Iraqi Journal for Computer Science and Mathematics

Manuscript 1257

Cipher Text to Secure Li-Fi System Using Hybrid Encryption Algorithm

Mohammed M. Ahmed

Satea H. Alnajjar

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:210–220

ORIGINAL STUDY

Cipher Text to Secure Li-Fi System Using Hybrid Encryption Algorithm

Mohammed M. Ahmed [a,*], **Satea H. Alnajjar** [b]

[a] Department of Computer Engineering, College of Engineering, Al-iraqia University, Baghdad, Iraq
[b] Department of Network Engineering, College of Engineering, Al-iraqia University, Baghdad, Iraq

ABSTRACT

It is important to pay attention to develop our security systems, due to the increase in cyberattacks and the development of their methods and the work to develop quantum computers capable of penetrating the solution of complex equations of encryption algorithms. The need to develop protection methods has emerged in line with the development of hackers to ensure the security and safety of users' data. In this research, work was done on the modern Li-Fi technology based on comparing the values with Kim's model and a distance of more than 13 km was reached in the fresh air. This technology provides security and privacy inside rooms because it sends signals through light, so the signal cannot be modified from the outside. However, the threat remains through the transmission medium. Therefore, a hybrid algorithm was created from chacha20 with a key size of 256 and RSA with a key size of 2048, which guarantees us a high level of security, making it immune to threats. The chacha20 algorithm provides encryption speed and security, while the RSA algorithm increases the level of security of the algorithm, as the total time taken to encrypt data from the sender and decrypt it from the receiver was 0.036 seconds. This ensures high and fast performance for this hybrid algorithm.

Keywords: Li-Fi, FSO, Fiber optics, ChaCha20, RSA, Hybrid encryption algorithm

1. Introduction

1.1. Literature review

Recent years have seen incredible advances in cryptography by harnessing the power of quantum computing. Many new primitives such as fully secure key agreements, quantum copy protection, one-shot signatures, and others, which are not known to exist in the classical world, can be created in the quantum environment, leading to significant advances in cryptographic capabilities [1]. Comprehending the various methods employed by different regions is crucial in the realm of modern information security, as data encryption plays a pivotal role [2]. In order to safeguard sensitive information such as client data and business details, it is imperative to employ encryption techniques. By implementing encryption, one can effectively mitigate the risks of illegal access, data breaches, and the subsequent financial ramifications, reputation harm, and legal complications. Furthermore, in order to streamline the implementation of data mining methods, the encryption must be compatible with domain computation [3]. Encryption is a mathematical discipline that focuses on converting multimedia data through a series of transformations. It serves as a crucial instrument for ensuring security in the storage and transfer of data. The process transforms unprocessed photos, video, or audio into an unintelligible data format using a confidential encryption key. Encryption methods can be categorized into three types: keyless methods, single-key methods, and double-key methods [4].

The transformation function in two-key approaches employs a pair of distinct keys. The two keys are

Received 20 September 2024; revised 3 April 2025; accepted 16 April 2025.
Available online 24 May 2025

* Corresponding author.
E-mail addresses: mohamed1997aldulaimy@gmail.com (M. M. Ahmed), sateaahn@gmail.com (S. H. Alnajjar).

https://doi.org/10.52866/2788-7421.1257

interconnected and are commonly known as the public and private keys. The public key is widely known, while the corresponding private key is exclusive to a single individual [5]. 5G wireless networks are anticipated to heavily rely on Free-space optical (FSO) communication. FSO lines offer a viable alternative to traditional fiber optic cables used for backhaul links since they are easy to deploy, have a quick setup time, and need low maintenance costs [6, 7]. Optical Wireless Communication (OWC) systems can deliver high-data-rate services from nanometers to 10,000 kilometers. Thus, OWC could be a suitable solution for high-density, high-capacity networks [8]. Wi-Fi is the most adaptable and effective wireless data transfer technology. Wi-Fi faces capacity, availability, efficiency, and security issues due to various accesses [9]. Li-Fi uses visible light for communication. The wall is impermeable to light, making Li-Fi technology more secure and solving Wi-Fi's radio frequency bandwidth shortage. If an indoor communication vulnerability arises and the wall leak may prompt a hacker to attack the network, an exception can be established. Therefore, one or all levels of Li-Fi technology need encryption data to secure data [10, 11]. Authenticated Encryption (AE) ensures the confidentiality, integrity, and validity of encrypted data [12]. The ChaCha20 stream cipher authenticator is a cryptographic algorithm developed by Daniel J. Bernstein with the aim of providing a high level of security [13]. The ChaCha family of stream ciphers was introduced by Daniel J. Bernstein. The revised Salsa family of stream ciphers demonstrates enhanced diffusion per round, making it a notable improvement over the previous version Around the same time, the CFRG began looking into whether the ChaCha20 stream cipher and the Poly1305 authenticator could be used as alternative ciphers in the Transport Layer Security (TLS) protocol. This was done because the RC4 cipher had major security issues and the CBC block mode was hard to implement [15]. The authenticator that is made when ChaCha20 is used to make Poly1305 one-time secret keys from public nonce values is called Poly1305-ChaCha20 [16]. Chacha20 is a stream cipher that is derived from Salsa20. It employs an 8-round cipher known as Salsa 20/8 and uses 256-bit keys [17]. The RSA algorithm was first introduced in 1977 by Rivest, Shamir, and Adleman as the initial comprehensive public-key cryptographic algorithm [18]. The RSA algorithm is a widely employed asymmetric algorithm. It utilizes the process of multiplying two prime numbers of significant magnitude in order to generate a cryptographic key. The public key is utilized for encryption, whereas the private key is employed for decryption. The security of the RSA method is based on the challenging task of factoring huge prime integers. The process of factoring is performed in order to acquire the private key [19, 20].

The RSA algorithm is implemented to encrypt messages that have been prepared previously. The RSA encryption process is carried out using mathematical formulas that have been specified in the RSA algorithm [21, 22].

1.2. Contribution of the study

After a comprehensive review of the research and identification of the relevant research gaps, our work makes a contribution to increasing the security of the Li-Fi communication system, which uses encryption algorithms. Li-Fi technology addresses the issue of limited wireless bandwidth in Wi-Fi and offers enhanced security due to the inability of light to pass through walls. However, an exception can be made if a security vulnerability appears when making an internal connection, and the leakage of the wall may lead the hacker to attack the network. Hence, the implementation of data encryption is essential in either one or all layers of Li-Fi technology to ensure the security of the data. The research paper suggests a hybrid encryption technique that combines the chacha20 and RSA algorithms. This methodology enables to increase the security level of the Li-Fi network. By using this hybrid algorithm to encrypt users' private data, our approach ensures the security of users' data transmitted through the Li-Fi system and maintains privacy. Thus, adopting this formula ensures high network security and reliability in transmitting important and sensitive data.

The paper is organized in this way. This paper consists of five parts: the details of the study are presented in Section 2, the hybrid algorithm is explained in Section 3, the results are specified in Section 4, and the conclusions are presented in Section 5.

2. The proposed method

The proposed system is configured using Optisystem V21, OptiSystem is a software tool designed for the simulation and analysis of optical communication systems. It is widely used in engineering and research to model, design, and optimize optical networks and components. as shown in Fig. 1. Each part of the design will be explained in detail in sequence.

2.1. Transmitter module

The two components of the transmitter. To produce a 3 Gbps NRZ signal, there is an NRZ transmitter. The output of the MATLAB bit sequence generator

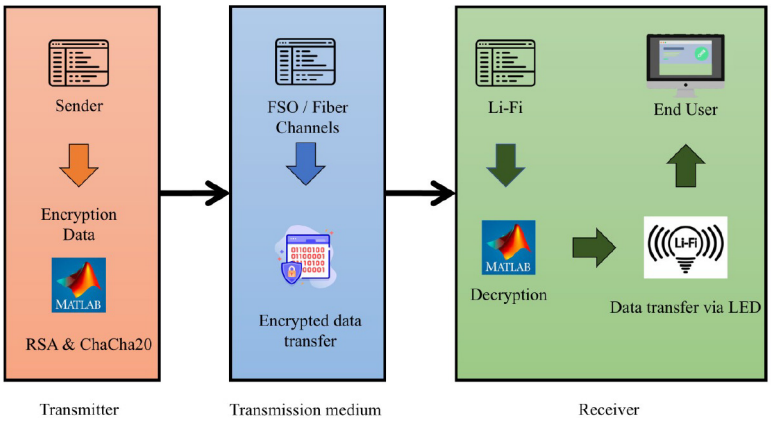

Fig. 1. Proposed system design.

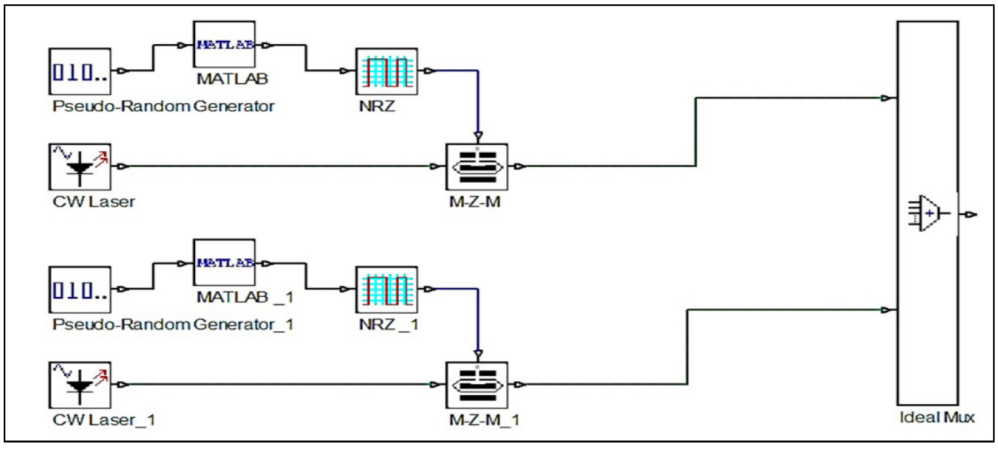

Fig. 2. Transmitter part design.

is placed in a pulse generator. An externally modulated laser operating at a wavelength of 1550 nm and 1555 nm is modulated using NRZ pulses. The Mach-Zehnder modulator is an interferometric intensity modulation device. It implements a continuous wave (CW) laser. The output is sent to the FSO channel as shown in Fig. 2.

2.2. Free space optical

FSO employs laser technology to transmit high-capacity optical connections without the need for physical cables. Additionally, it employs an optical communications method to transmit data for telecommunications and computer networking. FSO systems are designed to natively handle many channels as shown in Fig. 3.

2.3. Fiber optic channel

The fiber optic cable consisted of a 40-kilometer single-mode fiber (SMF) and two 3.2-kilometer dispersion-compensating fibers (DCF) (FOC). An optical amplifier is required to assess the effectiveness of the performance design of the FOC system shown in Fig. 4.

2.4. Li-Fi

Li-Fi, an advanced optical wireless communication technology, holds significant potential compared to other solutions due to the energy and cost efficiency of the light-emitting diode. Li-Fi may fulfill this requirement by using its numerous benefits, such as its ability to achieve high data transfer speeds, minimize electromagnetic interference, and provide indoor localization capabilities These units or components may be used as either a band-reject or a band-pass filter. Consequently, there will be a certain degree of light reflection as the light passes through the portion of the fiber that contains Fiber Bragg Grating (FBG). The reflected light is returned to the source because its wavelength matches Bragg's. In contrast, other wavelengths are transmitted by trans impedance

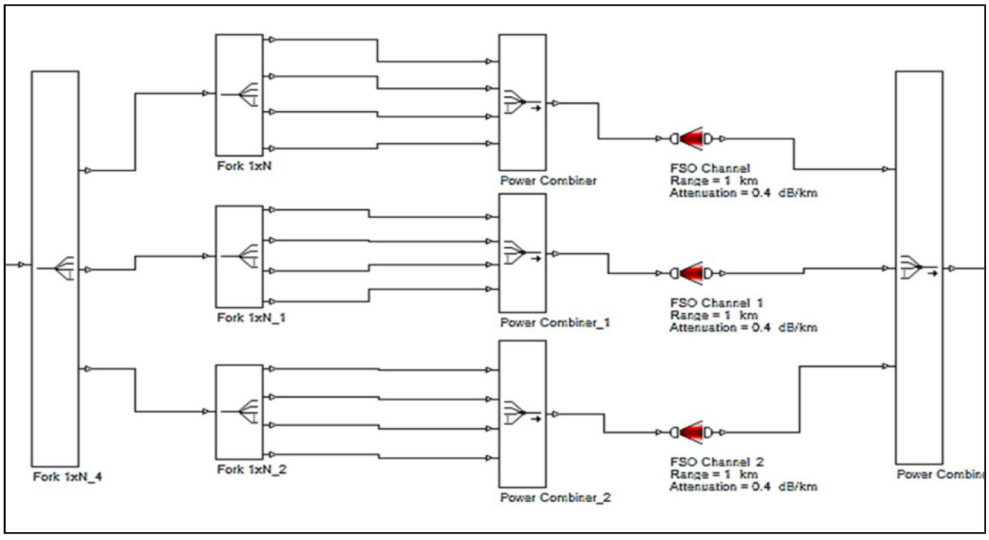

Fig. 3. The FSO channel design.

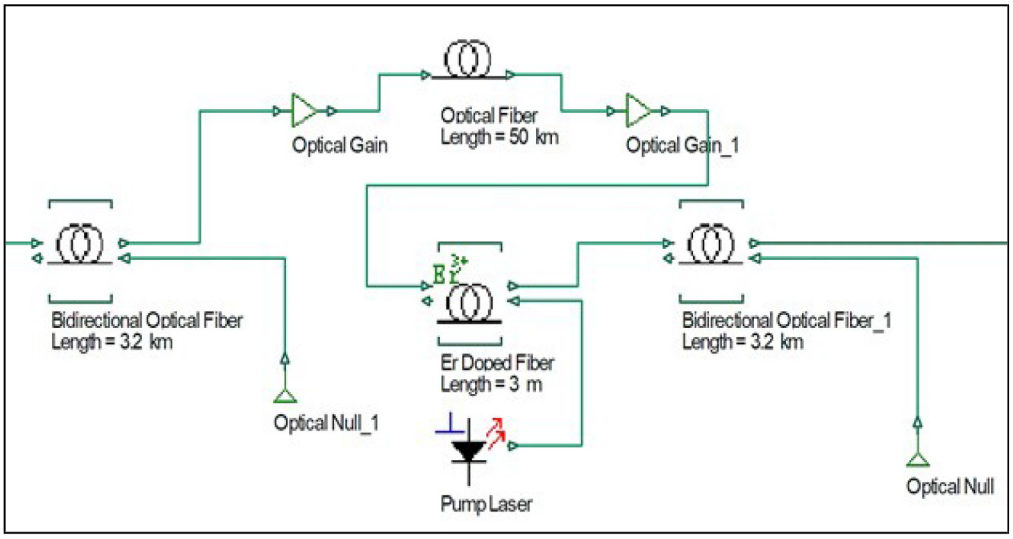

Fig. 4. The fiber optic channel design.

amplifiers to enhance the electrical signal received by a photodetector. As shown in Fig. 5.

2.4.1. Fiber bragg grating (FBG)

FBG is extensively utilized in various forms of communication, encompassing both wireless and cable technologies, as well as in wavelength division. It has the ability to offset the effects of dispersion. Furthermore, UFBG is widely regarded as one of the most effective reflectors utilized in several technologies, including the simultaneous equalization of Erbium amplifier gain.

2.4.2. Visible light communicator

The whole transmitter zone is covered by LEDs with a half-angle transmitter of around 60°. LEDs outperform incandescent and fluorescent lights in energy efficiency due to their low power consumption and high brightness.

2.4.3. LOS channel

LEDs emit a beam of light that travels directly from the source to the receiver, which is a photodiode (PD).

2.5. The receiver side

The receiver comprises a photodetector, a DC block to prevent the entry of DC voltage into the electrical input signal, and a low-pass cosine roll-off filter to eliminate interference. Fig. 6 depicts the configuration on the receiver side. There are a combined total of 16 end customers distributed throughout 4 rooms.

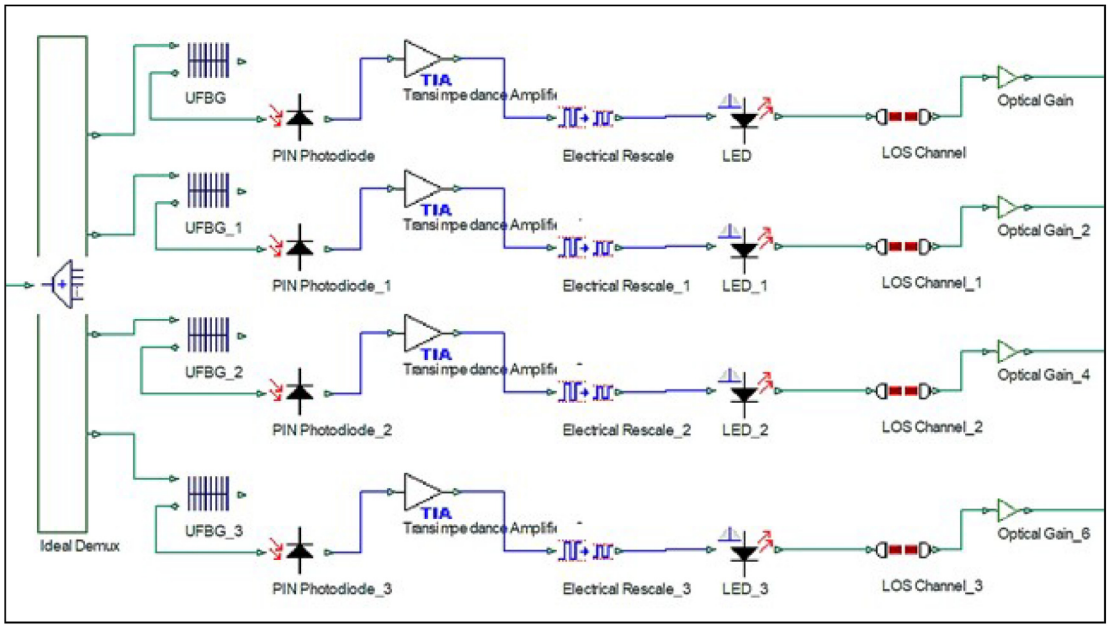

Fig. 5. The Li-Fi channels design.

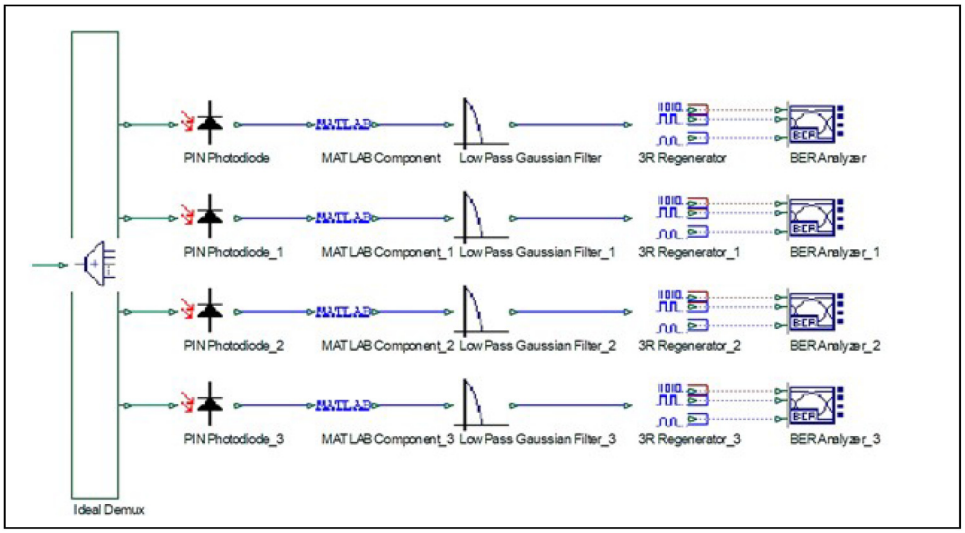

Fig. 6. The receiver side design.

3. Hybird algorithm

Cryptography is a discipline that applies mathematical principles to ensure the security of information, namely by protecting secrecy, data integrity, and authentication. Two methods of encryption have been used, the first is symmetric, represented by the chacha20 algorithm, and the second is asymmetric, which is RSA. Fig. 7 shows Encryption and Decryption Hybrid Algorithm adopted in the proposed design.

3.1. Chacha20

The ChaCha20 cipher functions by transforming a comparatively tiny confidential key, referred to as ks, which is shared between the sender and receiver, into a sequence of characters known as a keystream KS. Keystream is a term that denotes a substantial binary number that can be partitioned into multiple smaller binary numbers, denoted as k, which are employed in the encryption and decryption procedures. The term “encryption keys” refers to these lower quantities.

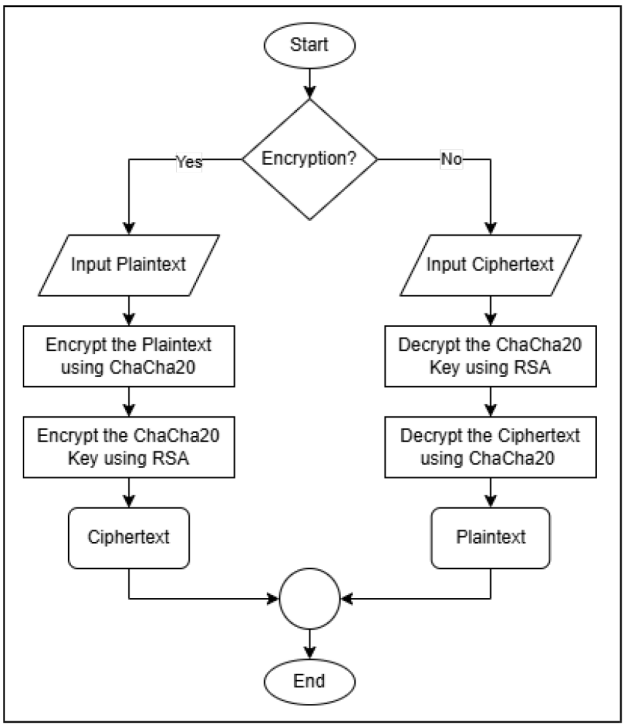

Fig. 7. Encryption and decryption hybrid algorithm.

Particularly, the ChaCha20 cipher utilizes a secret key ks with 256 bits and 96 additional bits, termed nonce, denoted as η, where η cannot be repeated after producing a keystream KS, i.e., the nonce must be updated all the time a new keystream is generated. Furthermore, in most cases, η is a randomly or pseudo-randomly generated number, in contrast to the secret key ks which is deliberately selected. The key size used is 256. It was employed in the encryption of the first plaintext.

How ChaCha20 Works:

1. **Key and Counter Setup:** ChaCha20 relies on a 256-bit secret key, along with a 64-bit nonce (number used once), and a 64-bit block counter.
2. **Initial Matrix:** It forms an initial matrix consisting of 16 words (32 bits each) arranged as follows:
   - Four constant words that are the same for all encryptions.
   - Eight words from the 256-bit secret key.
   - Two words from the 64-bit nonce.
   - Two words from the 64-bit block counter.
3. **Rounds of Operations:** The matrix undergoes a number of rounds, typically 20. Each round includes operations such as rotation, addition, and XOR which modify the values in the matrix.
4. **Generating Output Block:** After completing all rounds, a new matrix is produced. This matrix is then used to generate an output block which is XORed with the original data to create encrypted data.
5. **Encryption/Decryption:** For textual data, the encryption process involves XORing each data block with the output block from ChaCha20. Decryption is done by XORing the encrypted data with the same output block to retrieve the original data.

This process provides high security and fast encryption/decryption, making ChaCha20 suitable for environments requiring strong performance and security.

3.2. RSA

The RSA algorithm with 4096 key size is a commonly employed asymmetric key encryption method. The algorithm is designated with names derived from the monikers of the developers. The RSA algorithm employs the discrete logarithm method for its implementation. In our research, we utilized the RSA method to ensure the security of the content. Due to the complex nature of the RSA algorithm, which relies on discrete logarithms, it is challenging to use in various real-world information security applications. However, we have chosen to utilize this algorithm for our information security purposes. The method can be utilized to attain both security and authenticity of information. Public key encryption solutions are mostly employed for the purpose of safeguarding data during the process of communication. RSA is a cryptographic algorithm that employs a set of asymmetric keys, consisting of a public key and a private key. Therefore, the message is encoded by the sender using the public key and decoded by the recipient using the receiver's private key. The RSA technique is employed due of the primary challenge of factorizing huge integers. Security is attained through the multiplication of two substantial prime numbers throughout the execution of the method. The production of the public key and the private key is the most intricate aspect of RSA encryption. Rabin-Miller's prime number testing method creates two prime numbers, p and q. Each of the two prime numbers connects the private key to the public key. Usually, bits are used to talk about the size of the key. The chacha20 key was encrypted there.

Steps of RSA Algorithm

- **Key Generation**:

  Initial step: Pick two prime numbers, p and q.

  The next thing we need to do is find n, which is the modulus for both the public and private keys. The key length, which is usually given in bits, is a way to measure how big it is.

We need to figure out Euler's totient ϕ (n). ϕ is Euler's totient function in this case. This rate is not shared.

The next step is to choose a number e such that e $<$ ϕ (n) and gcd (e, ϕ (n)) $= 1$.

Next, we can use the equation d $\equiv$ e $-$ 1 (mod ϕ(n)) to find d's value. Here, d is the modular inverse of e modulo ϕ(n).

The operation is carried out by finding d, which is shown by d $\cdot$ e $\equiv$ 1 (mod ϕ (n)). We use the expanded Euclidean method to figure this out.

People use the fake code from the section on modular numbers, where a and n stand for e and ϕ, respectively. Discover the secret key d.

- The value of n and e are used in the public key. The number of the private key is n and d, and it is kept hidden. The numbers of p, q, and ϕ(n) are kept secret because they can be used to figure out d.
- **Encryption:**

  Sender encrypts message m using receiver's public key (e, n):

  The congruence c $\equiv$ me (mod n) is true when, in this context, the variables c, m, e, and d represent the encrypted text, plain text, public key, and private key, respectively.
- **Decryption:**

  The recipient decrypts the cipher text c using their private key (d, n) by using the equation m $\equiv$ cn (mod n), where c represents the cipher text, m represents the plain text, e represents the public key, and d represents the private key. Decryption of communications

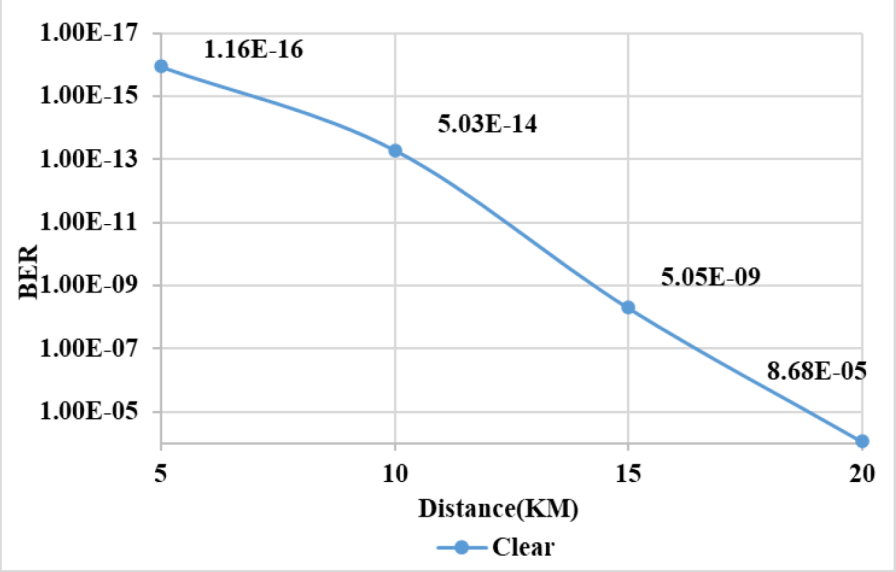

Fig. 7A. BER in different distance in clear weather.

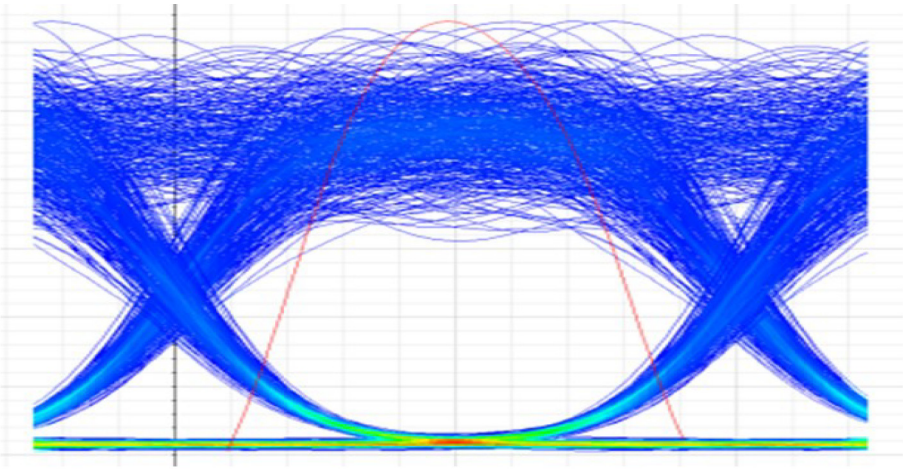

Fig. 7B. Eye diagram in clear weather.

encrypted with the matching public key is only possible for the specified private key holder. Asymmetric encryption and decryption, which relies on mathematically linked key pairs, avoids the requirement of discreetly exchanging a common key, as is essential with symmetric ciphers.

4. Result and discussion

The Optisystem V21 and MATLAB R2020a execution environment on a Lenovo ThinkPad running Windows 11 64-bit, an Intel(R) Core (TM) i7-7500U 2.70GHz/2.90GHz processor and 16 GB of RAM, was used to build the proposed system based on Li-Fi in the communication system and link it with MATLAB to implement a hybrid algorithm to encrypt the data.

4.1. Communication system

The Li-Fi communication system was validated by calculating the bit error rate and eye diagram of the system. The results show that the communication system is successful and achieves satisfactory performance at different distance, as shown in Figs. 7A and 7B. Fig. 7A shows the relationship between the bit error rate and the distance and shows the working status of the system at different distances in clear air, while Fig. 7B shows the stability of the system by drawing an eye diagram.

Table 1. The Wavelength have been entered in the CW lasers.

CW lasers	entered Wavelength (nm)
1	1550 nm
2	1555 nm

Table 2. The Wavelength has been entered in the UFBG.

UFBG	entered Wavelength (nm)
1	1550 nm
2	1545 nm

In the suggested system that examined the particular UFBG Properties of the for the frequencies entering the CW laser, where the frequency testing had been performed programmed distinct frequencies into four CW lasers as introduced in the Table 1, UFBG may be used as either a band-reject or a band-pass filter To increase the percentage of information security as shown in Figs. 8A and 8B. In Fig. 8A, the graph of the optisystem program shows that the system is working and the network is stable, while Fig. 8B shows that the signal is scattered and there is no signal, which proves that the UFBG filter is working as it has passed the allowed band and prevented other bands from passing through the network.

On the other hand, the following frequencies has been entered in the UFBG, as introduced in the Table 2.

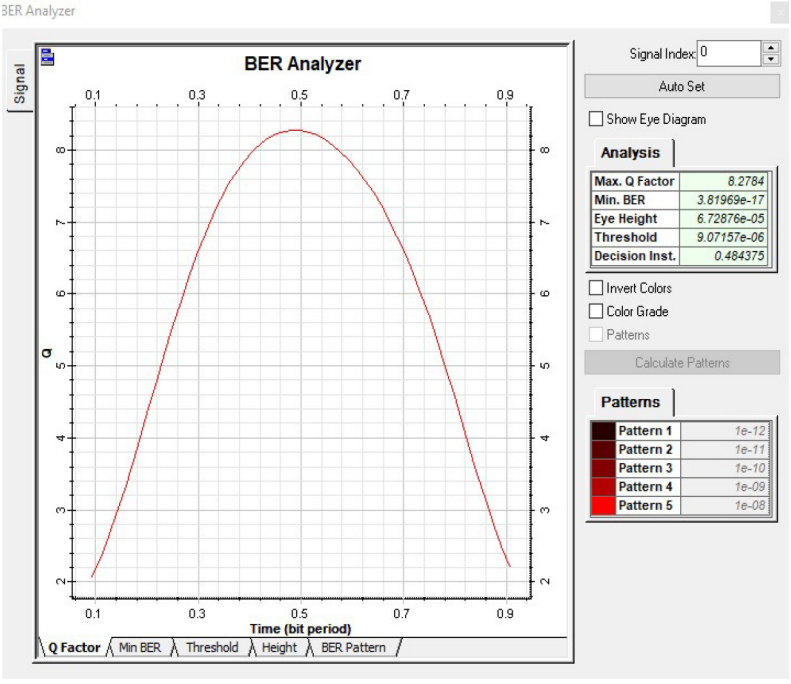

Fig. 8A. Eye diagram in the band-pass filter, at a frequency of 1550 nm.

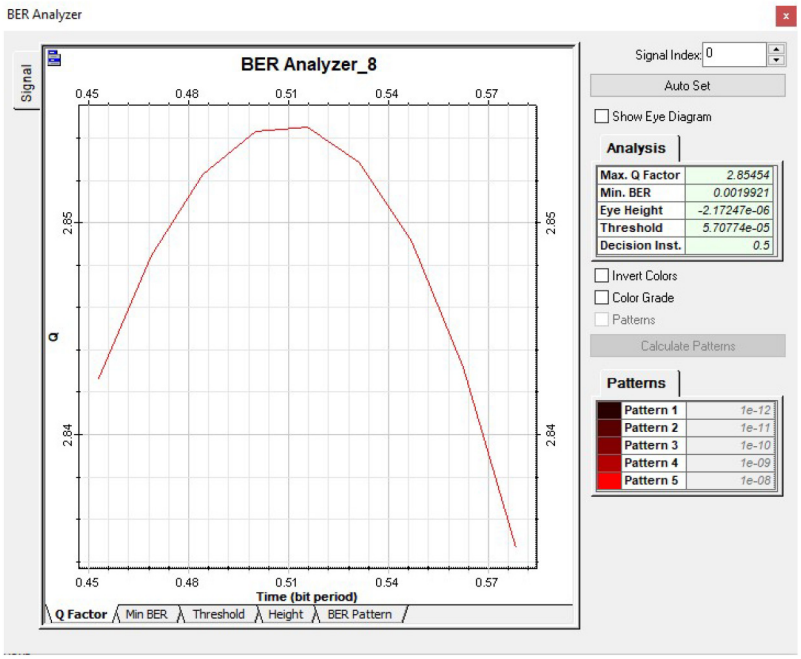

Fig. 8B. Eye diagram in the band-reject filter, at a frequency of 1545 nm.

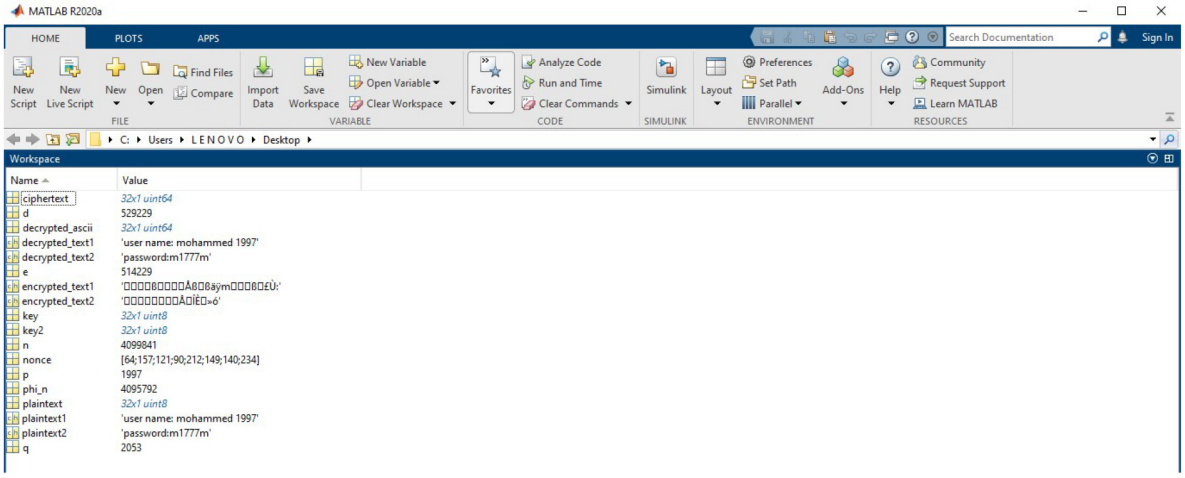

Fig. 9. Variables used in the hybrid algorithm by MATLAB.

Fig. 10. Data encryption and decryption using the proposed algorithm.

4.2. Hybrid algorithm

At the sending end, the text is encrypted by the chacha20 algorithm using the secure key, then its key is encrypted by the RSA algorithm using the public key. At the receiving end, the chacha20 secure key is decrypted using the RSA private key, then the message is decrypted with the chacha20 secure key, as

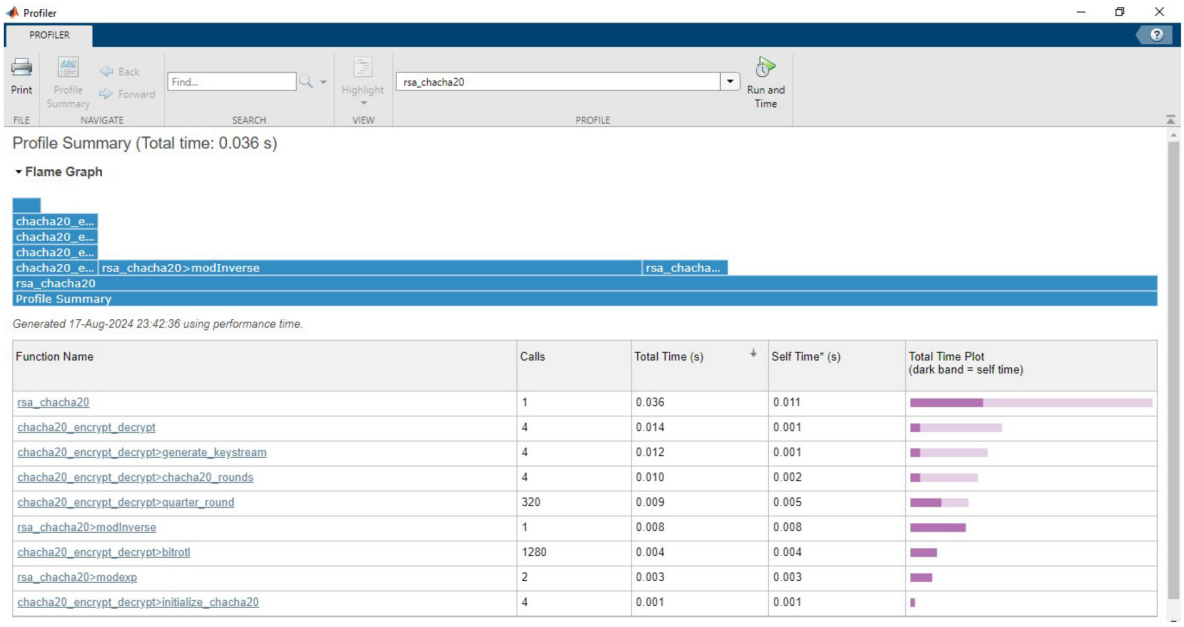

Fig. 11. Execution time for encryption and decryption in hybrid algorithm in MATLAB.

Table 3. The execution time of hybrid algorithm for encryption and decryption.

Function Name	Number of call	Total Time
Hybrid Algorithm	1	0.036 sec
ChaCha20 Encryption & Decription	4	0.014 sec
ChaCha20 generate key stream	4	0.012 sec
ChaCha20 Rounds	4	0.010 sec
ChaCha20 quarter rounds	320	0.009 sec
RSA generate private key	1	0.008 sec
ChaCha20 Bit Rotation	1280	0.004 sec
RSA generate public key	2	0.003 sec
ChaCha20 Inetialization	4	0.001 sec
Total execution time of Hybrid Algorithm to enecription and decription data = 0.036 sec		

shown in the Fig. 9, which shows the variables and functions used in the system.

The Fig. 10 shows the encryption and decryption of data sent through the Li-Fi suggested system

The time taken to execute the hybrid algorithm in MATLAB is calculated as shown in Fig. 11. The time for the operations is calculated as shown in Table 3.

5. Conclusion

In conclusion, this study presents a secure Li-Fi technology for data transmission and messaging between network users. It addresses the network vulnerabilities that hackers exploit to steal and manipulate information. The Li-Fi communication system was validated by calculating the bit error rate and Q factor of the system. The results show that the communication system is successful and achieves satisfactory performance, with a bit error rate of (3.25*e-17) and a Q factor of (8.275). The data was encrypted using chacha20, which ensures security and speed in encryption, while the RSA algorithm was used to encrypt the key used in the chacha20 algorithm to ensure additional security of the system. The execution time was reduced to 0.03 sec. The keys were generated randomly in all encryption and decryption operations in the ChaCha20 and RSA algorithms. The results presented demonstrate our contribution to enhancing the security of the proposed system.

References

1. S. Agrawal, F. Kitagawa, and R. Nishimaki, “Public key encryption with secure key leasing,” pp. 1–68, 2023, doi:10.1007/978-3-031-30545-0_20.
2. A. Atadoga, O. A. Farayola, and B. S. Ayinla, “A comparative review of data encryption,” vol. 5, no. 2, pp. 447–460, 2024, doi:10.51594/csitrj.v5i2.815.

3. S. Murthy, “Ciphertext-only attack on a secure k-NN computation on cloud,” doi:10.48550/arXiv.2403.09080.
4. K. S. Babu, K. B. Raja, K. K. Kiran, T. H. Manjula Devi, K. R. Venugopal, and L. M. Patnaik, “Authentication of secret information in image Steganography,” in *TENCON 2008 - 2008 IEEE Region 10 Conference*, IEEE, Nov. 2008, pp. 1–6. doi:10.1109/TENCON.2008.4766581.
5. K. M. Hosny, S. Member, M. A. Zaki, and N. A. Lashin, “Multimedia security using encryption: A survey,” *IEEE Access*, vol. 11, no. June, pp. 63027–63056, 2023, doi:10.1109/ACCESS.2023.3287858.
6. M. Alzenad, M. Z. Shakir, H. Yanikomeroglu, M. Alouini, and N. I. May, “FSO-based vertical backhaul /fronthaul framework for 5G + wireless networks,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 218–224, doi:10.1109/mcom.2017.1600735.
7. B. Bag, A. Das, I. S. Ansari, A. Prokes, C. Bose, and A. Chandra, “Performance analysis of hybrid FSO systems using FSO/RF-FSO link adaptation,” *IEEE Photonics J.*, vol. 10, no. 3, pp. 1–17, Jun. 2018, doi:10.1109/JPHOT.2018.2837356.
8. G. Tu, “The security in optical wireless communication: A survey,” vol. 55, no. 14, 2023, doi:10.1145/3594718.
9. A. A. Ali *et al.*, “Audio streaming using Li-Fi communication,” vol. 7, no. 1, pp. 1–7, 2023, doi:10.46759/IIJSR.2023.7101.
10. C. Kaur and M. K. Dubey, “An overview of secure Li-Fi and Wi-Fi hybrid network,” pp. 677–688, doi:10.56155/978-81-955020-2-8-60.
11. M. M. Msallam and R. Samet, “A review of security methods in light fidelity technology a review of security methods in light fidelity technology,” no. July, 2024, doi:10.46604/peti.2024.13149.
12. “Failures of secret-key cryptography,” [Online]. Available: https://cr.yp.to/talks/2013.11.29/slides-djb-20131129-a4.pdf.
13. H. H. Alyas and A. A. Abdullah, “Enhancement the ChaCha20 encryption algorithm based on chaotic maps enhancement the ChaCha20 encryption algorithm based on chaotic maps,” no. October, 2021, doi:10.1007/978-981-16-0666-3.
14. S. V. D. Kumar, S. Patranabis, J. Breier, D. Mukhopadhyay, and S. Bhasin, “A practical fault attack on ARX-like ciphers with a case study on ChaCha20,” doi:10.1109/fdtc.2017.14.
15. F. De Santis, A. Schauer, and G. Sigl, “ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications,” pp. 692–697, 2017, doi:10.23919/date.2017.7927078.
16. “ChaCha20 and Poly1305 for IETF protocols,” [Online]. Available: https://www.rfc-editor.org/rfc/rfc8439.
17. V. R. Kebande, “Extended-ChaCha20 stream cipher with enhanced quarter round function,” *IEEE Access*, vol. 11, no. October, pp. 114220–114237, 2023, doi:10.1109/ACCESS.2023.3324612.
18. S. Pinto, “SS symmetry an improved public key cryptographic algorithm based on chebyshev polynomials and RSA,” 2024, doi:10.3390/sym16030263.
19. A. Smartphones, R. Apau, and C. Adomako, “Design of image steganography based on RSA algorithm and LSB insertion for android smartphones,” no. April, 2017, doi:10.5120/ijca2017913557.
20. H. Rasmita, A. Anand, S. Hendra, and A. Ahmad, “E-surveillance system security using RSA-AES algorithm (rivest shamir adleman - advanced encryption standard),” vol. 5, no. 1, pp. 22–32, 2024, doi:10.22487/sciencetech.v5i1.17175.
21. Y. Ramadhan, S. Suhardi, and Y. Aditama, “Data security using low bit encoding algorithm and RSA algorithm,” *J. Mantik*, vol. 8, no. 1, 2024, doi:10.35335/mantik.v8i1.4945.
22. S. Arifin, “Application of unimodular hill cipher and RSA methods to text encryption application of unimodular hill cipher and RSA methods to text encryption algorithms using python,” no. March, 2024, doi:10.3844/jcssp.2024.548.563.