Titre Thèse (subject)	**Study and Development of Automatic Signal Recognition Based On Deep Learning and Imaging Technologies: Application in e-Health**	
Directeur (supervisor)	Abdelmalik Taleb-Ahmed	E-mail : Abdelmalik.Taleb-Ahmed@uphf.fr
Co-Directeur (co-supervisor)	Ihsen Alouani	E-mail : Ihsen.Alouani@uphf.fr
Laboratoire (research unit)	DOAE	Web :
Equipe (research team)	COMNUM	Web :
Financement prévu ☐	Contrat Doctoral Etablissement ☒ Région ☐ – Autre ☐ Contrat de recherche ☐ Préciser :	ULille ☐ UPHF ☒ Centrale Lille ☐ UGE ☐ IMT ☐ Autre ☐
Financement acquis ? ☐	Contrat Doctoral Etablissement ☐ Région ☐ – Autre ☐ Contrat de recherche ☐ Préciser :	ULille ☐ UPHF ☐ Centrale Lille ☐ UGE ☐ IMT ☐ Autre ☐

Abstract :

Study and Development of Automatic Signal Recognition Based On Deep Learning and Imaging Technologies: Application in e-Health

I. INTRODUCTION

Deep Learning (DL) technologies have shown outstanding achievements in many fields such as computer vision, healthcare, and Internet of Things (IoT). Inspired by these advances, many researchers in the field of wireless communications suggest adopting such models to solve problems in this area. For instance, several researches work based on DL, are being conducted in signal processing area such as Automatic Signal Recognition. The main idea behind these works is to convert the signal processing problem into image processing one to take advantage of the advancements of several DL models already developed in imaging technologies. however, although Deep Learning algorithms have gained popularity owing to their practical problem-solving capacity, they suffer from a serious integrity threat, i.e., their vulnerability to adversarial examples [1-3]. These attacks consist of inputs crafted carefully by additive imperceptible adversarial noise to force the system output to a wrong label. Therefore, using DL in the context of wireless communication should consider the potential threat of these attacks to the system integrity and the communication availability.

There are still currently regions where access to care remains very limited. The objective of this action is to offer an innovative system for the diagnosis and medical monitoring of patients, who are in regions where there is no economic reasons for high-level medical infrastructures, relying on new digital wireless communications technologies combined with Artificial Intelligence. AI is a disruptive technology in the medical field. Thanks to advances in nanotechnology, information technology and wireless communication, today's patient can receive care or monitoring at home. This new way of monitoring the state of health of patients makes it possible to anticipate health problems and human losses. It also makes it possible to reduce the cost and time of hospitalization, and above all to offer quality care for everyone, regardless of where they live.

These technological advances will be able to meet the needs of users in health services, to improve the quality of care or to fight against medical deserts by promoting access, sometimes remotely, to diagnoses and prescriptions adapted to the entire territory, with limited human intervention, even tomorrow without requiring this type of intervention

In this thesis work, we propose to develop innovative solutions in the field of secure transmission / reception, automatic (blind) extraction and classification of data and up to DL treatment, for advanced diagnosis and patient monitoring at distance [4, 5].

On the other hand, medical records of patients represent highly sensitive personal data. For this reason, transmitting this information in wireless represents an important challenge from a security perspective. Using DL in a wireless communication context is promising given its efficiency in solving complex real-life problems. However, it has been proven recently that these systems have a critical vulnerability to "adversarial attacks" [6]. These attacks consist of carefully designed additive low-amplitude noise that forces the DL output to a wrong label when superimposed to a benign input.

Therefore, we propose to explore the efficiency and practicality of adversarial attacks in the context of wireless communication for e-health, and investigate denoising-based mitigation techniques to enhance DL robustness against adversarial attacks. We plan to investigate the problem on three different levels:

1st level: Explore the recognition of the signal source to prevent rogue emitters from jamming or impersonating the communication

2nd level: Investigate the robustness of DL-based system against different noise distributions, especially noise related to medical operating environment such as impulsive noise.

3rd level: Proof of concept of adversarial malicious noise targeting DL in a wireless communication setting, and denoising-based defense in the receiver side.

Implement the solutions proposed in this thesis on a USRP/NI RIO Intelligent Radio platform available at the IEMN-DOAE laboratory.

This work will be carried out in close collaboration with the Valenciennes hospital center (CHV)

REFERENCES

[1] Z. Zhang, C. Wang, C. Gan, S. Sun and M. Wang, "Automatic Modulation Classification Using Convolutional Neural Network With Features Fusion of SPWVD and BJD," in IEEE Transactions on Signal and Information Processing over Networks, vol. 5, no. 3, pp. 469-478, Sept. 2019.

[2] D. Wang et al., "Modulation Format Recognition and OSNR Estimation Using CNN-Based Deep Learning," in IEEE Photonics Technology Letters, vol. 29, no. 19, pp. 1667-1670, 1 Oct.1, 2017.

[3] M. Zhang, M.Diao and L.Guo, "Convolutional Neural Networks for Automatic Cognitive Radio Waveform Recognition," in IEEE Access, vol. 5, pp. 11074-11082, 2017.

[4] Maier, C. Syben, T. Lasser, C. Riess, "A gentle introduction to deep learning in medical image processing",Zeitschrift für Medizinische Physik, Vol 29, Issue 2, Pages 86-101, 2019,

[5] K. Mingyu Kim, Y. Jihye Yun, C. Yongwon , "Deep Learning in Medical Imaging", Neurospine. Vol 16, N°4, pp 657-668, 2019; DOI: https://doi.org/10.14245/ns.1938396.198

[6] V. Venceslai, A. Marchisio, I. Alouani, M. Martina and M. Shafique, "NeuroAttack: Undermining Spiking Neural Networks Security through Externally Triggered Bit-Flips," 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, United Kingdom, 2020, pp. 1-8, doi: 10.1109/IJCNN48605.2020.9207351.