AlexNet-based Visible light communication devices fingerprint extraction and authentication in broadcast systems

Ziqi Liu, Dayu Shi, Samia Oukemeni, Xun Zhang

AlexNet-based Visible light communication devices fingerprint extraction and authentication in broadcast systems

Ziqi LIU
LISITE-ECoS
ISEP
Paris, France
ziqi.liu@eleve.isep.fr

Dayu SHI
LISIT-ECoS
ISEP
Paris, France
dayu.shi@ext.isep.fr

Samia OUKEMENI
LISIT-ECoS
ISEP
Paris, France
samia.oukemeni@isep.fr

Xun ZHANG* (IEEE senior member)
LISIT-ECoS
ISEP
Paris, France
xun.zhang@isep.fr

***Abstract*—Visible Light Communication (VLC) is one of technology for the sixth generation (6G) wireless communication and also broadcast system. VLC systems are more resistant against Radio Frequency interference and unsusceptible to security like most RF wireless networks. Since VLC is one of suitable candidate for enforcing data security in future wireless networks. This paper considers improving the security of the next generation of wireless communications by using wireless device fingerprints in visible light communication, which could be used potentially for ATSC broadcasting applications. In particular, we aim to provide a detailed proposal for developing novel wireless security solutions using Visible light communication device fingerprinting techniques. The objectives are two-fold: (1) to provide a systematic review of AI-based wireless device fingerprint identification method and (2) to identify VLC transmitter, with respect to the ATSC physical layer modulation scheme, by analysing the differences in the modulated constellations signaled received by photo-diode, which will be proved by laboratory experimentation.**

***Index Terms*—ATSC 3.0, VLC, fingerprint, cyber security, broadcast**

I. Introduction

The next-generation Digital Terrestrial Television(DTT) standard, known as "ATSC 3.0", which does not have any backwards-compatibility constraints with existing ATSC standards [1]. It provides television services to both fixed and mobile receivers, including conventional TV sets, handheld devices, car screens, and portable receivers [2]. Nowadays, massive demand for mobile data demand for mobile data broadcasting and location-related broadcasting service in broadband networks is rapidly increasing [3], and specially in indoor environment. It makes the ability of the spectrum to accommodate multiple users is limited and will be difficult in the future [4]. The security protection requirements, including security access method, security authentication, security transmission, and data privacy etc, are significantly increasing. In the ATSC 3.0 standard, encryption is indeed a fundamental part of the overall system. This includes cryptographic signatures for signaling and applications [5] [6], security protocols in the Studio-to-Transmitter (STL) link [7], and protection of broadcast content through encryption [8], in which the security authentication is most important one.

Meanwhile, VLC has been proved which is one of good broadcast and broadband indoor access technology [3]. It is a key technology for the Beyond 5G/6G in using artificial environmental lights as a data transfer channel. It provides hundreds of terahertz (THz) bandwidths that are available worldwide and unlicensed. It has the advantages of anti-electromagnetic interference and high data rates (up to 100 Gbps) [9]. Especially with the approval of the IEEE 802.15.7 standard, it has brought considerable prospects and benefits to indoor VLC research [10], and IEEE 802.11 LC, which aims to amend base IEEE 802.11 standard and enable communications in the visible light medium [11].

VLC communication systems can exhibit better security performance in indoor communication environments due to the impenetrability of their own visible channels to opaque objects [12]. Therefore, the VLC system can make indoor broadcast communication free from eavesdropping or interference by external devices to guarantee the security of ATSC3.0 system.

In this paper, we propose a visible light signal frequency fingerprinting identification (VLFID) scheme that combines with two-layer model is proposed to realize extracion and authentications for visible light communication systems. VLC device fingerprint recognition is a potential solution to reduce the vulnerability of wireless networks that are prone to have forged nodes pretending to be insiders [13]. However, in the field of visible light communication, the method of device fingerprint identification is still new and not well studied. Existing fingerprint identification methods in visible light communication only have fingerprint identification methods based on the characteristics of LED hardware [14], however, research is lacking of fingerprint identification methods based on the difference in signal characteristics of different devices during signal transmission. In this context, our proposed VLFID scheme by observing the distortion of received ATSC modulated signal on the receiver side. This constellations image distortion is dependent on the non-linearity of VLC device and should be unique for each one.

The main contributions of this paper can be summarized as follows:

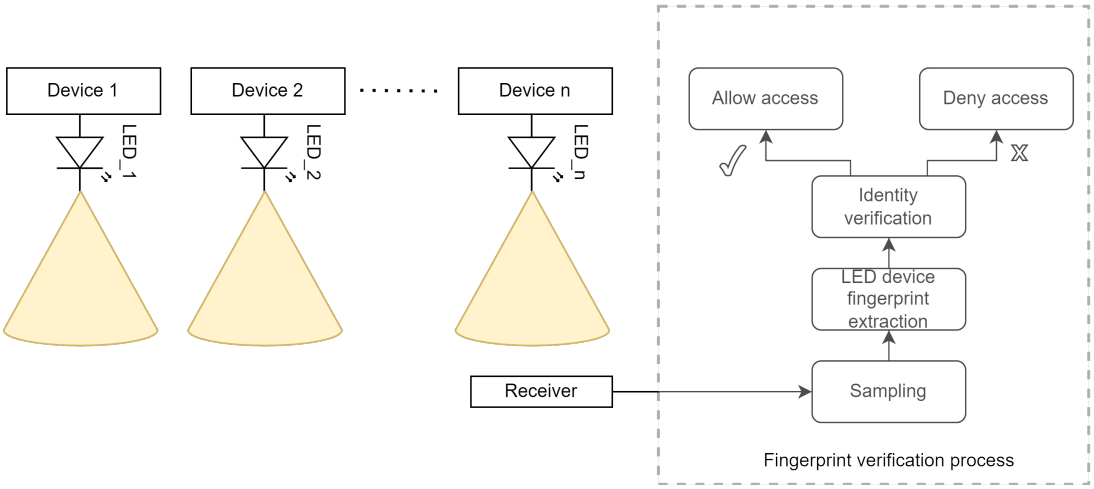

Fig. 1. Indoor VLC application scenario diagram.

- Establishing a device fingerprint model for the VLC communication system. The difference of the constellation diagram of different LED devices in the process of optical communication is used as the fingerprints.
- Proposing a new method for identifying and extracting the fingerprint
- Testing the accuracy of the method for identifying equipment using simulation experiments

The remainder of this paper is organized as following: the section II proposes theoretical sources on device fingerprinting. The section III proposes the system model in detail. The section IV presents the construction, operation, and result analysis of the experimental environment. The discussion and conclusion are presented in the section V.

II. Previous Work

In this section we describe the mechanism of Radio Frequency Fingerprinting (RFF) identification and the feasibility of using RFF method in VLC communication systems.

In the literature, RF Device fingerprinting technology is a new security mechanism designed to identify transmitters by extracting hardware-based features present in the signal [15] [16]. These unique hardware characteristics result from non-linearities and defect-induced tolerances in the transmitter circuit manufacturing process [17].

RFF of a wireless communication device is an intrinsic feature that is difficult to imitate. Therefore, in theory, all wireless communication devices can be identified by extracting radio frequency fingerprints [18]. The key step of RFF is feature extraction. Existing work has proposed various features, including carrier frequency offset [19], time-frequency statistical characteristics [20] and in-phase/quadrature imbalance [21], etc. Recently, deep learning-based RFF techniques have been proposed for radio frequency systems, and have achieved high recognition accuracy through data accumulation and model training [22].

Inspired by the success of radio frequency fingerprinting technology, RF device fingerprinting technology has been carried out in the field of VLC communication to improve the security of VLC communication system. In our recent work, a light-emitting diode (LED) fingerprint extraction method for the VLC system was proposed [14]. Using the k-means clustering method, the recognition accuracy of five commercial white LEDs can reach 98.8%. This work demonstrates the feasibility of VLC device fingerprinting [14]. This method is dependant strongly on LED characteristics, which can not be adapted with various LED technology like OLED, QLED and Laser-diode. Based on this previous work, we proposes a VLC fingerprint feature identification method by using Convolutional Neural Network (CNN)-AlexNet. Here, the visible light signal fingerprint of VLC devices is based on the different characteristics of the modulated lighting signal constellation.

III. System Model

In this section, our proposed system model is described. Firstly, an indoor VLC security scenario is shown in the Fig.1. On the receiver side, a fingerprint verification process is established firstly before accessing users data. It makes decision to allow access or not. In the rest of this section, we present VLC fingerprint extraction and identification mechanism, and a description of convolutional Neural Network (CNN) which has been used in our VLC device fingerprint identification method.

A. Extraction and Identification Mechanisms

Our proposed VLC device fingerprint extraction and identification mechanism is illustrated in the Fig.2. As shown here, the VLC device fingerprint extraction and identification method consists of six steps: signal collection, signal analysis and process, feature extraction and classification, fingerprint database, and device identification. Our device identification method refers to identification based on the visible light signal fingerprint of the VLC devices to confirm the access

of the legal wireless devices, thereby realizing the identify authentication of the wireless devices. The device identification methods, which embodies the hardware property of the VLC transmitters, we [14] made a description of VLC device fingerprint and introduced electronic component tolerances due to differences in hardware devices, such as LED front-end circuits. The electronic component tolerance effect of visible light transmitters is the main reason fore generating VLC device fingerprint. Since the hardware of any two VLC devices is different and hard to be faked, it is feasible to uniquely identify electronic component by visible light signal fingerprinting.

It mainly includes two processes. The first one is offline to establish a fingerprint database for legitimate VLC devices by implementing, analyzing and processing the modulated lighting signals after collecting the signals of legitimate devices.

Here, received VLC broadcasting signals from n VLC channels are input in our training model. The signal constellation is analyzed and processed, and the classification model is obtained through the AlexNet deep learning network. This model is used as the standard for equipment identification and classification certification.

The second process is an online authentication process. The signals of the VLC devices to be identified are collected and the fingerprint features are extracted through signal analysis and processing. Then, checking and recognition are carried out in the existing legitimate fingerprint database.

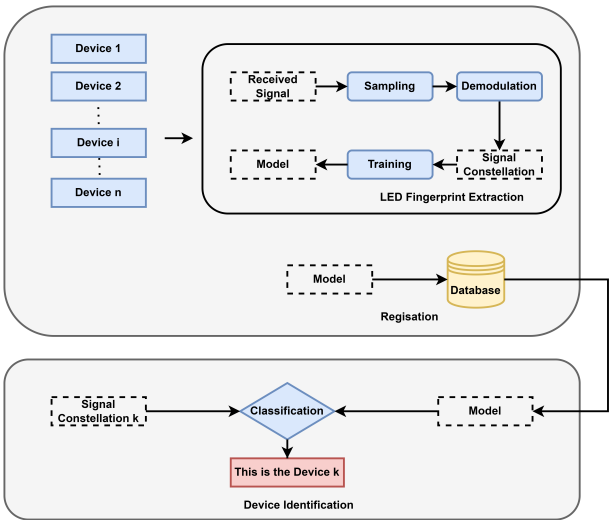

Fig. 2. LED Fingerprint Extraction and Identification Mechanism.

Recently, in order to further improve the authentication rate of visible light signal fingerprinting identification, machine learning method is taken as a recognition algorithm in our previous work [14]. This method extracts the unique LED fingerprint to identify the devices in a multi-access VLC scenario to further strengthen the network security. The method targets specific LEDs to perform feature vector extraction. It has high recognition accuracy when targeting the same type of LEDs, but it still needs to reconfirm new feature vectors for classification by machine learning when classifying devices with different LED types. For this reason, in this paper, deep learning classification is chosen for different uses of the device communication signal constellation graph, avoiding both the complexity of extracting fingerprints based on the features of the LED itself and the difficulty of representing manual features to the machine due to the need to provide them in machine learning. For example, in RF fingerprint identification, a device fingerprint identification method based on continuous multi-interval differential constellation trace figures(DCTF) using DL to build a classification model achieves 96.3% and 98.4% classification accuracy at 5 dB and 10 dB, respectively [23]. However, there is still a lack of research applying such methods to the field of VLC, so here, an AlexNet CNN network is used to train the classification of signal constellation maps in VLC communication systems for the purpose of device identification.

In the next, the detail of AlexNet CNN network will be detailed.

B. Convolutional Neural Network-AlexNet

In this section, we propose a convolutional Neural Network algorithm to distinguish the differences in the constellation maps generated by different devices with a satisfied authentication rate.

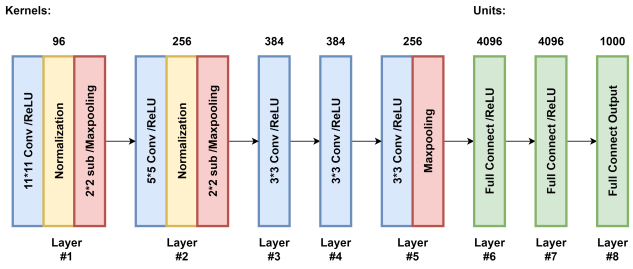

Fig. 3. Alexnet structure.

As the landmark model for ImageNet classification and the winner of ILSVRC'12, AlexNet made a huge contribution in popularizing the CNN in computer vision with a large and deep architecture [24]. AlexNet consists of five convolutional layers and three fully connected layers with a 1000-way softmax layer, as shown in Fig.3. AlexNet uses several new features to improve training efficiency and classification accuracy. For example, AlexNet uses a non-saturating activation function Re-LU [25], as shown in the following equation:

$$f(x) = tanh(x) or f(x) = (1 + e^{-x})^{-1} \quad (1)$$

This results in a much faster training process than before. Another highlight feature is a regularization method, "dropout", which is achieved by reducing the co-adaptation of neurons to prevent overfitting [26]. Technically, it sets the hidden neuron output to zero with probability 0.5. This requires the network to learn more features than usual.

IV. Visible Light Signal Fingerprinting Identification Method Evaluation

In this section, the feasibility and accuracy of the proposed method was evaluated by a demonstration implemented in a practical laboratory environment. Our method has been tested in two different environment: ideal situation without any ambient light and classic ambient lighting environment. In the rest of this section, the demonstration setup, AlexNet training steps and results analysis will be details.

A. Demonstration Setup

To test and evaluate the above proposal, we designed and implemented the following demonstration. More specifically, the NI PXIe-1071 is the terminal which generates the QPSK signal comforming to the ATSC 3.0 standard. It connects to the VLC front-end via Universal Radio Software Peripheral(USRP). Visible light signal is received by PDA10A-EC photo-diode via the environmental channel and sent back to the NI PXIe-1071 through the NI USRP-2950R. LabView is used to process the received signal, draw and observe the corresponding signal constellation diagram and store the corresponding signal data. The actual scene of signal generation and collection is shown in Fig.4:

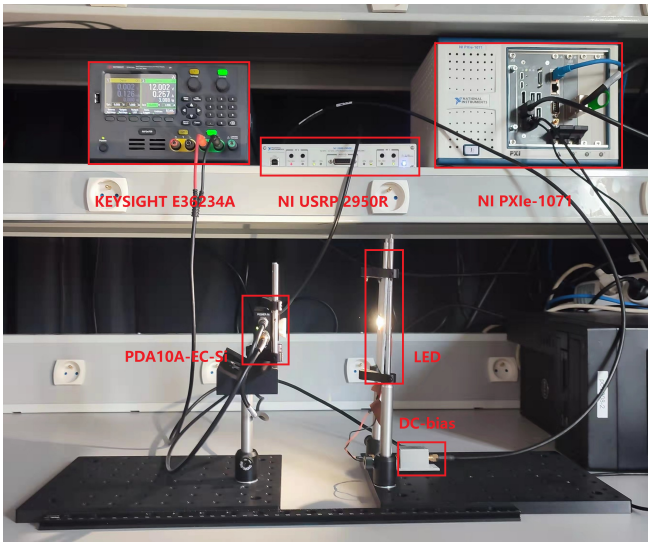

Fig. 4. Demonstration Environment Scenario.

B. AlexNet Training steps

There are several steps of AlexNet training, as shown in the Fig.5:

1) Once received signal data of each LED were stored in our server (1000 samples for each LED) and the constellation diagram images are generated. Each image is labeled according to the name of LED,

2) 3000 and 1000 labeled images per modulation category are collected to form training and validation data sets, respectively. In our test, 70% datasets (constellation diagram image) are used for training set and the rest of 30% for validation set,

3) both data sets are fed to DL networks for training with AlexNet,

4) after a maximum of 1200 training iterations, some trained models with suffix ".model" can be obtained. In this paper, training is conducted on our computing server with a Nvidia GeForce GTX1080 GPU, and the training time of AlexNet is about 6 min each time.

C. Results analysis

The final AlexNet-based Visible light communication devices fingerprint extraction results are shown in the Fig. 6.

Under the conditions of different lighting and different transmission distances (set 25cm, 30cm, 40cm, 50cm four kinds of signal transmission distance for testing sampling), the prediction accuracy rate is above 97.49%, and the average accuracy rate is 98.25%.

Because of Lambert distribution of our LED device [27], the lighting power the weakest at $30cm$ distance and thus the identification accuracy is less than the three others setup. The best distance of communication is $40cm$, afterthat the received signal power is decreased.

V. Conclusions

This paper has developed a AlexNet-based Visible light communication device fingerprinting identification method , which could be used potentially to enhance ATSC 3.0 network security. The presented two-layer model is suitable for broadcasting network paradigms. The proposed method is verified by experiments for various communication distances (25cm, 30cm, 40cm, 50cm) in three environments (with sunlight and lighting, with sunlight without lighting, without sunlight without lighting). Its average accuracy is 98.25%. Our experimentation have demonstrated the effectiveness of this method in actual laboratory environments.

Acknowledgment

The authors gratefully acknowledge the financial supports of the Chinese Scholarship Council and the EU Horizon 2020 program towards the 6G BRAINS project H2020-ICT 101017226.

References

[1] L. Fay, L. Michael, D. Gómez-Barquero, N. Ammar, and M. W. Caldwell, "An overview of the atsc 3.0 physical layer specification," *IEEE Transactions on Broadcasting*, vol. 62, no. 1, pp. 159–171, 2016.

[2] L. Michael and D. Gómez-Barquero, "Modulation and coding for atsc 3.0," in *2015 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, pp. 1–5, IEEE, 2015.

[3] L. Shi, D. Shi, X. Zhang, B. Meunier, H. Zhang, Z. Wang, A. Vladimirescu, W. Li, Y. Zhang, J. Cosmas, *et al.*, "5g internet of radio light positioning system for indoor broadcasting service," *IEEE Transactions on Broadcasting*, vol. 66, no. 2, pp. 534–544, 2020.

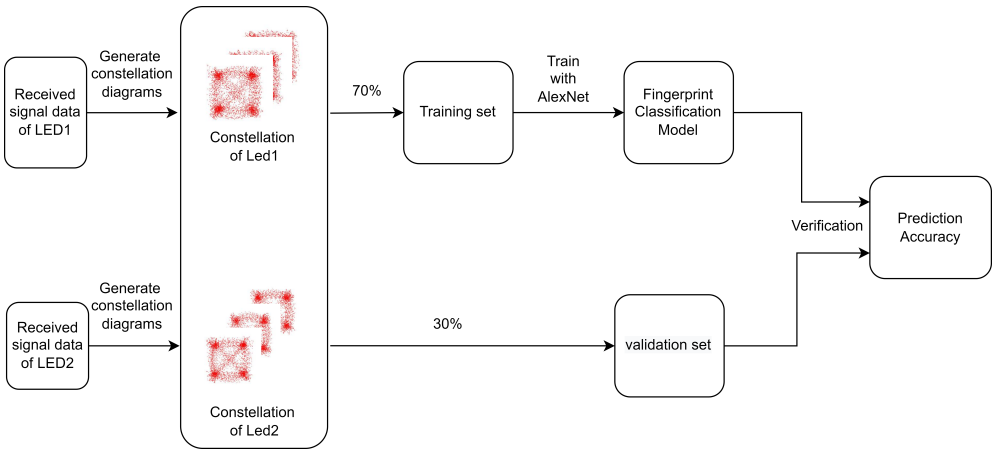

Fig. 5. Classification training validation structure.

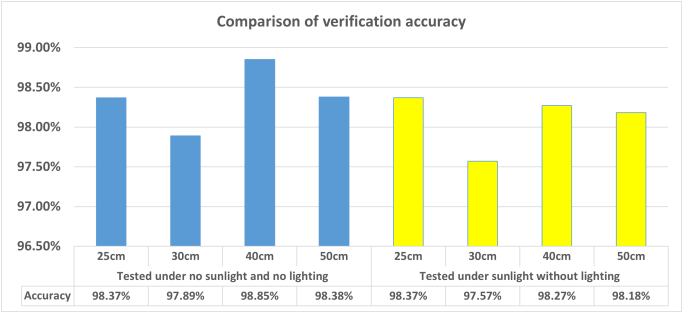

Fig. 6. The accuracy of distinguishing two LEDs at different distances under different lighting conditions.

[4] F. Aftab, S. Ali, *et al.*, "Light fidelity (li-fi) based indoor communication system," *arXiv preprint arXiv:1606.02831*, 2016.

[5] "Recommended Practice for ATSC 3.0 Television Sets, Security & Protected Services (CTA-CEB32.9)," September 2018.

[6] "ATSC 3.0 Security and Service Protection, ATSC Standard A/360," August 2019.

[7] "ATSC Standard:Scheduler / Studio to Transmitter Link, ATSC Standard A/324," January 2018.

[8] "ATSC Recommended Practice:Digital Rights Management (DRM), ATSC Standard A/362," January 2020.

[9] A. Tsiatmas, F. M. Willems, J.-P. M. Linnartz, S. Baggen, and J. W. Bergmans, "Joint illumination and visible-light communication systems: Data rates and extra power consumption," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, pp. 1380–1386, IEEE, 2015.

[10] S. Hranilovic and F. R. Kschischang, "Short-range wireless optical communication using pixilated transmitters and imaging receivers," in *2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577)*, vol. 2, pp. 891–895, IEEE, 2004.

[11] M. S. Amjad, C. Tebruegge, A. Memedi, S. Kruse, C. Kress, J. C. Scheytt, and F. Dressler, "Towards an ieee 802.11 compliant system for outdoor vehicular visible light communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5749–5761, 2021.

[12] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *2014 IEEE International Conference on Communications (ICC)*, pp. 3342–3347, IEEE, 2014.

[13] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 94–104, 2015.

[14] D. Shi, X. Zhang, A. Vladimirescu, L. Shi, Y. Huang, and Y. Liu, "A device identification method based on led fingerprint for visible light communication system," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–7, 2020.

[15] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.

[16] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 116–127, 2008.

[17] K. G. Gard, L. E. Larson, and M. B. Steer, "The impact of rf front-end characteristics on the spectral regrowth of communications signals," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 6, pp. 2179–2186, 2005.

[18] N. S. Aminuddin, M. H. Habaebi, S. H. Yusoff, and M. R. Islam, "Securing wireless communication using rf fingerprinting," in *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*, pp. 63–67, IEEE, 2021.

[19] C. G. Wheeler and D. R. Reising, "Assessment of the impact of cfo on rf-dna fingerprint classification performance," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 110–114, IEEE, 2017.

[20] Y. Yuan, Z. Huang, H. Wu, and X. Wang, "Specific emitter identification based on hilbert-huang transform-based time-frequency-energy distribution features," *IET communications*, vol. 8, no. 13, pp. 2404–2412, 2014.

[21] Y. Huang *et al.*, "Radio frequency fingerprint extraction of radio emitter based on i/q imbalance," *Procedia computer science*, vol. 107, pp. 472–477, 2017.

[22] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based rf fingerprint identification using differential constellation trace figure," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1091–1095, 2019.

[23] Y. Yang, A. Hu, J. Yu, G. Li, and Z. Zhang, "Radio frequency fingerprint identification based on stream differential constellation trace figures," *Physical Communication*, vol. 49, p. 101458, 2021.

[24] S. Peng, H. Jiang, H. Wang, H. Alwageed, Y. Zhou, M. M. Sebdani, and Y.-D. Yao, "Modulation classification based on signal constellation diagrams and deep learning," *IEEE transactions on neural networks and learning systems*, vol. 30, no. 3, pp. 718–727, 2018.

[25] M. A. Abdel-Moneim, R. M. Al-Makhlasawy, N. Abdel-Salam Bauomy, E.-S. M. El-Rabaie, W. El-Shafai, A. E. Farghal, and F. E. Abd El-Samie, "An efficient modulation classification method using signal constellation diagrams with convolutional neural networks, gabor filtering, and thresholding," *Transactions on Emerging Telecommunications Technologies*, p. e4459, 2022.

[26] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, 2012.

[27] I. Moreno, C.-Y. Tsai, D. Bermudez, and C.-C. Sun, "Simple function for intensity distribution from leds - art. no. 66700h," *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 6670, 09 2007.