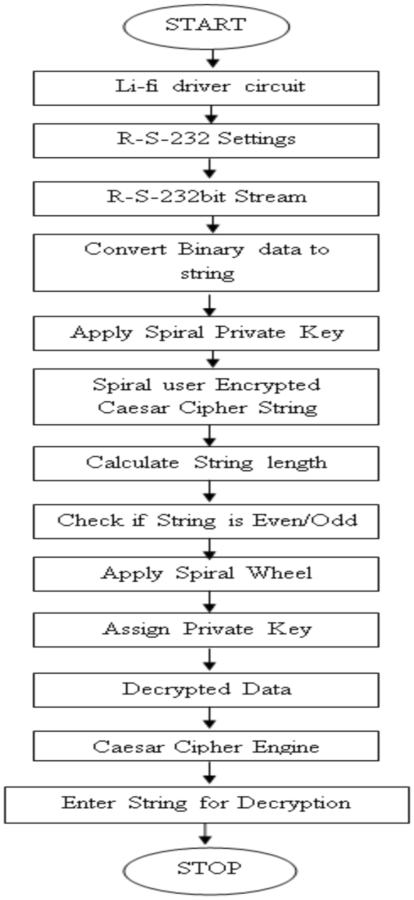


Fig 5.Hardware flow control at receiver

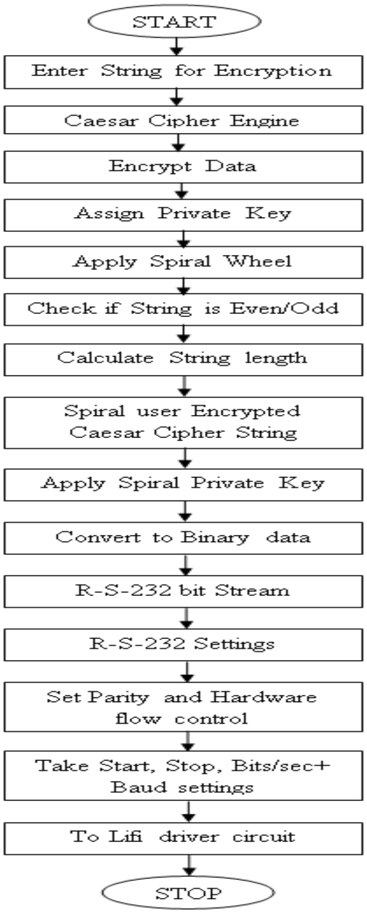


Fig 6.Software flow control at receiver

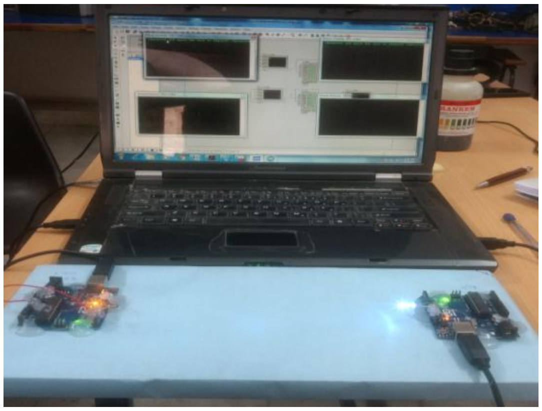


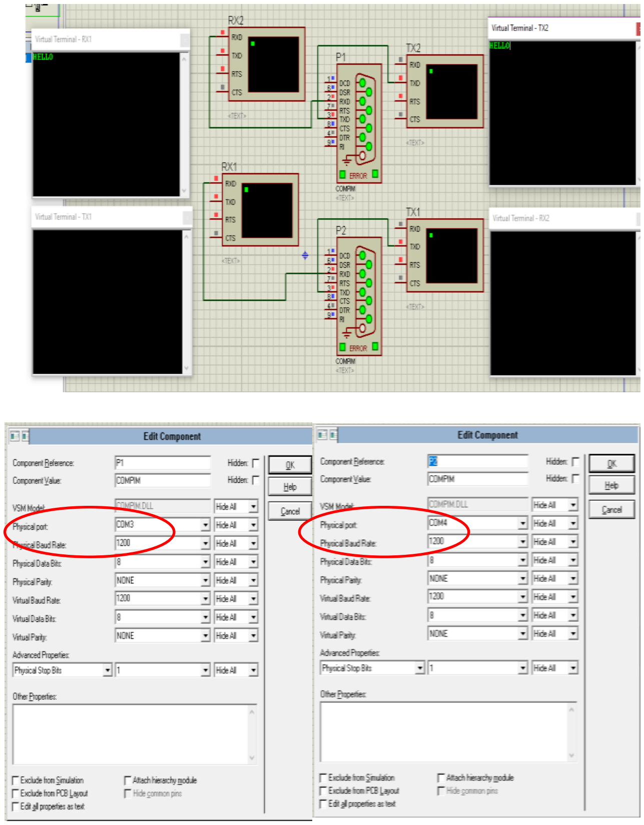
Fig 7.Implementation of Li-Fi system.

TABLE I
Comparison between Wi-Fi and Li-Fi

Features	Wireless Fidelity	Light Fidelity
Data Transmission	Radio waves	Bits
Frequency	Radio spectrum range	10000 times of Wi-Fi
Frequency band	2.4GHz, 4.9GHz and 5GHz	100 times of Tera Hz
Data transfer Speed	WLAN-11n offers 150Mbps, Wi-Giga/Giga-IR offers about 1-2 Gbps	1-3.5 Gbps
Coverage Area	20 - 100 meters vary based on type of transmission power and antenna	10 meters
Operation	Data transmission by radio waves with Wi-Fi router	Data transmission by light of LED bulbs
Interference	Interfere with neighbour AP Routers	No interference issues with RF waves

IV. Results

Successful implementation spiral wheel security algorithm is achieved on Li-fi system (Fig 7).Fig8 shows simulation in PROTEUS ISIS. As shown in fig transmitter and receiver COMPIMs (P1 and P2 respectively) are connected to virtual terminals. The baud rate is set at 1200 and physical ports are chosen appropriately (COM1 and COM2). The simulation design is able to transmit and receive the data from both sides i.e. from Tx1-> Rx2 and Tx2->Rx1.To make physical connections Arduino boards for transmitting and receiving side are connected to physical ports COM1 and COM2 respectivelyand visual basic code is compiled. Fig 9 shows the implement steps. Firstly transmitter and receiver output window is opened and connect button is clicked to make connection between transmitter and receiver as shown in figure 9(a). Once the connection is established “Input key” and message is entered followed by clicking of Encryption button, which results in encrypted text or chipper text. The text reaches the receiver side where it is decrypted to reveal the original message or plain text.



Edit Component

Component Reference: P1 Hidden: □
Component Value: COMPIM Hidden: □
VSM Model: COMPIM.DLL Hide All
Physical port: COM3 Hide All
Physical Baud Rate: 1200 Hide All
Physical Data Bits: 8 Hide All
Physical Parity: NONE Hide All
Virtual Baud Rate: 1200 Hide All
Virtual Data Bits: 8 Hide All
Virtual Parity: NONE Hide All
Advanced Properties: Physical Stop Bits 1 Hide All
Other Properties:
□ Exclude from Simulation □ Attach hierarchy module
□ Exclude from PCB Layout □ Hide common pins
□ Edit all properties as text

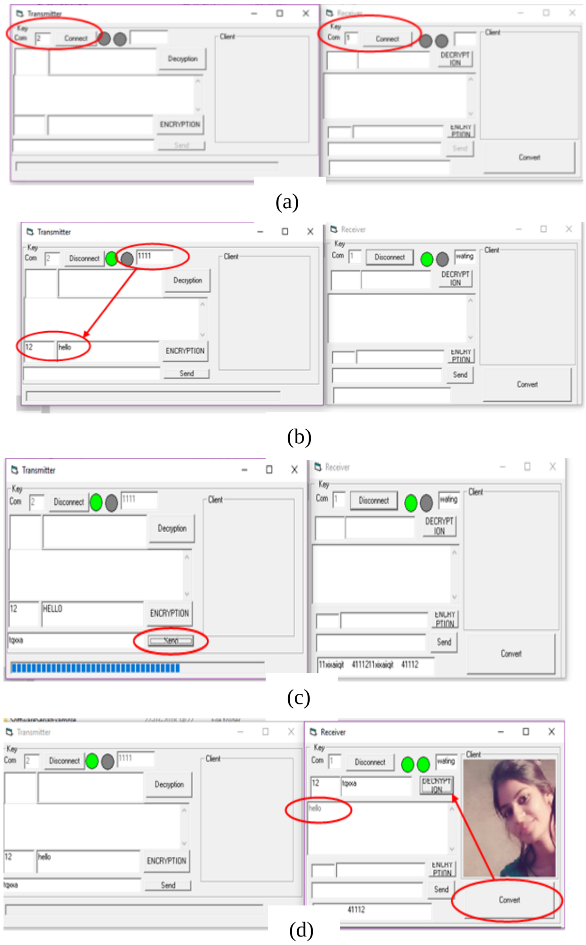
Edit Component

Component Reference: P2 Hidden: □
Component Value: COMPIM Hidden: □
VSM Model: COMPIM.DLL Hide All
Physical port: COM4 Hide All
Physical Baud Rate: 1200 Hide All
Physical Data Bits: 8 Hide All
Physical Parity: NONE Hide All
Virtual Baud Rate: 1200 Hide All
Virtual Data Bits: 8 Hide All
Virtual Parity: NONE Hide All
Advanced Properties: Physical Stop Bits 1 Hide All
Other Properties:
□ Exclude from Simulation □ Attach hierarchy module
□ Exclude from PCB Layout □ Hide common pins
□ Edit all properties as text

Fig 8.Simulation in PROTEUS ISIS.

V. Conclusion

In the research work, it is noticed that if the light contains encrypted message then both privacy and prevention from unwanted access along with high data rate can be achieved from Li-Fi. In this project a new encryption technique based on substitution of ASCII value of characters in reliable data transmission across Li-Fi system is successfully implemented. The proposed encryption algorithm primarily follows Caesar Cipher and it is further modified by applying our unique spiral wheel algorithm. Encryption of data, transmission, reception and conversion to original message are implemented successfully using phototransistor, Arduino, microcontroller and associated devices. It is derived from the experimental results that the proposed algorithm enhances the security across a Li-fi system by using advanced version of Caesar Cipheralgorithm. The proposed approach makes the data transmission immune to security breaches and is also convenient and scalable which makes system robust.



(a)

Transmitter: Com 2, Key 1111, 12 hello

Receiver: Com 1, wating

(b)

Transmitter: Com 2, Key 1111, 12 HELLO, tqoxa

Receiver: Com 1, wating, 11xixaiqt 4111211xixaiqt 41112

(c)

Transmitter: Com 2, Key 1111, 12 hello, tqoxa

Receiver: Com 1, wating, 12 tqoxa, hello, 41112

(d)

Fig 9.Encryption-Decryption in visual basic

VI. FUTURE SCOPE

Most of the research in the field of Li-fi primarily focuses on improving the data transmission speeds while little attention is paid for improving robustness and security aspects of the system. For instance, the data transmission speed and reliability across a li-fi system is compromised under low lighting conditions thus efforts should be made to resolve the above limitations. For example, hybridization of li-fi with infrared should be considered in future research. The developed security algorithm is efficient however; future research can be conducted for transmitting data in compressed form to enhance the speed.

REFERENCES

[1]ThiloFath and Harald Haas, "Performance Comparison of MIMO Techniques for Optical Wireless Communications in Indoor Environments", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 61, NO. 2, FEBRUARY 2013.

[2] H.Haas,LiFi is a paradigm-shifting 5G technology, https://doi.org/10.1016/j.revip.2017.10.001.

[3] V.Thayananthan,O. Abdulkader, K. Jambi andK. A. Bamahdi,Analysis of Cybersecurity based on Li-Fi in green data storage environments,978-1-5090-6644-5/17 2017 IEEE.

[4]Yu Gong, MatteoFiorani, and SlavisaAleksic, "Optical Interconnects at the Top of the Rack for Energy-Efficient Data Centers", IEEE Communications Magazine, pp. 140-148, August 2015

[5]TasfiaTasbin, AvijitHira, "Optical Wireless Data Transmission with Enhanced Substitution Caesar Cipher Wheel Encryption", International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017.

[6] A. Mishra, "Enhancing Security of Caser Cipher using Different Methods," in International Journal of Research in Engineering and Technology.

[7] K. Goyal, S. Kinger "Modified Caesar Cipher for Better Security Enhancement" in International Journal of Computer Applications, July 2013.

[8] U. Singh, U. Garg "An ASCII value-based text data encryption System" in International Journal of Scientific and Research Publications, November 2013.

[9] M. Lavanya1, "An Encryption Algorithm Functioning on ASCII Values and Random Number Generation"in Indian Journal of Science and Technology, Vol 8(35), December 2015.

[10] Charru, P. Singh, S. Rani "Efficient Text Data Encryption System to Optimize Execution Time and Data Security" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014.

[11] Atish Jain, RonakDedhia, AbhijitPatil "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication" in International Journal of Computer Applications, November2015.

[12] Satyajeet R. Shinge, Rahul Patil "An Encryption Algorithm Based on ASCII Value of Data" in International Journal ofComputer Science and Information Technologies.

[13]PriyaVerma, Gurjot Singh Gaba "Coherent Caesar Cipher for Resource Constrained Devices" in International Journal of Security and Its Applications, 2016.

[14] Ochoche Abraham, Ganiyu O. Shefiu "An improved Caesar cipher (ICC) algorithm" in International Journal of Engineering Science & Advanced Technology.

[15] S G Srikantaswamy and Dr. H D Phaneendra"ImprovedCaesar cipher with random number generation technique and multi stage encryption" in International Journal on Cryptography and Information Security (IJCIS), December 2012.

[16] Himanshu Gupta and Vinod Kumar Sharma "Multiphase Encryption: A NewConcept in Modern Cryptography" in Multiphase Encryption: A New Concept in Modern Cryptography International Journal of Computer Theory and Engineering, August 2013.

[17]Priyanka V. Deshmukh, Netra R. Bujad,Prof. SachinSonawane "Secure Encryption and Decryption using Play Color Cipher" in National Conference on Technological Advancement and Automatization in Engineering, January 2016.

[18] AsiyaAbdus Salam, Ruba Mahmoud Al Salah "Vertically Scrambled Caesar Cipher Method" in International Journal of Computer Applications, May 2015.

[19]AbikoyeOluwakemi, AdewoleKayode, OladipupoAyotunde "Efficient Data Hiding System using Cryptography and Steganography" in International Journal of Applied Information Systems (IJAIS), ISSN: 2249-0868, December 2012.

[20]WalidAbdallah and NoureddineBoudriga "Enabling 5G Wireless Access Using Li-Fi Technology: An OFDM Based Approach" in Communication Networks and Security Research Lab, 2016.

[21]Shiv Shakti "Encryption Using Different Techniques" in International Journal in Multidisciplinary and Academic Research, February-2013(ISSN 2278 – 5973).

[22]Naoki Nishikawa, Keisuke Iwai and TakakazuKurokawa "High-Performance Symmetric Block Ciphers on CUDA" in Second International Conference on Networking and Computing, 2011.

[23]ManishaYadav, Mauli Joshi, Akshita "Improved Secure Data Transfer Using Tiny Encryption Algorithm and Video Steganography" in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128, December 2013.

[24]Tang Songsheng, Ma Xianzhen "Research of typical block cipher algorithms" in International Conference on Computer, Mechatronics, Control and Electronic Engineering, 2010.

[25]P. Kuppusamy,S. Muthuraj, and "Survey and Challenges of Li-Fi with Comparison of Wi-Fi",978-1-4673-9338-6/162016 IEEE.