INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Data Transmission by Ceaser Cipher Wheel Encryption using Lifi

S. Jeya Anusuya
hodece@tjsec.in
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

S. Venket
venkatecetjs@gmail.com
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

V. Logesh Kumar
logima97@gmail.com
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

T. Manoj Gowtham
manojgowtham11031997@gmail.com
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

V. Goutham
gouthamnaidu153@gmail.com
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

R. Gowtham
rgowtham987@gmail.com
T. J. S. Engineering College, Puduvoyal, Tamil Nadu

ABSTRACT

The paper describes a microcontroller based secured optical wireless communication system using laser and phototransistor. These days the usage of Wi-Fi has reached to every nook and corner of the world. There are some downsides belong to the usage of Wi-Fi such as those concerning to the speed, limited bandwidth, security and range of its usage. In order to overcome these hitches, we can use the advanced version of Li-Fi which is efficient, high speed, and fully networked wireless communication. If light contains encrypted message then both privacy and prevention from unwanted access along with high data rate can be achievable from Li-Fi. A new encryption technique based on substitution of ASCII value of characters implemented and reliable data transmission carried out. The proposed encryption algorithm primarily follows Caesar Cipher WHEEL substitution, acts similarly with Caesar wheel device by rotating circularly and changes the ASCII value of original message according to predefined values and length of repetition. Encryption of data, transmission, reception, and conversion to original message are implemented successfully using laser, phototransistor, and microcontroller and associated devices. The microcontroller performs as overall controlling and processing unit.

Keywords: *LASER, OWC, VLC, Li-Fi, Cryptography, Modified Caesar Cipher Wheel.*

1. INTRODUCTION

This paper is based on the concept of Li-fi. It can transmit analog as well as digital signals using LASER light as a carrier in transmitter and phototransistor as a light detector in the receiver. Here, transmitted data are encrypted by a Caesar cypher algorithm in order to ensure secured optical communication. Further, the encrypted data is decrypted on the receiver portion.

Nowadays, Optical Wireless Communication (OWC) is already one of the most emerging technologies, spanning from physics, chemistry, and mathematics, electrical engineering up to architecture, psychology, and medicine [6]. In OWC infrared, visible, ultraviolet signals are used as a carrier to transfer information. OWC generally works in the bandwidth of visible region. Therefore, it can also be referred to as Visible Light Communication (VLC) [3]. Li-Fi is a subcategory of OWC, can also be a replacement of microwave communication in the context of network fidelity. Ensuring data transfer at high data rates, Li-fi has key benefits than conventional RF and microwave technology. It is wireless and uses visible light communication or infrared, which carries abundant information and solution to the RF bandwidth limitations. Spatial coherence and temporal coherence are two elementary phenomena of Lasers which permits the Laser light to travel uniformly on the narrow path and at the increased amount of speeds [3]. It has properties such as higher intensity, higher efficiency, better visibility and performance quality [4]. Typically, laser light has a much lower transmission loss per unit length (0.15-5db/km) and is not doughty to electromagnetic interference [3].

Here, on the transmitter, part modulation and optical conversion of data were implemented by the use of microcontroller and LASER. At the receiver, the phototransistor is used for optical to electrical signal conversion. Hence, another microcontroller was used to decode the different signal and the received data was given to the output. By this, a procedure has been developed for a wireless optical communication system employing Pulse Width Modulation (PWM) technique. This combines baseband or discrete

message signals with light frequency. Different width of laser pulse was used to represent different number and character. Alongside, the search for the best solution to offer the necessary protection against the data thieves' attacks along with timely manner is one of the most active subjects in the security related communities [5]. So, security is required to transmit confidential information such as banking transactions, credit information, and information about any secret mission over the network. Cryptography has come up with a solution which plays an exigent role in information security system against malicious attacks. It is the art of protecting the information by transforming it into an obscene format in which a message can be concealed from the unanticipated reader and only the intended recipient will be able to convert it into original text [7]. Cryptography is the scrambling of the content of information like text, image, audio and video to make it obscene or incomprehensible during transmission. In the language of cryptography, the original message which is in readable form is called the plaintext while the encrypted message which is in unreadable form is called the cipher text.

In this project, to make the text non-readable and secure, a new encryption algorithm primarily based on Caesar cipher wheel is implemented. It is a type of substitution type cipher, in this kind of cipher each letter (character, sign, symbol also) in the plaintext is replaced by another letter by changing its ASCII value in a cyclic manner. It is also a symmetric key type encryption algorithm because of secret key sharing among sender and receiver in order to meaningful communication. As conventional Caesar cipher has less strength and through brute force attack it can be easily broken using word matching and considering a couple of words of smaller length, the pattern of substitution can easily be realized by the third party.

The proposed and implemented algorithm presents a perspective on modification of ASCII value of the plain text in a regular manner which is on basis of Cipher wheel device. Existing Caesar Cipher was used only for alphabet but the proposed algorithm can encrypt characters, string, data as well as space within words.

2. ENCRYPTION USING CAESAR CIPHER

An encryption algorithm provides no access to unauthorized reader, authentication, confidentiality, integrity, and nonrepudiation. Depending on the key generation of an encryption algorithm, there are two types of encryption algorithm named as symmetric and asymmetric key encryption. In symmetric encryption, secret key, which can be a number, a word, or just a string of random letters, is applied to the data of a message to change the content in a particular way. As long as both sender and recipient should agree on that particular secret key, so they can communicate via cipher text and hide the original meaning of the messages from others. Symmetric encryption is typically more diligent than asymmetric encryption and is often used for bulk data encryption.

The Roman ruler Julius Caesar used a very simple cipher for secret data transfer in military purpose. He shifted each letter of the message with a letter three positions further along. Later, those ciphers that used this “displacement” concept for the generation of a cipher message were referred to as a Caesar cipher. Among all the substitution type ciphers, this Caesar cipher is the easiest to solve and most widely used, since there are only 25 possible combinations. Later, this type of cipher is implemented on a wheel device. A disk or wheel has the printed alphabet on it and then a movable smaller disk with the same alphabet printed on it is mounted forming an inner wheel. The inner wheel than can be rotated so that any letter on one wheel can be aligned with any letter on the other wheel and thus making the cipher text. The structure of a Caesar cipher wheel is shown in Fig. 1.

Fig. 1. Caesar cipher wheel

Lack of robustness, inability to encrypt symbols, sign, and numeric number and so on, several modifications are carried out based on the principle of Caesar cipher wheel. In addition to simple substitution ciphers, the cipher wheel opened the way for convenient poly alphabetic ciphers where multiple monoalphabetic ciphers were used with a specific monoalphabetic cipher to encode a letter in a specific position in the plaintext message. Another technique known as transposition cipher has been studied [12]. An encryption algorithm based on Caesar cipher has been proposed where alphabet index is checked first; if the alphabet index even then increases the value by one else the index is odd decrease the key value by one [13]. An assembled symmetric key algorithm which is generally an amalgamation of bit manipulation modified Vernam Cipher and modified Caesar Cipher has been presented [18]. A symmetric key algorithm based on ASCII value has been proposed where the key of fixed length 4 is used [10]. A concept of using floating point number as the symmetric key has been introduced [14]. To ameliorate the security, cipher text is watermarked in an existing

work [9]. A symmetric key algorithm has been proposed with the exclusive-OR operation to increase the level of security [15]. In another existing work, XOR operation was performed with XAES algorithm to improve security [16]. It is done for better security but as complexity increases resulting in speed decrease.

In this proposed modified Caesar cipher wheel algorithm, the modification increases the security keeping the speed of the symmetric encryption technique almost same.

3. PROPOSED ENCRYPTION METHOD

From the concept of this cipher wheel, in this algorithm, the sender and the recipient should have to agree on a certain number of characters into the code which is in an array and the scales would be shifted one character to the right according to the value of iteration repeating the procedure in a cyclic manner of the array. This would make it more difficult to crack, using statistical methods. For example, the array structure is:

i	ii	iii	.	.	.	N-1	N
X_1	X_2	X_3	.	.	.	X_{n-1}	X_n

Here, an array containing the values for replacing actual ASCII of length N is depicted. In this proposed algorithm, every N characters of plain text will be replaced by the array values. Substitution of ASCII values will continue in a periodic manner with periodicity N, till the end of the plain text.

A. Algorithm for Encryption Method:

Step 1: Take an array of size N.
Step 2: Choose any value of the array.
Step 3: Generate a loop for circulating the operation.
Step 4: Take the plaintext and ASCII values of the corresponding characters.
Step 5: Take any mathematical equation.
Step 6: Transmit that ASCII value's character which is evaluated in step 5.
Step 7: Transfer encrypted ASCII to cipher text.

B. Algorithm for Decryption Method:

Step 1: Take the same array of size N as used in the encryption process.
Step 2: Take the same values of the array as applied for encryption.
Step 3: Generate a loop for circulating the operation.
Step 4: Take the cipher text that was transmitted and take the ASCII values of the transmitted characters.
Step 5: Take the reverse mathematical equation which was used in the encryption process.
Step 6: Receive that ASCII value's character which is evaluated in step 5.
Step 7: Transfer decrypted ASCII to plain text.

C. Example of the proposed algorithm:

For the realization of proposed enhanced Caesar cipher algorithm, an example of message concealing in unreadable format is depicted below. For simplicity, an array of size, N = 12 was taken, hence the following cipher text was obtained.

i	ii	iii	iv	v	vi	vii	viii	ix	x	xi	xii
14	9	6	13	5	-1	7	16	11	-2	8	10

Plaintext: our glorious&evergreen Bangladesh
Cipher text: }~x-lkv¸tm}}4n|rwfyupl(Lowmyfcl*f*s

It is very convenient to say that the cipher text is far away from the original. Hence, consecutive same letter "ee" in plain text appeared by different one as well as similar adjacent symbol in cipher text "}}" representing different original character. Here space character is also encrypted so that prediction from small word is impossible. A minor change in the text key will change the cipher text quite a lot. After decryption, we will get the plaintext "our glorious & evergreen Bangladesh" in receiver.

In this algorithm, an array of any size and any chosen values are taken according to our pleasure. A loop is used to circulate the iteration number (i). After taking plaintext and ASCII values of the corresponding characters, a mathematical equation is used where the plain text character's ASCII values and the value of the array which is in present iteration number's position are used. Now,

cipher text is transmitted which is evaluated from the equation. For the next iteration the array position will also change as a result the value of the array in that position will also change. In the decryption part, the reverse process occurs.

4. IMPLEMENTATION OF PROPOSED METHOD

A. Proposed Model:

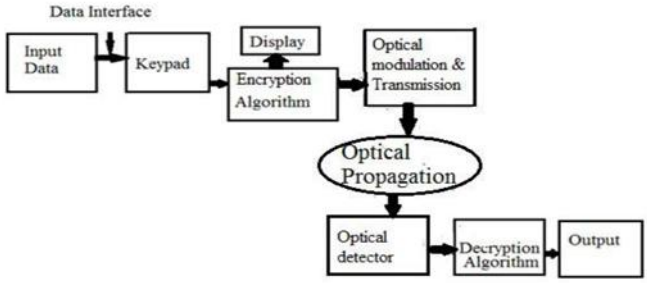

Fig. 2. Block diagram of the proposed method

Overall secured optical wireless communication is analyzed. At first, input data is taken from the user via the keypad. After taking the data as plain text, processing unit encrypt those using proposed encryption algorithm and displays the cipher text in LCD which is parallel communication. Then, the pulse duration of data is given for optical modulation and transmission. The information is steered in the pulse duration of the LASER. Its length carries the information of data. This process is denoted as optical propagation in the block diagram. Here, occurs the serial data communication. Data transfer through LASER from one processing unit to another via optical detector such as phototransistor is serial communication. When the LASER beam strikes the phototransistor, the signal would be sufficiently amplified and fed to one of the ports of the processing unit. When the port is high, the microcontroller reads the data. Here, Decryption algorithm decrypts data using a reverse algorithm that was encrypted and displays the plain text on LCD. Data from the microcontroller to LCD display is again parallel communication.

B. Hardware Implementation:

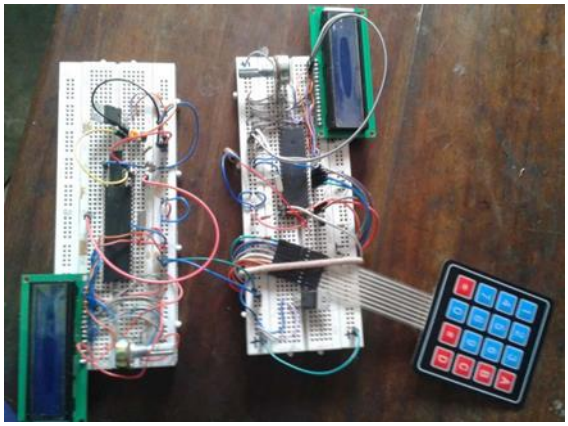

Fig. 3. Transceiver circuit

For practical implementation of the proposed method, a 4x4 keypad matrix (Hex code) was used to take the input. Microcontroller PIC16F877A was used as a processing and controlling unit. Here, 8 pins of keypad were connected to 8 pins of the microcontroller. ASCII pulses corresponding to keypad digits are transferred to the processing unit through a bus line. An op-amp (LM324) which is operated at 5V input is used as a comparator and it's inverting input is connected to a variable resistor of 1K. 5V power supply was used to conduct the circuit operations. A NPN transistor (BC547) was used for switching purpose. A normal (650 nm 5V) red dot LASER was used to transfer the data. At the receiver end, this LASER beam would strike the photo transistor and the signal would be sufficiently amplified and fed to one of the ports of the microcontroller. When the port is high, the output of photo transistor is thus fed to the receiving port of the second microcontroller. Later, this microcontroller reads and displays the characters in LCD display. Here, Asynchronous data transfer was used for serial communication which is done at 2400 baud rate.\

5. ROBUSTNESS OF THE ALGORITHM

The proposed encryption algorithm ensures strong security than conventional Caesar cipher Wheel algorithm as well as present modifications of it due to the wide variety of security parameters and flexibility of choosing their value. Proposed method substitutes the ASCII field randomly rather than sequential shift. Eventually, the same alphabet will appear different in several positions due to array length. Same character in cipher text for instance 'a' will reflect different meaning due to this reason.

Robustness of implemented algorithm is discussed below.

A) Security parameter: The proposed algorithm provides the choice of wide security parameters compared with traditional Caesar cipher which is as follows:

1) Length of array or wheel: Length of the used wheel or array is variable. One can choose the length according to their purpose. The more the size of the wheel the more strong security it provides. It is possible to encrypt the message whether the array length is smaller or larger (for small text) compared to the total length of the text.

2) Choice of value: Values of the array is user frankly. So, one can choose any value to encrypt their message. Larger shift corresponding to larger array value will introduce less frequently used a character from 8 bit extended ASCII table, will be harder to intercept by an intruder. But one caution should be taken that ASCII value must remain in between 255 after encryption.

3) Mathematical equation: By using complex mathematical formula, cipher text can be made more difficult to break. In this project, addition is used only. Modulus, subtraction or use multiple operators will enhance the algorithm. Eventually, several mathematical operations within each iteration and their sequence will make harder for breaking using Brute force attack.

B. Security level: In traditional Caesar cipher, characters are shifted by a fixed character which makes it easier to break. But in the proposed method, characters are replaced in a cyclic manner not by any sequential shift eventually differs in a change of ASCII value in a different position.

C. Flexibility: Encryption of all characters enlisted in eight-bit ASCII table is possible using this algorithm. This is a great achievement in the field of cryptography. The proposed method provides flexibility in the conversion from ASCII value to binary or hexadecimal value. The encrypted message can easily be modulated with the optical carrier by using a laser. Simple operations to encrypt plain text require less circuit complexity and processing delay.

An algorithm has been proposed which operates only when the length of input and length of the key are same [11]. In another existing encryption algorithm, automatically generated key having length equal to the plain text is used which requires more execution time for large plain text [17].This same key length limitation has overcome in the proposed algorithm. If anyone wants to break the cipher text, he has to know the three shared keys which are as security parameters.

6. FURTHER EXTENSION

Multiple operations such as voice, data, picture, and video can be transmitted simultaneously to perform secured optical communication using a LASER. Free space data communication can be implemented which is useful to transmit data wirelessly to the remote users and also provides connectivity to mobile platforms such as aircraft, ships. In order to increase the length, power received by the phototransistor is the limiting factor. It is intelligent to ensure high power available at the input terminal of phototransistor rather reduce the threshold of detection. High power LASER, as well as optical amplifier, can further enhance the range of communication. By using appropriate light coupling arrangement to the optical fiber, implemented encryption technique will ensure secured optical transmission over existing fiber link. The LASER can be replaced by IR LED that can't be visible by bare eyes. Security provided by this algorithm can be enhanced further if more the security parameters are used. Moreover, a combination of one more algorithm such as transposition cipher will make it more secure to transmit data.

7. CONCLUSION

Secured data transferring prototype of visible light communication system has been verified here. Caesar cipher is simplest encryption method because it is easy to compute but used less frequently due to its lack of robustness. Simplicity in implementation but difficulties in intercepting is the novelty of the introduced encryption technique. In this project, successful wireless secured data transmission has been conveyed using LASER, within 1m range because of low power of laser transmitter. The distance depends on the beam focusing capacity, optical transmission power, and use of optical amplifier etc. By introducing these or ensuring light coupling to fiber network, long distance secured optical communication can easily be achievable. Only specified receiver after knowing the security parameters can easily intercept the message due to the symmetric nature of the proposed algorithm.

8. REFERENCES

[1] S. Shekhar Singh, S.Bala, "Digital Data Transmission Using LASER" in Progress In Science in Engineering Research Journal ISSN 2347-6680 (E).
[2] B. Balachander, "Laser Based Data Signal Transmission Using Free Space Optics" in International Journal of Scientific Research æ´ä æ´ä ´¸Ï ´´ Â¸ ɔG
[3] A. Agrawal, G. Kumar, M. Narayan singh, P. kumar, P. mathur, D. Tsonev, S. Videv and H. Haas "Light Fidelity (Li-Fi): Towards All-Optical Networking" in Institute for Digital Communications, Li-Fi R&D Centre, The University of Edinburgh, EH9 3JL, Edinburgh, UK.
[4] A. Agrawal, G. Kumar, M. Narayan Singh, P. Kumar, Pransumathur "Data Transmission Using Laser Light", in International Journal of Advanced Computer Technology (IJACT) ISSN:2319-7900.]
[5] E. Ismael Imran, F. abdul, A. abdul kareem "Enhancement Caesar Cipher for Better Security" in IOSR Journal of Computer Engineering (IOSR- JCE)e-ISSN: 2278-0661, p- ISSN: 2278 8727Volume 16, Issue 3, Ver. V (May-Jun. 2014).
[6] L. Summerer, Oisin Purcell in "Concepts for wireles transmission via laser" ESA - Advanced Concepts Team Keplerlaan.
[7] A. Anagaw Ayele, Dr. V. Sreenivasarao "A Modified RSA Encryption Technique Based on Multiple public keys," in International Journal of Innovative Research in Computer and Communication Engineering [Vol. 1, Issue 4, June 2013].

[8] G. Mathew Padayattil, D. Poly, P. K. Paulson, M. Thomas, J. Joseph "Highly Efficient Free Space Laser Communication," in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 4, Issue 4, April 2015.
[9] R. Sultana, T. Madhavi Kumari "An ASCII Value based Optimized Text data Encryption System" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 5, Issue 8, August 2016.
[10] U. Singh, U. Garg "An ASCII value based text data encryption System" in International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013.
[11] A. Mathur "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," in International Journal on Computer Science and Engineering (IJCSE).
[12] A. Mishra "Enhancing Security of Caser Cipher using Different Methods," in IJRET: International Journal of Research in Engineering and Technology.
[13] K. Goyal, S. Kinger "Modified Caesar Cipher for Better Security Enhancement" in International Journal of Computer Applications (0975– 8887) Volume 73– No.3, July 2013.
[14] M. Lavanya1, R. Vijay Sai, A. Festina, J. Eshwari, T. Manopriya and V. Vaithiyanathan "An Encryption Algorithm Functioning on ASCII Values and Random Number Generation"in Indian Journal of Science and Technology, Vol 8(35), December 2015.
[15] 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.
[16] Charru, P. Singh, S. Rani "Improved Cryptography Algorithm to Enhanced Data Security" in International Journal for Research in Applied Science and Engineering Technology (IJR ASET), Vol. 2 Issue IX, September 2014.
[17] R. Satyajeet Shinge, R. Patil "An Encryption Algorithm Based on ASCII Value of Data" in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234.
[18] S. Dey,"SD-AREE-I Cipher: Amalgamation of Bit Manipulation, Modified VERNAM CIPHER & Modified Caesar Cipher (SD-AREE)" in I.J.Modern Education and Computer Science, 2012, 6, 43-49 Published Online June 2012 in MECS.
[19] Senior John M, Optical Fibre Communication
[20] G. Sharma, A. Kakkar "Cryptography Algorithms and approaches used for data security" in International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 ISSN 2229-5518.

