Acta Scientific COMPUTER SCIENCES

Volume 6 Issue 1 January 2024

Research Article

# Light-Fidelity Systems: Architecture and Modulation

**Hamada Louiza[1]*, Lorenz Pascal[2] and Djerouni Aicha[3]**

[1]*MAGELLAN Laboratory, Jean Moulin University, France*

[2]*IRIMAS Institute, University of Haute Alsace, France*

[3]*LARESI Laboratory, University of Sciences and Technology of Oran, Algeria*

***Corresponding Author:** Hamada Louiza, MAGELLAN Laboratory, Jean Moulin University, France.

**Received:** December 11, 2023

**Published:** December 19, 2023



## Abstract

New technologies such as Wireless Fidelity now make wireless Internet access possible. Wi-Fi, also known as IEEE 802.11, uses WLAN -11n to transmit broadband data over a 150 Mbps range. A more robust wireless access technology was needed to address the many issues of security, transmission capacity, throughput, and interference. Optical bandwidth is underutilized and offers promising solutions with tens of gigabits per second, making it particularly suitable for indoor environments. A major technology revolution, such as VLC: visible light communications and/or Li-Fi: light fidelity, might promise significantly upper binary data as well as improved physical layer security and data integrity. This new technology enables the transmission of data through visible light using a light-emitting diode bulb that can be turned on and off several thousand times imperceptibly to the eye. This paper describes modulation schemes in visible light communication systems, introduces Li-Fi and the different noises in a Li-Fi system, and the contribution we made.

**Keywords:** Light Fidelity; Visible Light Communication; Modulation; OOK; Berlekamp-Massey

## Abbreviations

BM: Berlekanp Massey; BM-XOR: Berlekampmassey-xor; DC: Direct Current; FOV: Field of View; IPPM: Inverse Pulse Position Modulation; LED: Light Emitting Diode; LFSR: Linear Feedback Shifting Register; Li-Fi: Light Fidelity; LOS: Line of Sight; NLOS: Non Line of Sight; OCT: optical Coding Technique; OFDM: Orthogonal Frequency Division Multiplex; OOK: On-Off Keying; PD: Photo-Detection; PHY: Physical Layer; PPM: Pulse Position Modulation; RS: Reed-Solomon; VLC: Visible Light Communication; VPPM: Variable Pulse Position Modulation

## Introduction

VLC is the new wireless communication technology paradigm, which was proposed for the first time in the early 2000s [1]. A visible light communication systemis intended to be a straightforward wireless communication link from one point to another electroluminescent diode and a photodiode device as a receiver [18]. The bit rate obtained is determined by the digital technology and the brightness [2,3]. This system with white electroluminescent diode illumination received much attention in the last decade [17]. According to [3]. To increase bandwidth transmission, the authors propose an indoor cellular system handover algorithm [3]. The development of Li-Fi technology is still in its early stages. Many security studies have been conducted in various fields such as physics, MAC layer, topologies, indoor and outdoor communications, co-channel interference, and many others. However, most research on security concerns in light fidelity communication has concentrated on individual attacks.

The author cites the physical characteristics of visible light communications relevant to security in [4], and systematically criticizes security risks and weaknesses regarding the unique characteristics of visible light communications devices, as well as a summary of all security techniques proposed in the literature. So far, visible light communications have addressed physical layer security based on an information theory standpoint, as well as issues of accessibility and reliability (specifically, transmission scrambling and potential data corruption) [5]. Several authors have used transmission and modulation strategies in their articles, in [4,6] data transmission methods based on diode light modulation are discussed. Without mentioning [6] the authors suggest a light fidelity system access point structure based on OFDM and an OCT to enable full optical transmission and processing in the collection network [18]. We will also look at an LED-based study to describe the viability of a visible-light emitter receptor in open space as the foundation of an internal no-wire network and achieve an adoption rate. The error is acceptable for internal use with a low-cost system. The article's authors [5] provide a detailed overview of Li-Fi technology, including its operation, applications, benefits, and drawbacks.

IEEE 802.15.7, enabled by recent advances in light-emitting diode technology, provides high-speed visible light up to 93 Mb/s via rapid modulation of dimmable optical light sources [6]. Peak transmission rates of up to 8 Gbps using a single light source have been demonstrated in [7]. At this point, Harald Haas discusses new Li-Fi applications.

## LI-FI system architecture

A Li-Fi system has two parts: a transmitter that modulates the light coming from the LEDs, and a receiver based on a photodetector to recover the modulated signal. The transmitter and receiver are connected via the VLC channel.

## Transmitter section

A Li-Fi transceiver's transmitter is an LED, whose illumination function assures more than 50,000 hours of usage while lowering energy consumption by 80%. The cheapest LEDs are phosphor converted (pc-LEDs), which contains a blue InGaN LED bulb that pumps a layer of YAG phosphor. Phosphor transforms some blue light to green brightness, yellow brightness and the red brightness; a combination of the intensities of the primary colours allows for the creation of cold white, neutral white, or warm white while retaining maximum efficiency. RGB LEDs, also known as multi-chip LEDs, are substantially more costly but have a greater bandwidth.

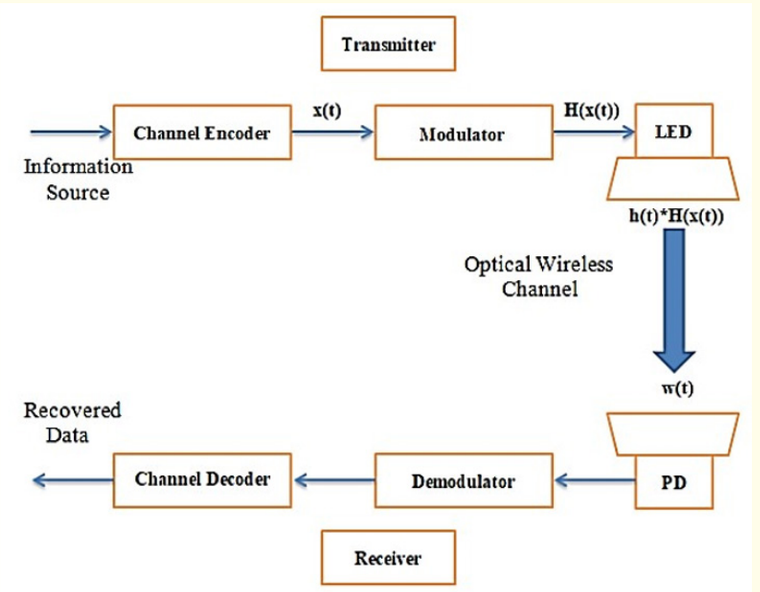


**Figure 1:** The modified block diagram for Li-Fi system.

## Receiver section

The photo-diode (PD) and the light-collecting lens are the two main components of the receiver. The choice of lens design is determined by the PD. Because of the avalanche process, an avalanche PD has a high gain but is also highly sensitive to quantum noise. PIN-type photo-diode are more stable at high temperatures, have a higher light output, and are less expensive. A PIN photo-diode is an excellent choice for a low bandwidth application; however, an avalanche PD is recommended for a high flow rate application. The capacitance of photo-diode is linked to its reaction time: the smaller the detecting surface, the smaller the capacitance, and the faster the response.

The luminous flux, on the other hand, is less essential and hence captures less signal. Lenses can be used to improve signal reception by allowing sensors to enhance light flow, resulting in (a) increased throughput and (b) increased signal range. The form of the lenses must be considered while developing them because a hemispherical lens cannot be integrated into mobile communication devices owing to its size and volume. It is also important to consider the total volume of the lens and possibly the size of the image of the emitting source.

## Propagation links

VLC propagation links are classified into three types based on the directionality of the transmitter and receiver: directional links, non-directional links, and hybrid links. The transmitter and receiver in a directional link point directly at each other, and the half angle and field of view (FOV) are small. As a result, the system based on the direct link performs well. The transmitter and receiver in the non-directional link have a wide half-angle for ease of operation. The transmitter and receiver in the hybrid link are oriented differently (narrow half-angle transmitter combined with a large field of view receiver or large half-angle transmitter combined to a close field of view receiver). The different propagation links are shown in Figure 3 [16].

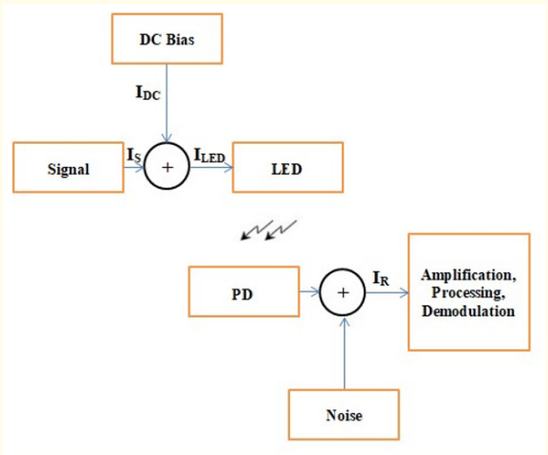


**Figure 1:** Basic diagram of the Li-Fi system. IDC: bias current, IS: signal current, ILED: LED supply current, IR: signal current.

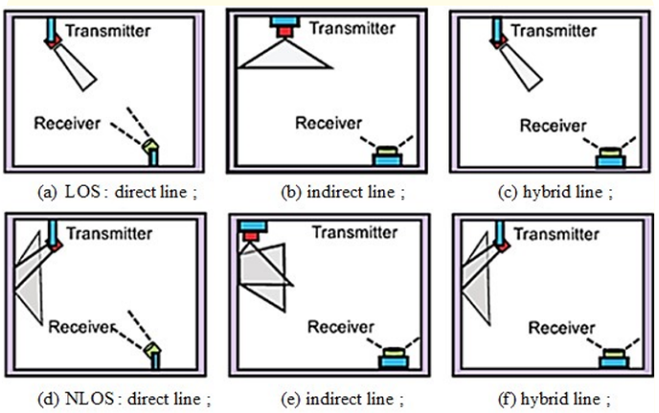


**Figure 3:** Propagation links.

## Introduction to security in VLC systems

Nowadays, the issue of security for a visible light transmission system is a major one. First of all, it is necessary to maintain the confidentiality of information to ensure that only approved persons have access, as well as to protect networked information, access to computer systems and applications, as well as backing up files or keywords saved on networked machines [14]. This issue can be remedied by requesting users to use passwords to access their machines and also to protect their confidential documents with passwords and use a digital signature for their emails. The other security challenge is infrastructure protection. The goals are to protect against network device configuration attacks, theft of network resources, and thus malicious network nodes or connections with data parasites that prevent communication [14]. The IEEE 802.15.7 standard defines the security and modulation mechanisms at the physical layer level, and at the data link layer, access control with the MAC sub-layer. As already mentioned several articles have elaborated the security subject in Li-Fi, our algorithm constitutes a contribution to secure more LiFi networks. Even if an attacker knows the encryption principle, he will not be able to decipher the confidential message due to the method of encoding and decoding of this message. We do not take into account the redundancies in the message, unlike other existing algorithms.

## Modulation in Li-Fi systems

In this part, we go through four distinct modulation strategies for encapsulating information in the temporal domain in the context of VLC in further depth. The fundamental distinction between traditional communication scenarios and VLC is the requirement to maintain appropriate communication performance while also dimming the light intensity.

## On-Off Keying methodology

The system employs OOK: on off keying modulation, which is the most fundamental modulation pattern for visible light communications systems. The light emitting diodes are turned on and off based on whether the data bits are ”one” or ”null” [18]. When modulation on off keying is disabled, the illumination can be easily reduced as long as the network can distinguish between ”on” and ”off” [18]. On off keying modulation represents data bits ”1” and ”0” with an light emitting diode that blinks on and off. The intensity of the light is lowered but not completely shut off in the off state. The main benefit of OOK is its simplicity and ease of usage. It is typically used in wireline communication. The bulk of the researchers employed OOK modulation for VLC utilizing White LED in their early work. It generates the blue emitter using a yellow phosphor. Because of the sluggish reaction time of the yellow phosphor, the primary constraint of white light diode is its limited transmission speed (few megahertz [8]). [9] proposes using NRZ-OOK with a bright LED, and a VLC connection with a data throughput of 10 Mbps was shown [17].

The blue filter is employed to reduce the yellow component’s poor reaction rate, resulting in a data rate of 40 Mbps [8].

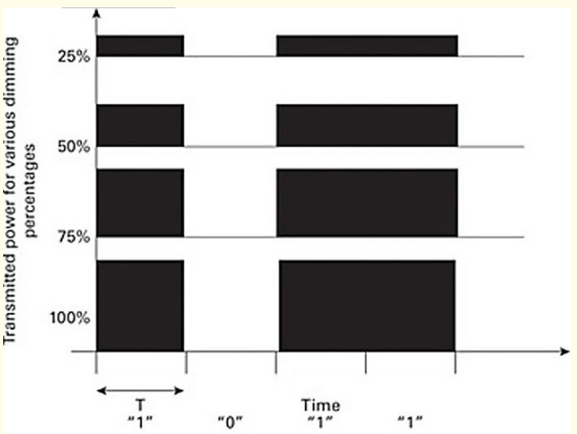


**Figure 4:** OOK with varying dimming levels, the encoded information is “1 0 1 1”.

As a result, [10,11] advocated combining blue filtering with basic equalization at the receiver to limit and reach data speeds of 100 Mbps and 125Mbps, respectively. The performance may be improved by selecting the right photodiode. The authors of [12] shown that the avalanche photodiode, rather than the P-I-N photodiode, performs effectively at the receiver side. A data rate of up to 230 Mbps was achieved using an avalanche photodiode. The combination of RGB frequencies produces white brightness. The key advantage of white light emitting diodes is that they do not have a poor reaction time [17]. To avoid the white light, RGB white LEDs require three distinct driving circuits. In this study [13], a novel technique is applied, and it was discovered that while the white light emitting diode with RGB characteristics was used, only the red light emitting diode was controlled by the data transfer while remaining to give light. The authors employed a P-I-N photodiode and attained a data throughput of 477 Mbps but were unable to establish a distance range. The two approaches were proposed in IEEE Standards in [7] as IEEE 802.15.7, which supports dimming and on off keying as a modulation scheme.

Redefining the on and off levels: The varied levels of light intensity are assigned to the on/off rates to attain the appropriate amount of gradation. The advantage of this approach is that the necessary amount of dimming may be obtained without the addition of an overhead bit. It maintains the same data rate as non-return to zero with on off keying modulation, although the transmission is reduced at low gradation levels. The use of lower light intensities for switching on and off is a disadvantage that requires the use of low power circuits, which has been proven to acquire changes in rendering (radiated shade of LED changes) [14].

Compensation periods: When the LED is entirely turned on, more compensating periods with the same on and off level of modulation are added, which are known as on periods or off periods (off periods). Compensation period's term duration is decided by the desired amount of dimming. If the needed dimming level is greater than 50%, the on times are added; otherwise, the off periods are added. The authors of [15] developed a technique for determining dimming level based on the percentage duration of active data transmission β within the emission range Tr to produce a gradation degree DM as

$(2 - 2DM) * 100: DM > 0.5$

$\beta = \{ (1)\ 2DM * 100: DM \leq 0.5$

The maximum communication efficiency $E_D$ can be computed by utilizing information theoretic entropy as the input when the required gradation degree is DM with on off keying as the input

$$E_D = -DMlog_2DM - (1 - DM)log_2(1 - DM) \quad (2)$$

It suggests that the effectiveness of a communication system is a triangle function of the gradation degree, with maximal proficiency at a gradation degree of 50%. When the dimming intensity is reduced from 0% to 100%, the efficiency decreases linearly. Because of the compensating intervals utilized in dimming, the data rate is lowered. The intensity attribute of ON/OFF modulations remains unaltered, as does the scope of the communication. In order to address the issue of low data rate during compensating periods, [16] proposed employing a reverse coding of the source to maintain rate of data throughput while attaining the necessary amount of gradation.

## Variable pulse position modulation

VPPM is a type of modulation that a text represented by bits is encrypted by broadcasting a pulse at the beginning and end of the symbol for ”0” and ”1” [12]. The duration of the pulse is governed by the proportion of needed light (dimming). The fundamental advantage of this technology is that as long as there is some illumination, changes in the degree of dimming have no effect on communication. This technique is repeated every T seconds, resulting in a bit rate of 1/T bits/second conveyed (Figure 5) [11].

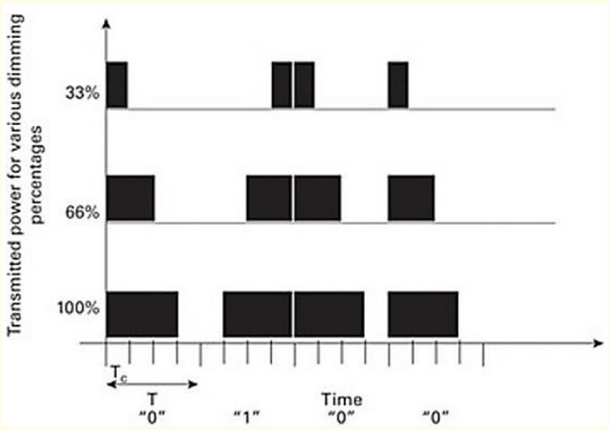


**Figure 5:** VPPM with varying dimming levels, the encoded information is “0 1 0 0”.

## Pulse position modulation

PPM [6-8] is a type of signal modulation that M message bits are encoding by the transmission of a pulse with a duration of $T_C = T/2^M$ seconds in one of $2^M$ possible time shifts within a T-second time interval. This pattern is repeated every T seconds, resulting in a bit rate of M/T bits per second. Light dimming is accomplished by lowering the power of the transmitted pulses by the required dimming percentage (Figure 6) [11].

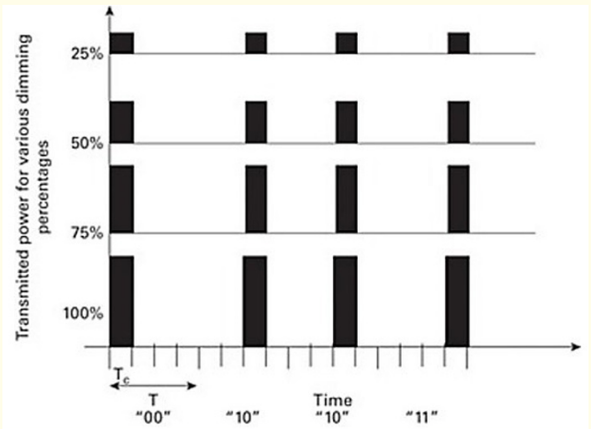


**Figure 6:** PPM with various dimming percentages, where the encoded information is ”00 10 10 11”.

## Inverse pulse position modulation

Inverse Pulse Position Modulation [9] is a type of signal modulation that M bits of the message are encoding by the transmission for T seconds, except for a ”hole” in one of the $2^M$ possible time shifts. This ”hole” has a duration of $T_C = T/2^M$. This pattern is repeated every T seconds, resulting in a bit rate of M/T bits per second. Dimming the light is accomplished by lowering the power of the transmitted pulse by the required dimming percentage (Figure 7) [11].

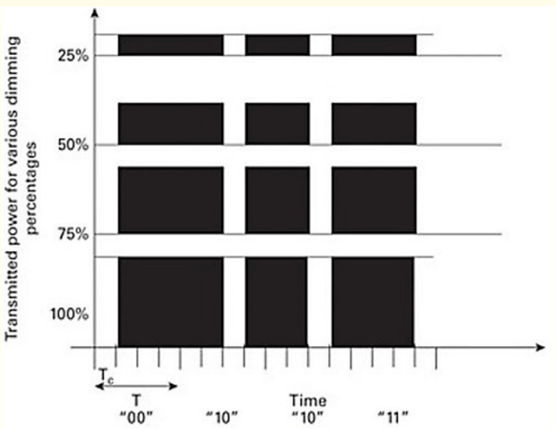


**Figure 7:** IPPM with varying dimming percentages, where the encoded information is ”00 10 10 11”.

## Contributions and analysis

For our study we used Reed Solomon’s error correcting codes. Berlekamp-Massey is a derivation of Reed Solomon’s error-correcting codes[18], which consists on the one hand in constructing an LFSR of length L*N for all N, and an output polynomial $f_N$ which allows to generate the first N bits of sequences [13]. The idea of proposing this algorithm is to ensure data confidentiality and authentication of the persons authorized to access the network. We have modified the Berlekamp-Massey algorithm and then proposed a method to encode, decode and correct the transmission errors of the data sent through the Li-Fi.

**Algorithm I** Berlekamp-Massey

Input: $b_0$; $b_1$; …; $b_{N-1}$ a sequence of bits of N length

Output: LFSR of length N/2

$f(x) = 1 + c_1x + c_2x^2 + \ldots + c_nx^n$ (to find) Initialisation: f(x)=1; m=-1; L=0; g(x)=1;

For N = 0 to n-1

calculer $d = bN + \sum_{i=1}^{L} C_i b_{N-i} \bmod 2$

If d = 1 do t(x) = f(x)

$f(x) = f(x) + g(x)*x^{N-m}$

If 2L ≤ N then { L=N+1-L, m = N, g(x)=t(x) }

The algorithm takes as input the sequence of N bits, as output we expect (02) values, f(x) the feedback polynomial, and the succession of values of d’ which constitutes the key of our algorithm. In BM, d represents the distance between the feedback coefficients $C_i$ and the bits $b_i$.

**Algorithm II** Berlekamp Massey-XOR

Input: $b_0$, $b_1$,….,$b_{N-1}$ a sequence of bits of N length

Output: LFSR of length n = N/2 ; $f(x) = 1 + c_1x + c_2x^2 + \ldots\ldots + c_nx^n$ (to find) ; d’ Initialization: f(x)=1; m=-1; L=0; g(x)=1;

For N = 0 ◊ n-1

$d' = bN + \sum_{i=1}^{L} c_i b_{N-i} \bmod k$

If d’ = 0 do n=n+1

If d’≠0 do

$\{ f(x) = f(x) + g(x).x^{N-m}$

g(x)=t(x) } If 2L≤ N then { L=N+1-L, m = N, t(x) = f(x)

}

The modification made consists in adding the variable ”k” a prime number different from 1 [18]. Our algorithm allows to encrypt and decode as well as to correct transmission errors. The coding is done at the transmitter level by applying an xor between the initial message in binary, the feedback polynomial f(x), the key d’ and the value of k. All these variables are handled in binary. For the operation of decoding is made at the level of the receiver always by applying a xor between the coded message and the key d’ as well as the variable of k. In final, comes the operation of the correction of errors which consists in applying a xor between the decoded message and the polynomial of feedback. The advantage of this algorithm is the absence of redundancies in the decoded message and the speed of execution, despite the simplicity of the calculations, an attacker cannot know the encrypted message even if he knows the initial algorithm.

The complexity is at the level of the key ”d’”, for example if d’ = [122111] and k = 3 and 6 bits for the message to be coded, for the encryption and decryption we will take d’= [101001] the decimal values will be converted into binary on 3 bits (of k), we thus consider only the first six bits of the key. The complexity is of O(L) for the encoding and the decoding [18].

## BM or BM-XOR

The table below (Table 1) shows a comparison between BerlekampMassey and BM-XOR. Encoding is done at the transmitter level, we encode the information sent through the signal to prevent any unauthorized user to access the confidential data. As we have already mentioned, the objective of our study is to modify the Ber-

| BM | BM-XOR |
|---|---|
| Mod 2 | Mod k |
| Localize transmission errors | Localize transmission errors;<br>Encrypting a message;<br>Decrypt a message;<br>Correcting transmission errors. |
| $O(L^2)$ coding and decoding | O(L) coding and decoding |

**Table 1:** CHOICE OF BM-XOR.

lekampMassey (BM) algorithm to encode and decode a message, and to propose an algorithm to correct transmission errors. The decoding and error correction step is performed at the receiver.

## Future works

At this point, we have several ideas that we would like to develop in the future: 1) Li-Fi systems are usually deployed for indoor environments, why not try to deploy them (indoor), why not try to deploy them in outdoor systems (outdoor) systems; 2) The modulation of the signal is a major point for a Li-Fi system, at the physical layer the architecture is based on the Manchester two-phase coding, and we would like to develop more this coding to be able to code a message by the Manchester coding, to modify it at the transmitter side and to send it through the signal to the receiver; 3) Develop an application within the universities, to be able to identify the students by visible light for example during an exam or a lecture; 4) Review the line of sight problem that is LOS in LiFi systems, see the NLOS propagation link and how to deploy it, maybe the idea will offer a solution for the non propagation of light waves through walls and objects; 5) What we are looking to do more is a two-factor authentication using the OTP protocol. To remember, OTP is only valid for a single session or transaction [19]. OTPs help solve some of the drawbacks of standard static passwords, such as vulnerability to rejection attacks. This means that if a potential intruder saves an OTP that was previously used to log in to a service or execute a transaction, they will not be able to use it because it is no longer valid. OTPs, on the other hand, cannot be stored by humans and therefore require the use of another technology [15]. The user provides a one-time key, which will be stored in a database, the user will not be able to provide the same password the next time he/she logs in, each time a key will be generated, it will be automatically stored in a database, all these manipulations are done from a smartphone LED for a cost reduction. The user indicates his password, then he will receive a coded message on his smartphone for the 2nd authorization. The OTPs are created by a mathematical process that bases the new password on a challenge or a counter.

## Conclusion

The globe is on high alert due to the outbreak of the COVID-19 virus. The patients in critical centers care in hospitals should be continuously watched at any times and necessitate specific technology to keep regular physiological processes [1]. The issue is determining how to keep track of each patient while protecting their confidential data [4]. This paper summarizes the various works already and in progress within the realm of visible light communications. The essential components of a Li-Fi system have been mentioned.

Our current objective is to develop a secure system within hospitals (also in other environments) for the transmission of confidential data based on error correction codes to generate random keys and to be able to encrypt and decode data transmitted through the Li-Fi light signal. BM-XOR is an original idea based on a subalgorithm of the RS algorithms, BM-XOR allows to encode, decode a message and to correct the transmission errors produced in a small time interval, the algorithm will not take into account the redundancies added to the sending of the message, i.e. if a transmitter sends a message of 6 bits the receiver will receive the message with errors of 6 bits, which makes that one has a complexity of O(L) whereas for BM one has a complexity of $O(L^2)$ and for RS $O(n\log_2 n)$ and which makes this last longer.

## Bibliography

1. Lorenz P and Hamada L. "LiFi Towards 5G: Concepts Challenges Applications in Telemedecine". 2020 Second International Conference on Embedded and Distributed Systems (EDiS), (2020): 123-127.

2. Haas H. "LiFi is a paradigm-shifting 5G technology". *Reviews in Physics* 3 (2017): 26-31.

3. Karunatilaka D., *et al*. "LED Based Indoor Visible Light Communications: State of the Art". *IEEE Communications Surveys and Tutorials* 17.3 (2015): 1649-1678.

4. Hamada L and Lorenz P. "A Revolution in Wireless Networking for Smart Communication Through Illumination". *Acta Scientific Computer Sciences* 3.10 (2021): 53-58.

5. Al-Moliki Y M., *et al*. "Secret Key Generation Protocol for Optical OFDM Systems in Indoor VLC Networks". *IEEE Photonics Journal* 9.2 (2017): 1-15.

6. Rajagopal S., *et al*. "IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support". *IEEE Communications Magazine* 50.3 (2012): 72-82.

7. Ghassemlooy Z., *et al*. "Optical Wireless Communications: System and Channel Modelling with Matlab®". *CRC Press* (2012).

8. Choi J-ho., *et al*. "Visible light communications employing PPM and PWM formats for simultaneous data transmission and dimming". *Optical and Quantum Electronics* (2014): 1-14.

9. Arnon S. "The effect of clock jitter in visible light communication applications". *Journal of Lightwave Technology* 30.21 (2012): 3434-3439.

10. "IEEE Standard for Local and Metropolitan Area Networks–Part 15.7: Short-Range Wireless Optical Communication Using Visible Light". in IEEE Std 802.15.7-2011 (2011): 1-309.

11. Arnon S. "Visible Light Communication". Cambridge University Press, (2015).

12. Arnon S., *et al*. "Advanced Optical Wireless Communication Systems". Cambridge University Press (2012).

13. https://en.wikipedia.org/wiki/Berlekamp-Massey

14. Farrel A. "The Internet and Its Protocols: A Comparative Approach". Morgan Kaufmann Publishers In, Chapter 14 (2004): 677-681.

15. https://en.wikipedia.org/wiki/One-time-pad

16. Wang Z., *et al*. "Visible Light Communications: Modulation and Signal Processing". (2017).

17. Faisal A., *et al*. "A Review of Modulation Schemes for Visible Light Communication". *International Journal of Computer Science and Network Security* 18 (2018): 117-125.

18. Hamada L., *et al*. "Security Challenges for Light Emitting Systems". *Future Internet, MDPI* 13.11 (2021): 1-11.

19. Thuraisingham B. "Developing and Securing the Cloud". Auerbach Publications (2018).