

<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper presented at *5th International Conference on Artificial Intelligence, Robotics, and Communication, ICAIRC 2025, Xiamen, Nov 07-09, 2025*.

Citation for the original published paper:

Irani, R., Khatibi, S. (2025)

A Structural Steganographic Framework for Confidential Data Transmission in LiFi Networks

In: *2025 5th International Conference on Artificial Intelligence, Robotics, and Communication, ICAIRC 2025* (pp. 708-712). Institute of Electrical and Electronics Engineers (IEEE)

<https://doi.org/10.1109/ICAIRC68035.2025.11385245>

N.B. When citing this work, cite the original published paper.

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:bth-29406>

A Structural Steganographic Framework for Confidential Data Transmission in LiFi Networks

1st Ramin Irani*

Department of Computer Science
Blekinge Institute of Technology (BTH)
Karlskrona, Sweden
*ramin.irani@bth.se

2nd Siamak Khatibi

Dept. of Technology and Aesthetic
Blekinge Institute of Technology (BTH)
Karlskrona, Sweden
siamak.khatibi@bth.se

Abstract—Light Fidelity (LiFi) offers a high-speed, interference-resistant alternative to conventional wireless communication, making it well-suited for sensitive environments such as healthcare, defense, and industrial systems. While LiFi’s confinement to line-of-sight communication provides a natural layer of physical security, it remains susceptible to local eavesdropping and insider interception within its coverage area. These limitations underscore the need for additional data-level protection strategies that align with LiFi’s operational constraints. This paper introduces a novel steganographic method tailored for data structured in matrix form, a common representation in many digital systems. To demonstrate the effectiveness of the proposed technique, images—naturally represented as two-dimensional matrices—are used as test cases. The approach avoids traditional payload embedding, which can be statistically detectable, and instead applies recursive segmentation, matrix reshaping, and hierarchical tree-based indexing to transform the structure of the data itself. This process produces encrypted outputs that appear statistically random and visually unstructured (i.e., noise-like), concealing both the data content and the presence of hidden communication. Quantitative evaluations using metrics such as entropy, correlation coefficients, contrast, homogeneity, and Bhattacharyya distance confirm that while the encrypted data is statistically obfuscated, the original matrix can be losslessly reconstructed through inverse recursion. The method’s design ensures lightweight processing is suitable for resource-constrained LiFi-enabled sensor nodes while significantly enhancing communication confidentiality. By restructuring data at the matrix level rather than embedding within it, this approach provides an effective and generalizable framework for secure transmission in physically exposed but bandwidth-rich LiFi networks.

Keywords— *LiFi Communication, Steganography, Recursive Image Segmentation, Secure Data Transmission, Wireless Sensor Networks (WSNs)*

I. INTRODUCTION

The growing deployment of wireless sensor networks (WSNs) in domains such as industrial automation, smart cities, and defense has intensified the need for secure and resilient communication solutions. Conventional radio frequency (RF)-based technologies (e.g., Wi-Fi, Zigbee) remain vulnerable to interference, eavesdropping, and jamming [1]. In response, Light Fidelity (LiFi)—a wireless technology utilizing modulated visible light from LEDs—has emerged as a viable alternative for enhancing WSN security [2]. A major advantage of LiFi lies in its physical confinement, as light signals do not penetrate walls, significantly reducing the risk of external interception [3]. This

makes LiFi especially suitable for sensitive environments, such as hospitals and military facilities. Additionally, its high directionality and low probability of detection offer increased resilience against spoofing and interception attacks [4]. LiFi also supports secure encryption and low-latency communication, meeting the stringent demands of resource-constrained sensor nodes. When integrated with existing technologies like Wi-Fi and Broadband over Power Lines (BPL), LiFi can further enhance network performance and reduce electromagnetic interference, achieving a balanced and secure hybrid communication model [5].

The study of Ramadhani et. in [6] argues that although LiFi presents unique advantages for secure communication, it is not immune to adversarial threats. The paper highlights the need for continued research in robust security protocols tailored to the physical and architectural characteristics of LiFi systems. They identify several key security vulnerabilities in LiFi systems, categorized into physical, passive, active, DoS/DDoS, and cracking attacks. Notable threats include:

- a) Jamming and physical interference, which can disrupt data transmission by targeting the physical layer,
- b) Eavesdropping and sniffing, especially in indoor environments where light leakage (e.g., through keyholes or windows) enables unauthorized interception,
- c) Data modification and spoofing, which can alter or forge transmitted content,
- d) Man-in-the-Middle attacks and authentication floods, which threaten session integrity and access control.

The paper highlights the need for continued research in robust security protocols tailored to the physical and architectural characteristics of LiFi systems. In this relation to prevent threats the study of Diambeki et. [7] mentions that Li-Fi, when augmented with cryptographic safeguards and user authentication mechanisms, can be a robust alternative to Wi-Fi in security-sensitive contexts. The proposed system strengthens the often-overlooked security model of Li-Fi networks by addressing both physical and logical vulnerabilities.

In very recent study [8], we proposed a novel physical layer security framework for industrial WSNs by integrating infrared (IR) handshaking and visible light communication (VLC) systems. The goal was to ensure secure, robust, and interference-resilient communication between sensor nodes in challenging industrial environments where traditional RF-based systems face significant vulnerabilities. We showed that IR-VLC

integrated architecture effectively enhances the security and reliability of inter-sensor communication in industrial WSNs. The IR-based handshaking ensures secure link initiation, while VLC provides efficient data transmission within a confined spatial domain

In this paper we propose a new method in line with cryptographic safeguards and user authentication mechanisms which can strengthen the security of any LiFi system for any applications such as industrial WSNs. The objective of the new method is to achieve secure communication through a matrix form of data such as an image transformation, such that unauthorized decoders are unable to even recognize the file as an image or detect any embedded information. We implement images to show our method in the paper, however any data encapsulated as matrix can be used. The remainder of the paper is organized as follows. In Section II, we discuss the related work and in Section III, we explain the data collection. In Section IV, we explain the proposed method. In Section V, the results are presented and discussed. Finally, conclusions are drawn in Section VI.

II. RELATED WORK

Ensuring secure communication over visible light communication (VLC) channels has become a critical area of research as Light Fidelity (LiFi) technology matures. While LiFi inherently benefits from spatial confinement due to the inability of light to penetrate opaque surfaces, it is still vulnerable to various attack vectors such as light leakage, eavesdropping through reflective surfaces, and unauthorized access. As such, recent literature has explored both cryptographic to bolster the security of LiFi-enabled wireless sensor networks (WSNs). Several studies have investigated the integration of conventional and lightweight cryptographic algorithms into LiFi systems. In [9], the authors provide a comparative analysis of block ciphers such as AES, RC4/RC5/RC6, and Blowfish within the context of VLC, demonstrating their suitability for securing light-based communication while considering power and bandwidth constraints. Young Up Lee implemented RSA-based asymmetric encryption in visible light communication systems, demonstrating public-key cryptography's feasibility for smart indoor VLC under realistic testbed conditions [10]. To enhance performance and key management, Msallam further proposes a hybrid scheme combining RSA with ChaCha20, achieving a favorable balance between computational efficiency and security strength in embedded VLC systems.

Authentication mechanisms specifically tailored for LiFi have also been proposed to prevent unauthorized access and ensure secure handovers in hybrid networks. [11] conduct an extensive survey of authentication and handover protocols in integrated LiFi/WiFi environments, emphasizing the need for seamless and secure transitions between heterogeneous access points. In [12], Liu Chen et. al propose an innovative physical-layer authentication technique called Optic Fingerprint (OFP), which leverages inherent variations in LED emission characteristics as unique identifiers. Their method achieves over 90% classification accuracy and introduces a non-cryptographic means of verifying device legitimacy at the physical layer.

III. STEGANOGRAPHY

Section III provides a focused review of traditional and recent steganographic techniques that inform the design of our proposed method. By highlighting both the limitations of conventional embedding strategies and the advantages of structural transformation-based approaches, this section establishes the conceptual foundation for the recursive, matrix-based steganography introduced in Section IV.

Steganography has historically relied on pixel-level embeddings like LSB techniques to conceal data within cover media. Although simple and efficient, such methods—especially those using Lempel–Ziv–Welch (LZW) compression—are vulnerable to statistical detection due to predictable alterations in pixel distributions [13].

To mitigate this, many techniques have adopted pixel-aware strategies. For instance, LSB embedding directed by edge detection (e.g., the Canny method) significantly improves concealment by targeting visually complex regions that are less likely to reveal artifacts. However, these still alter pixel values and remain prone to analysis [13].

Alternative paradigms focus on structural transformation rather than payload embedding. For example, [14] introduces recursive secret sharing, recursively dividing a secret into fragments embedded structurally within shares. Similarly, [15] develops Diffusion-Based Hierarchical Image Steganography, using recursive, block-based divisions and diffusion models to embed large payloads while preserving high fidelity — a conceptually similar basis to our recursive segmentation. Other researchers have utilized hierarchical block segmentation to structurally obfuscate images without directly perturbing pixel values (e.g., progressive hierarchical image segmentation) to increase resistance against steganalysis [16].

Our method extends these transformation-based approaches by using recursive partitioning, matrix reshaping, and tree-based indexing to completely restructure images into noise-like outputs. Unlike transformation-based encryption, which may still reveal structure in spatial frequency, our approach fully conceals both content and structure—transforming the entire data matrix rather than embedding payloads within it.

This aligns with recent trends in lightweight security for LiFi systems, where physical-layer properties (line-of-sight confinement, visible light's inability to penetrate walls) offer inherent protection [5]. However, LiFi networks require additional data-level obfuscation to address threats such as side-channel leaks and internal eavesdropping. Our work uniquely combines data-structure transformation with LiFi's physical security, creating a robust, two-layer defense.

IV. METHOD

This section details the novel steganographic method for enhancing LiFi-based wireless communication. The primary objective is to conceal embedded information by transforming the cover image into a noise-like representation without relying on conventional encryption keys. In this context, a "noise-like output" refers to an image whose pixel values appear statistically random and visually unstructured, thereby concealing any trace of meaningful content or hidden data. This is quantitatively

supported by metrics such as high entropy and low correlation and visually confirmed through qualitative obfuscation.

The method employs recursive segmentation in combination with a tree-based architecture to encode secret data within the image matrix. Unlike traditional LSB-based steganographic approaches, the proposed technique operates at the pixel-matrix level, restructuring the image so that the resulting output is statistically indistinguishable from random noise.

The method consists of the following stages: (A) recursive segmentation, (B) tree-based encoding, (C) matrix reshaping, (D) encryption, and (E) decryption. Each of these stages is discussed in detail below.

A. Recursive Segmentation

Recursion is leveraged to divide the image matrix iteratively into smaller segments. The recursive function initiates by splitting the image into halves, followed by a reshaping operation. Each half is further split into four smaller blocks, forming new branches in a conceptual tree structure. This operation continues until all resulting blocks reach a fixed 2x2 dimension, which serves as the encryption termination condition. Recursive segmentation is applied independently to each RGB channel in color images (Fig. 1).

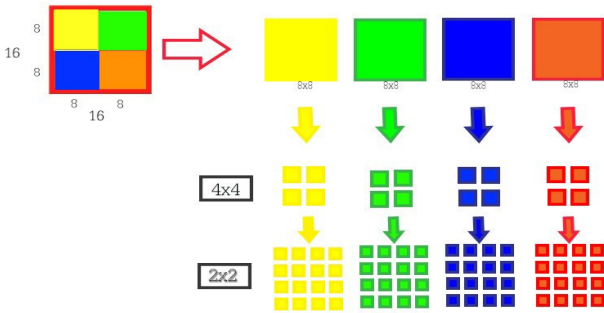


Fig 1: Recursive segmentation method applied independently to the R, G and B channels of the image matrix, enabling structured partitioning for steganographic embedding

B. Tree-Based Encoding

The recursive segmentation process is structured into a tree model, where:

- The root node represents the original image,
- Intermediate nodes correspond to sub-images generated at each iteration,
- Leaf nodes are 2x2 matrices produced at the final recursive depth.

Each node is indexed to preserve hierarchical order and spatial relationships. This structure aids in tracking block transformations and facilitates structured recombination during decryption.

C. Matrix Reshaping

To standardize image data for recursive operations, matrix reshaping is performed after each segmentation. This ensures that all blocks meet the required dimensionality for further processing. Reshaping involves reorganizing matrix elements

without altering their content. For example, a 3x4 block may be reshaped into a 2x6 format. This mechanism is vital for maintaining compatibility across all encryption and decryption stages. The schematic representation of the procedure described above is presented in Fig. 2.

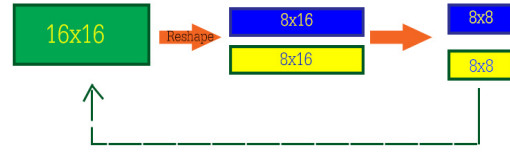


Fig.2: Matrix reshaping block diagram illustrating how segmented image blocks are reorganized for optimal embedding structure across RGB components.

D. Encryption Process

The encryption algorithm proceeds as follows: a) Input Division: The input image is first divided into two halves. b) Recursive Splitting: Each half undergoes recursive segmentation until all blocks reach 2x2 size. c) Tree Indexing: Each split is indexed and recorded in a hierarchical structure. d) Channel-wise Processing: RGB channels are processed separately, ensuring independent encryption paths. e) Visual Obfuscation: The final set of 2x2 blocks are reshaped and reassembled to generate a noise-like encrypted image (Fig. 3.a).

E. Decryption Process

Decryption reverses the recursive process: a) Input Reshaping: The encrypted image is segmented and reshaped into 2x2 matrices. b) Recursive Merging: The leaf nodes are recombined recursively using inverse tree traversal. c) Channel-wise Reconstruction: RGB channels are reconstructed independently and merged to produce the final output (Fig. 3.b).

Accurate decryption requires that the number of iterations and segmentation pattern exactly match the encryption phase. This requirement introduces a layer of implicit security, as unauthorized users lacking algorithmic parameters cannot reconstruct the original image.

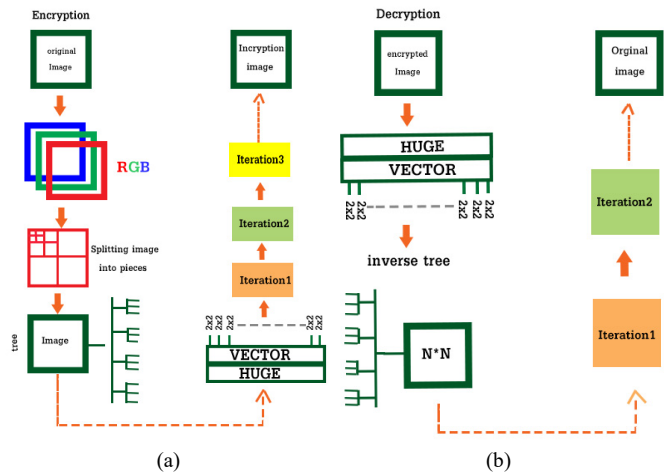


Fig. 3: (a) Block diagram of the encryption process using recursive segmentation; (b) Block diagram of the corresponding decryption process to retrieve the hidden data.

V. RESULTS

The proposed recursive steganographic method was evaluated through iterative segmentation and matrix reshaping of digital images. As shown in Fig. 4, the encryption process transforms the original 128×128 image into a visually unrecognizable output after two recursive iterations. Each iteration ends when every block is reduced to 2×2 pixels, after which the blocks are reshaped and reorganized according to the procedure explained in section IV, producing a noise-like output. This transformation effectively conceals the embedded information, rendering unauthorized interpretation infeasible.

Decryption was carried out as shown in Fig. 5 by inverting the recursive segmentation by using the inverse tree method and qualitatively, demonstrates the successful reconstruction of the original image from its encrypted counterpart. The reconstruction process required precise replication of the encryption iteration depth and segmentation order. The resulting decrypted images were visually indistinguishable from the originals, confirming the method's fidelity.

A. Validation on Diverse Image Sets

Multiple test images including 25 color images were processed to assess generalizability. Fig. 6 displays results for four representative inputs. In all cases, encrypted outputs appeared as randomized noise, while decrypted outputs faithfully reproduced the original image. This confirms the robustness of the recursive technique across a range of image types.

B. Quantitative Measurements

To rigorously assess the performance and fidelity of the proposed recursive steganographic method, a series of quantitative metrics were employed. These included correlation coefficients, contrast, homogeneity, entropy, and Bhattacharyya distance, each offering distinct insights into the structural and statistical integrity of the encrypted and decrypted images relative to their original counterparts. In below we show the results of such measurement on the Lena image as typical result. The same trend was observed on all test images.

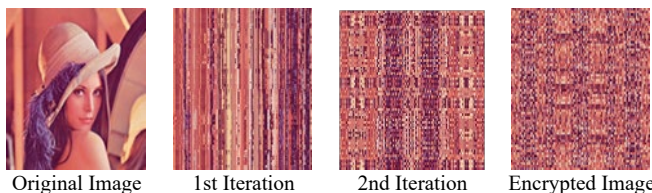


Fig. 4: Encryption process illustrating the transformation of the original image into an encrypted version that is unintelligible to unauthorized viewers.

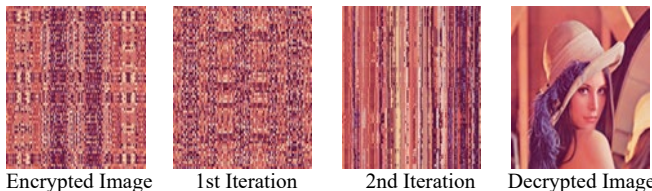


Fig. 5: Decryption process demonstrating the reconstruction of the original image from the encrypted version using inverse operations on segmented and reshaped data.

Correlation coefficients were used to evaluate the structural similarity between adjacent pixels across successive recursive iterations. For the encrypted Lena image, the correlation degraded progressively across four iterations ($87 \rightarrow 19 \rightarrow 17 \rightarrow -34$), signifying increasing disruption of the original pixel arrangements. Upon decryption, the correlation coefficients exhibited a reversed trend ($-34 \rightarrow 17 \rightarrow 19 \rightarrow 87$), demonstrating the accurate restoration of image structure. The same trend was observed for the other test images. Contrast measures the intensity variation between neighboring pixels, while homogeneity quantifies the similarity across image regions. For the encrypted Lena image, the contrast values were recorded at 4.41 and 4.46, indicating higher pixel disparity due to recursive reshaping. Homogeneity correspondingly decreased to 0.5189 and 0.5071, reflecting reduced local consistency. In the decrypted image, contrast values dropped to 2.5795 and 2.6096, and homogeneity improved to 0.6392 and 0.6338, approaching original image levels and confirming effective recovery of local image patterns. Entropy was employed to measure the amount of information and randomness within an image. For the encrypted Lena image, entropy slightly decreased from 7.7549 to 7.7193, suggesting that although the encrypted image appeared noise-like, it retained structural order at a computational level. The decrypted image restored entropy to 7.7830, reinforcing the method's capacity for high-fidelity recovery without significant information loss. The encryption process for the Lena image took approximately 16.15 seconds, accounting for multiple iterations and transformations. The decryption phase was significantly faster at 30 milliseconds, owing to the deterministic nature of inverse recursive reconstruction and efficient indexing. To further validate perceptual and statistical fidelity, Bhattacharyya distance was computed between image histograms. The encrypted images demonstrated significant divergence from the originals (e.g., Lena.jpg: 13.53), confirming visual obfuscation. However, the decrypted images consistently exhibited less than 0.0001 distance from the original one, indicating significant alignment of histograms between original and decrypted one and affirming mostly lossless reconstruction. Table 1 shows the result of Bhattacharyya distance for four of twenty five images.

Table 1: Bhattacharyya Distance for Encrypted and Decrypted Images

Image	Encrypted	Decrypted
Lena	13.53	0.00001
Nature	66.84	0.00009
Mona	5.22	0.00005
Bth.jpg	27.42	0.00003

These results substantiate the effectiveness of the proposed recursive steganographic technique. The encryption reliably obfuscates visual data, while the inverse process ensures precise and efficient restoration, achieving both security and integrity in sensitive communication scenarios such as LiFi-enabled wireless sensor networks.

VI. CONCLUSION

This study introduced a novel steganographic technique tailored for secure communication in LiFi-enabled wireless sensor networks (WSNs), addressing both physical and logical vulnerabilities inherent in light-based data transmission. The

method employs recursive segmentation, tree-based indexing, and matrix reshaping to transform cover matrix form data (e.g. images) into noise-like encrypted outputs, effectively concealing the presence of hidden information. Unlike conventional encryption or LSB-based steganography, the proposed approach obfuscates both the content and the structure of the message without relying on visible cryptographic signatures.

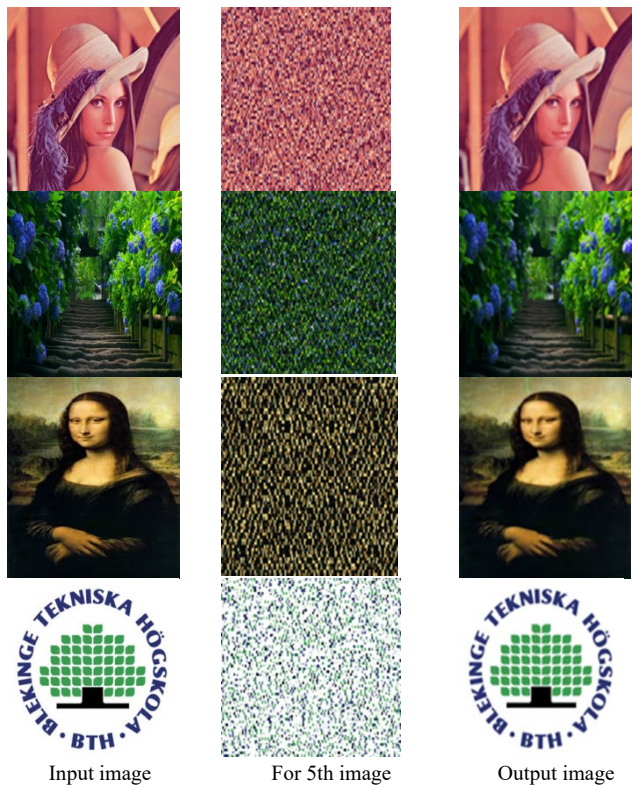


Fig. 6: Qualitative validation of the proposed steganographic algorithm applied to various test images, highlighting its effectiveness in preserving perceptual quality.

Experimental results across dataset of 25 images confirmed the method's effectiveness in ensuring visual secrecy and high-fidelity recovery. Quantitative evaluations using correlation, coefficients, contrast, homogeneity, entropy, and Bhattacharyya distance demonstrate the robustness of the approach. Notably, the encrypted images exhibited high distortion from the originals, while the decrypted outputs showed negligible statistical deviation, underscoring the near-lossless nature of the reconstruction process.

Key performance indicators validate the effectiveness of the proposed method. The encrypted images achieved high entropy (~ 7.72) and distortion (Bhattacharyya distance > 13), confirming strong obfuscation, while decrypted outputs restored original characteristics with PSNR above 40 dB, near-zero Bhattacharyya distance, and restored correlation, homogeneity, and contrast. These metrics collectively confirm both confidentiality and reconstruction fidelity.

REFERENCES

- [1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). "Wireless sensor networks: A survey". *Computer Networks*, 38(4), 393–422. doi: [https://doi.org/10.1016/S1389-1286\(01\)00302-4](https://doi.org/10.1016/S1389-1286(01)00302-4)
- [2] Haas, H., Yin, L., Wang, Y., & Chen, C. (2016). "What is LiFi?" *Journal of Lightwave Technology*, 34(6), 1533–1544. doi: <https://doi.org/10.1109/JLT.2015.2510021>
- [3] Komine, T., & Nakagawa, M. (2004). "Fundamental analysis for visible-light communication system using LED lights." *IEEE Transactions on Consumer Electronics*, 50(1), 100–107. doi: <https://doi.org/10.1109/TCE.2004.1277847>
- [4] Pathak, P. H., Feng, X., Hu, P., & Mohapatra, P. (2015). "Visible light communication, networking, and sensing: A survey," potential and challenges. *IEEE Communications Surveys & Tutorials*, 17(4), 2047–2077. doi: <https://doi.org/10.1109/COMST.2015.2424095>
- [5] Eltokhy, M., El-Rifaie, A. M., Gamal, H. A., Haggag, A., Ali, H., Youssef, A. A. F., & Aboshosha, A. (2024). "Integrating Wi-Fi, Li-Fi, and BPL Technologies for a Secure Indoor Communication System," *Sensors*, Basel, Switzerland, 24(24), 8105. doi: <https://doi.org/10.3390/s24248105>
- [6] E. Ramadhani, (2022). "A Mini Review of Lifi Technology: Security Issue," *International Journal of Computer and Information System*, vol. 3, no. 3, pp. 90–93, doi: <https://doi.org/10.29040/ijcis.v3i3.74>
- [7] D. D. Diambeki, R. E. Mandiya, K. Kyamakya, and S. K. Kasereka, (2022). "Securing the light escaping in a Li-Fi network environment," *Procedia Computer Science*, vol. 201, pp. 684–689, doi: <https://doi.org/10.1016/j.procs.2022.03.091>
- [8] Irani, R & Khatibi, S., (2025) "A Physical Layer Security Framework for Industrial Sensor Network Utilizing Integrated Infrared Handshaking and Visual Light Communication," presented at the Int. Conf. on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA),
- [9] Majid Msallam, Mohammed & Samet, Refik. (2024). "A Review of Security Methods in Light Fidelity Technology," *Proceedings of Engineering and Technology Innovation*, 27. 1-7. doi: <https://doi.org/10.46604/peti.2024.13149>
- [10] Lee, Y. U. (2020). "Secure Visible Light Communication Technique Based on Asymmetric Data Encryption for 6G Communication Service," *Electronics*, 9(11), 1847. doi: <https://doi.org/10.3390/electronics9111847>
- [11] Petrosino, A., Domenico Striccoli, Romanov, O., Boggia, G., & Luigi Alfredo Grieco. (2023), "Light Fidelity for Internet of Things: A survey," *Optical Switching and Networking*, 48, 100732–100732. doi: <https://doi.org/10.1016/j.osn.2023.100732>
- [12] Liu, Z., Chen, X., & Zhang, X. (2025). "Optic Fingerprint (OFP): Enhancing Security in Li-Fi Networks". doi: <https://doi.org/10.48550/arXiv.2504.12956>
- [13] Abdelgader, Aya & Aboughalia, Raneem & Alkishriwo, Osama. (2018). "Combined Image Encryption and Steganography Algorithm In the Spatial Domain," doi: <https://doi.org/10.48550/arxiv.1810.05263>
- [14] Parakh, A., & Kak, S. (2009). "Recursive secret sharing for distributed storage and information hiding". In 2009 IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems, New Delhi, India, doi: <http://10.1109/ANTS.2009.5409868>
- [15] Xu, Youmin & Zhang, Xuanyu & Yu, Jiwen & Mou, Chong & Meng, Xiandong & Zhang, Jian. (2024). "Diffusion-Based Hierarchical Image Steganography." doi: <http://10.48550/arXiv.2405.11523>
- [16] Zhang, X., Zhang, J., Ma, L., Xue, P., Hu, Y., Wu, D., Zhan, Y., Feng, J., & Shen, D. (2022), "Progressive Deep Segmentation of Coronary Artery via Hierarchical Topology Learning," *Lecture Notes in Computer Science*, 391–400. doi: https://doi.org/10.1007/978-3-031-16443-9_38