국방 시스템을 위한 최신 인공지능기술 분석

김재우, 권기협+, 김동성*
+ICT융합특성화연구센터, *국립금오공과대학교
{jaewookim, +navkwon, *dskim}@kumoh.ac.kr

Analysis of Recent Artificial Intelligence Technologies for Defense Systems

Jae-Woo Kim, Gi-Hyeob Kwon+, Dong-Seong Kim*
+ICT Convergence Center, *Kumoh National Institute of Technology

요 약

최근 인공지능(AI) 기술의 발전은 다양한 분야에서 혁신적인 변화를 가져오고 있다. 특히 최근 생성형 AI, 설명가능한 AI(XAI), 강건한 인공지능(robust AI), 정보보호 인공지능(Privacy Protection AI) 기술은 그 중요성이 강조되고 있으며, 국방 분야에서도 큰 잠재력을 가지고 있다. 본 논문에서는 이런 최신 인공지능 기술들을 분류하고 각 기술의 특징과 국방 분야에서의 활용 가능성에 대해 논의하고자 한다.

Ⅰ. 서 론

인공지능(AI) 기술은 최근 몇 년간 급속히 발전하여 다양한 분야에서 혁신을 주도하고 있다. 기존의 인공지능 기술 분류는 크게 지도학습(Supervised Learning), 비지도학습(Unsupervised Learning), 강화학습(Reinforcement Learning) 등의 학습 방법에 따라 분류된다. '미래 국방 2030 기술 전략'에서는 AI 기술 분류 체계를 공통 AI 기술과 기능별 AI 기술로 구분하고 있다(그림1)[1]. 공통 AI 기술 분류는 다시 현재 빅데이터 기반의 딥러닝을 중심으로 발전하고 있는 AI 기술 측면을 고려하여 AI 학습을 위해 필요한 학습 지능, AI 기술에 대한 신뢰성을 부여할 수 있는 신뢰 지능, 서버 및 모바일 환경에서 AI 기능 적용 시 필요한 고성능 AI H/W 분야로 구분하고 있다. 기능별 AI 기술은 국방 AI 기능 발전 단계와 전투 수행 순서인 OODA (ObserveOrient-Decide-Act) Loop를 고려하여 감시, 정찰 등을 통해 전장 환경에 대한 정보를 획득하여 정보를 제공하는 전장인식 분야, 수집된 정보를 분석하여 전장 환경과 상황을 이해하고 상황추론의 결과를 제공하는 자율 판단 분야, 분석된 전장 환경에 대하여 수행임무를 식별/계획하고 임무를 할당하는 지휘 결심 분야, 부여된 임무를 수행하기 위한 수행 분야로 구분한다. 이러한 AI 기술들은 데이터 분석, 패턴 인식, 예측 모델링 등 다양한 응용 분야에서 사용되었다. 최근에는 생성형 AI, 설명가능한 AI(XAI), 강건한 인공지능(robust AI), 정보보호 인공지능(Privacy Protection AI) 등의 새로운 AI 기술들이 등장하면서, 보다 특화된 기능을 제공하며 특히 국방 분야에서의 활용 가능성이 주목받고 있다. 이와 같은 최신 AI 기술들을 바탕으로, 본 논문에서는 최신 인공지능 기술들에 개요와 특징을 분석하고, 이들 기술이 국방 분야에서 어떻게 적용될 수 있는지 그리고 기대효과와 제한사항에 대해 논의한다.

Ⅱ. 최신 AI 기술 분석

표1은 최신 AI 기술을 분석 정리한 것이다. 특히 국방 시스템에서의 활용과 기대효과와 제한사항을 통해 향후 도전과제를 제안하였다.

1. 생성형 AI (Generative AI)

생성형 AI는 주어진 데이터로부터 새로운 데이터를 생성하는 기술이다. 대표적인 예로는 GPT(Generative Pre-trained Transformer)와 같은 언어모델이 있으며, 이들은 텍스트, 이미지, 음악, 코드 등 다양한 형식의 콘텐츠를 생성할 수 있다[2]. 국방 분야에서는 생성형 대규모 언어모델(LLM)과 국방 데이터를 융합해 국방 GPT를 개발과 AI 관련 데이터수집

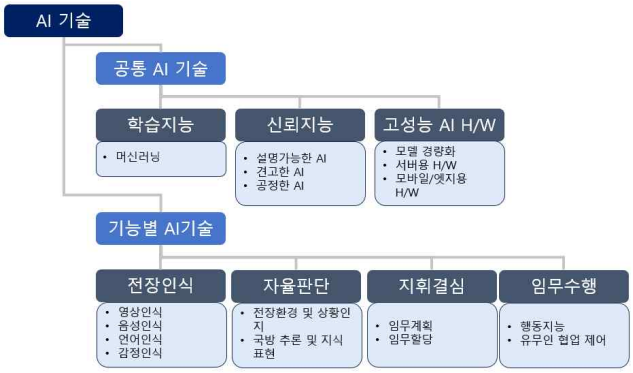

그림 1 국방 AI 기술분류체계 [1]

및 가공 전문업체들은 국방 분야를 혁신할 AI에 필요한 데이터를 직접 만들어 AI의 사용처를 확대하고 있다.

2. 설명가능한 AI (Explainable AI, XAI)

XAI는 AI 모델의 의사결정 과정을 인간이 이해할 수 있도록 설명해 주는 기술이다[3]. 국방 분야에서는 미래 국방 인공지능 특화연구센터 수행을 통해 군사적 XAI 이론 연구, 다종 국방 데이터의 융합 학습과 탐지 연구, 열악한 환경의 극소량 국방 데이터 기반 학습 연구, 탐지와 군사적 설명의 연동을 통한 최적의 방책 추천 연구 등을 수행 중으로 XAI 기술을 국방에 활용하기 위한 기초연구를 수행 중이다. 다양한 응용 분야에 따라 설명 방법이 다양하며, XAI 분야는 현재 연구 초기 단계에 해당되어, 실효성 있는 기술 발전을 위해서 지속적인 연구가 필요한 상황이다.

3. 강건한 인공지능 (Robust AI)

Robust AI는 외부 환경의 변화나 예기치 않은 상황에서도 안정적이고 신뢰성 있는 성능을 유지하는 AI를 의미한다[4]. 이는 적대적 공격이나 예측 불가능한 데이터로부터도 견고하게 작동할 수 있도록 한다. 국방 분야에서는 전장변화에 따른 사이버 보안 및 공격 탐지 측면에서 외부의 의도적인 공격을 감지하고 시스템과 네트워크를 보호하는 데 활용될 수 있다.

4. 정보보호 인공지능 (Privacy Protection AI)

정보보호 인공지능은 데이터의 프라이버시를 보호하면서도 유의미한 분석을 수행할 수 있는 기술을 의미한다. 이는 민감한 정보를 보호하기 위해 암호화, 연합 학습(Federated Learning), 차분 프라이버시(Differential Privacy) 등의 기법을 활용하여, 데이터 노출 없이 AI 모델의 성능을 유지

표 1 최신 AI 기술 분석

	특징	국방응용	기대효과	제약사항
Generative AI	- 새로운 데이터를 생성(Chat GPT) - 대규모 데이터셋을 학습 - 창작 수준의 결과 생성	- LLM에 국방 데이터를 적용 최적 판단 - 미국 팔란티어 국방 LLM 연구진행	- 군수, 전술, 무기체계 개발 특화된 국방 특화 LLM 개발 - 각 군 지휘 통제 시스템 혁신 및 차세대 전술 무전기 개발 가능	- 국방 분야에 AI 서비스를 도입하기 위한 양질의 데이터가 축적 - AI 기능 구체화 불가능 - 보안 고려 필요
Explainable AI (XAI)	- AI모델 결과 근거를 사용자가 쉽게 이해할 수 있도록 설명하는 AI - AI 모델의 판단에 근거를 설명함으로써 인공지능의 신뢰성 확보	- XAI 기반 국방 이미지 분석 및 딥러닝 가속화 기술 개발 - 국방 데이터의 융합 학습과 탐지 연구, 극소량 국방 데이터 기반 학습 연구, 군사적 설명의 연동 최적 방책 추천 연구	- XAI를 통해 AI 모델의 투명성 개선 - 추론 결과에 대한 신뢰수준을 향상 - AI가 동작 시각화, 추론 근거설명, AI 모델 사용자 지원가능	- XAI 분야는 현재 연구초기 단계 - 실효성 있는 기술 발전을 위해서 지속적인 연구가 필요
Robust AI	- 예기치 않은 상황에서도 안정적이고 신뢰성 있는 성능을 유지 - 예측 불가능한 데이터로부터도 견고하게 작동할 수 있도록 설계	- 전장 사이버 보안 및 외부의 공격 감지및 시스템보호에 활용 - 적 사이버 위협의 내·외부 및 물리 전장 정보융합 기술 활용 - 네트워크 침입감지 기술개발	- 환경 변화가 많은 자율주행 등의 분야나 적대적 공격 등이 존재할 수 있는 네트워크 및 사이버 보안 분야 등의 적용 시 AI 모델의 신뢰성을 확보	- 인공지능 모델은 데이터의 의존성이 높아 환경의 변화에 예민 - 다양한 환경 변화나 적대적 공격에 아직은 취약
Privacy Protection AI	- 민감한 정보를 보호하기 위해 암호화, 연합 학습, 차분 프라이버시 등의 기법을 활용 - 데이터 노출 없이 AI 모델의 성능을 유지할 수 있도록 한	- 개인정보 보호가 필요한 의무 분야나 인사/행정 등 다양한 전력지원체계에 활용하며, 디지털 인사체계나 영상판독, 맞춤형 체력관리 시스템 등에 적용 가능	- 연합학습 기법을 통해 데이터 및 개인정보를 보호 및 활용성이 확대 - 컴퓨팅 자원이 한정적인 군부대에서 개인정보 보호 및 기술들을 통해 이러한 문제를 해결할 수 있을 것	- 충분한 대역폭과 지연 시간이 필요 - 이동 장치와의 통신요소도 고려 - 클라이언트 간 데이터 분산 및 레이블 불균형 문제,데이터 유출, 중간 공격 및 모델 역공학과 같은 보안 위협은 존재
Edge AI	- 데이터가 생성되는 단말에서 직접 AI 알고리즘을 처리 - 실시간,저지연,개인정보보호 가능 - 네트워크 불안정 환경에서도 작동 - 경량화된 엣지 AI 프레임워크	- 무인기 및 군용 감시 장비 등 단말장치에서 엣지 AI 모델의 개발 - 군사 목적 무인 이동체, 대공 체계 등에 경량 AI 모델을 탑재하여 추론 지연 시간 감소, 전장에서 빠른 대응 속도 실현	- 대기 시간이 짧고 로컬에서 신속한 데이터 처리 가능, - 네트워크와 인프라 비용 절감 - 근거리 엣지 서버에서 동작으로 통신 제약이 적고 보안성이 향상되어 전장 환경에서 활용이 용이	- 오픈 소스의 경우 보안성 검증이 필요 - 사용목적과 엣지 H/W 제조사 성능에 따라 최적화가 요구 - 엣지 H/W 성능에 따라 AI 모델의 추론을 위해 높은 수준의 압축 기술 필요

할 수 있도록 한다. 국방 분야에서는 개인정보 보호가 필요한 의무 분야나 행정 등 다양한 전력지원체계에 활용하며, 디지털 인사체계나 영상판독, 체력관리 시스템 등에 적용가능하다[5]. 정보보호 인공지능을 국방에 적용하므로 기대할 수 있는 효과는 국방 데이터의 경우 보안 등의 이유로 데이터를 공유가 어려울 수 있고, 모델 개발 업체에 제공이 어려운 부분이 있으므로 연합학습기법을 통해 데이터 및 개인정보를 보호하는 기술을 적용 시 데이터 보호 및 활용성이 확대될 것으로 기대된다.

5. 엣지 AI

엣지 AI는 중앙 서버나 클라우드가 아닌, 데이터가 생성되는 디바이스나 현장에서 처리되는 엣지컴퓨팅을 기반으로 직접 AI 알고리즘을 처리하는 기술이다. 국방 분야에서는 드론, 자율주행 선박, 국방 무인 이동체, 대공체계 등에 경량 AI 모델을 탑재하여 추론 지연 시간 감소 등 전장에서 빠른 대응 속도 실현 가능하다[6]. 엣지 디바이스에서 실행할 수 있는 경량화 프레임워크 기술은 과학화 경계 시스템, 방공 C2A(Command Control and Alert) 체계, 초소형 스마트 무장지휘통제소, 무인 수상정·군집 드론 등 드론봇 전투체계, 국방 IoT, 군 야간 감시 장비 등에 활용된다.(그림2)

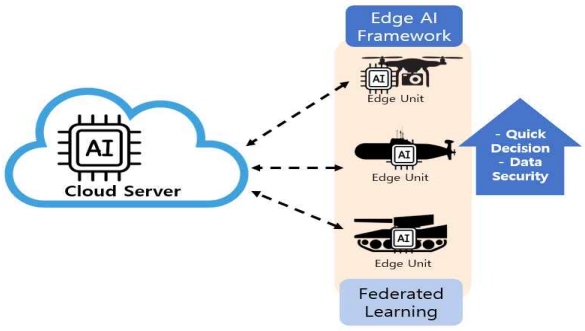

그림 2 엣지 AI 구조

Ⅲ. 결론

본 논문에서는 최근 활발하게 연구되고 있는 최신 인공지능 기술에 대해 분석하고 특히 국방분야에서 어떻게 활용하고 있으며 또한 활용할 수 있는 기대효과를 논의하였고 예상되는 제약사항을 제시하였다. 인공지능 기술 영역이 발전함에 따라 다양한 분야에서 활용되고 있고 다양한 인공지능 모델들이 등장하고 있다. 향후연구로는 다양한 인공지능 기술을 국방의 각군의 소요의 차원에서 어떻게 분류할 수 있는지 그리고 구체적인 인공지능 기술을 활용할 수 있는지 지속적으로 논의할 것이며 본 논문에서 제안하는 제한사항에 대한 해결방법을 논의할 것이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성사업과 대학ICT연구센터사업의 연구결과로 수행되었고 (IITP-2024-RS-2020-II201612,25%)(IITP-2024-RS-2024-00438430,25%) 2024년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업과 기초연구사업으로 수행된 연구임(2018R1A6A1A03024003, 2022R1I1A1A0107010058).

참 고 문 헌

[1] 김재훈, 신태성, 이종웅, 이재국."미래국방 2030 기술전략", 국방기술진흥연구소(KRIT), 2022. (www.krit.re.kr)

[2] Goodfellow, Ian, et al. "Generative adversarial nets." Advances in neural information processing systems 27 (2014).

[3] Arrieta, Alejandro Barredo, et al. "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI." Information fusion 58 (2020): 82-115.

[4] Marcus, Gary. "The next decade in AI: four steps towards robust artificial intelligence." arXiv preprint arXiv:2002.06177 (2020).

[5] Collaborative Machine Learning without Centralized Training Data for Federated Learning. (2022). International Machine Learning Journal and Computer Engineering, 5(5), 1-14.

[6] Cosmas Ifeanyi Nwakanma, Jae-Woo Kim, Jae-Min Lee and Dong-Seong Kim, "Edge AI Prospect using the NeuroEdge Computing System: Introducing a Novel Neuromorphic Technology", ICT Express, Vol. 7, No. 2, pp. 152-157, June 2021,