Ⅲ. 생성형 AI의 개별적인 기술구조와 금융에서의 각각의 활용

생성형 AI는 배포 초기 단계로 아직 기술적으로 미성숙한 상태에 있으나, 금융공학과 AI의 기술이 빠르게 발전하고 있기 때문에 그 기술적 활용이 어떻게 진행될지 섣불리 예측하기 곤란하다. 다만, 현재까지 나온 생성형 AI 모델들의 현황들을 살펴볼 때 위 각 모델들을 활용하여 이미 구현하였거나 구현할 수 있을 것으로 예상되는 금융 분야를 살펴보면 다음과 같다.

1. 생성적 적대 신경망(Generative Adversarial Networks: GAN)[32]

생성적 적대 신경망은 서로 적대 또는 대립하는 관계인 2가지 AI 모델, 즉 생성기(Generator)와 판별기(Discriminator)를 동시에 사용하는 비지도학습방법이다. 생성기는 문자, 음성, 이미지 등을 생성하는 데 최대한 사실에 가깝게 위조한다. 판별기는 위 위조 내용과 실제 내용을 모두 수신하고, 두 정보를 최대한 정확하게 구별하는 것을 목표로 한다.[33] 판별기에서 나타내는 출력값이 1이면 위 위조 내용이 실제에 부합하는 것이고, 0이면 가짜로 판명되는 것이다. 따라서 생성기가 생성한 내용은 1에 가까울수록 좋다고 볼 수 있다.[34]

예를 들어, 생성기는 인공적으로 생성된 금융거래 데이터를 판별기에 제공하고 판별기는 생성기가 만든 거래 데이터와 실제 금융거래 데이터를 모두 학습하여 그 차이(손실)를 최대한 줄이고 그 내용을 생성기에 전달하여 성능을 개선하게 된다.[35] 이와 같이 두 모델이 경쟁하면서 발전하여 나가는데,[36] 훈련 수(Epoch)가 증가할 때마다 생성기가 생성하는 거래 데이터가 더 정교해진다.

금융 분야에서 생성적 적대 신경망을 활용하는 방법은 다음과 같다. ① (사기성

32) 현재는 잘 사용되고 있지는 않지만 딥페이크와 관련하여 대표적인 생성형 AI이므로 이를 소개한다.

33) Antonia Creswell *et al.*, "Generative Adversarial Networks: An Overview", *IEEE Signal Process Magazine* 35(1)(2018), pp.53-54

34) 이때 생성된 데이터가 실제 데이터와 일치할 정도가 된다면 판별기는 생성기가 제공하는 모든 입력 데이터에 대하여 0.5 이상을 나타내어 혼란스러운 반응을 보이게 된다(Antonia Creswell *et al.*, *id.*).

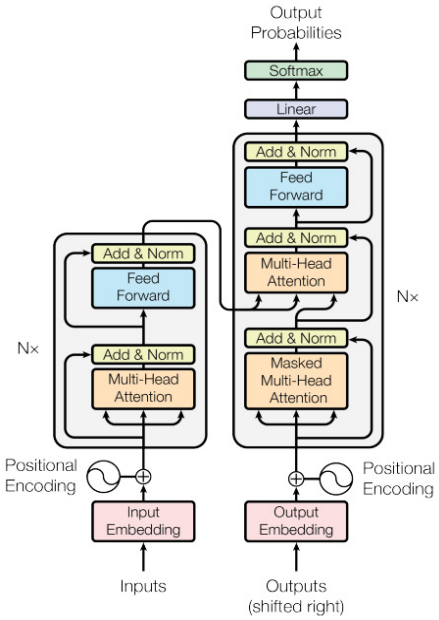
35) 생성기는 실제 데이터에 직접 접근할 수는 없고 이를 학습하는 유일한 방법은 판별기와의 상호작용을 통해서만 가능하다. 구체적으로 위 방법은 판별기의 잘못된 분류에 대하여 패널티를 부과하고 위 차이에 대하여 역전파를 통하여 입력 가중치를 새로 설정하는 방식으로 교정하게 된다.

36) Suman Kalia, "Potential impact of generative artificial intelligence(AI) on the financial industry", *IJCI Journal*, Vol. 12(2023), p.38.

거래, 시스템적 위험 탐지) 평상시와 비교하여 비정상적인 거래 패턴이나 수치를 식별함으로써 합법적인 거래와 사기성 거래를 구분하거나[37] 시스템적 위험을 미리 감지할 가능성이 있다. ② (악성코드 탐지) 금융보안을 침해하는 악성코드를 탐지하고 이를 분류할 수 있다.[38] ③ (데이터 편향 문제 해결) 많은 데이터를 최대한 학습할 필요 없이 정확하고 대표성 있는 합성 금융 데이터를 생성하여 데이터 편향(Bias) 문제를 해결할 수 있다.[39] 이에 따라 금융위험의 모델링과 리스크 관리, 포트폴리오의 최적화에 활용될 수 있다.

2. 트랜스포머 모델(Transformer model)

[트랜스포머 모델의 구동 메커니즘]



(출처: Ashish Vaswani *et al.*, "Attention Is All You Need", *Neural Information Processing Systems*(2017), p.3)

37) 특히 신용카드 사기거래 탐지에 있어서 상당한 효과를 발휘할 수 있다. 이에 대하여는 Emilija Strelcenia, Simant Prakoonwit, "A Survey on GAN Techniques for Data Augmentation to Address the Imbalanced Data Issues in Credit Card Fraud Detection", *Mach. Learn. Knowl. Extr.* 5(1)(2023), pp.304-329 참조〈https://www.mdpi.com/2504-4990/5/1/19〉.

38) 이에 대하여는 Ziyue Wang *et al.*, "CNN-and GAN-based classification of malicious code families: A code visualization approach", *International Journal of Intelligent Systems*, Vol. 37(2022), pp.12472-12489 참조.

39) Emilija Strelcenia, Simant Prakoonwit, *supra* note 37, p.311.

트랜스포머 모델은 오늘날 우리가 볼 수 있는 대규모 언어 모델(LLM)과 생성형 AI의 기반을 마련한 것으로, 기존의 순환신경망이나 합성곱신경망과는 별개인 '자기 주의 기법'(Self-attention)을 활용한다. 기계번역을 예로 들면 기존의 순환신경망이나 장·단기 기억네트워크는 번역을 단어 하나씩 처리하고 문장과 같은 긴 시퀀스의 유기적인 해석을 용이하게 해 내지 못하는 단점이 있는 반면에, 위 모델은 단어들 간의 관계, 의미를 추론하여 문장 정보를 정확하게 파악하고 문맥의 전체적인 흐름을 이해하여 번역하는 데 도움을 준다.

자기 주의 기법의 핵심 개념은 쿼리(Query, 해석하려는 단어와 다른 단어들과의 관련성을 파악), 키(Key, 단어들과의 유사성을 측정), 밸류(Value, 해당 단어의 중요도 측정)인데, 개별적인 여러 단어들에 대하여 각각 쿼리, 키, 밸류로 이루어진 세 가지 벡터를 생성한다. 위 세 가지 벡터를 통하여 입력된 각 단어와 다른 단어들과의 관련성과 유사도를 측정하고 (문맥에 따라 측정되는) 중요성의 정도에 따라 가중치를 부여함으로써 입력된 단어들 간의 상호작용을 강화한다. 이에 따라 트랜스포머 모델은 기계 번역, 문장 생성 및 문자 기반 활동에 효과적인 기능을 발휘할 수 있다.[40]

금융 분야에서 트랜스포머 모델을 활용하는 방법은 다음과 같다. ① (감정 분석) 금융 관련 뉴스, 소셜미디어 게시물 등에 나와 있는 감정이나 표현을 문맥의 흐름에 따라 이해함으로써 시장 동향과 투자자들의 정서를 분석할 수 있다. 또는 고객들의 상담 평가에 나타난 감정을 포착하여 고객에게 개별화된 투자조언을 할 수 있다. ② (금융 예측) 트랜스포머 모델은 시계열 예측(Time series)[41]에 좋은 성능을 발휘한다.[42] 데이터에서 나타나는 변화 양상과 추세를 포착함으로써 주가, 에너지나 곡물 수요 예측 등 다양한 금융응용 분야에 대하여 정확하게 예측할 수 있고, 특히 금융 포트폴리오 최적화에 도움을 줄 수 있다.[43] ③ (재무 분석) 트랜스포머 모델은 재무적인 흐름을 관찰하여 재무보고서나 설명서를 자동으로 생성하는 데 도움을 줄 수 있다.[44]

---

40) 자세한 구동 메커니즘은 Ashish Vaswani *et al.*, "Attention Is All You Need", *Neural Information Processing Systems*(2017) 참조.

41) 시간의 흐름에 따라 기록된 것.

42) Caosen Xu *et al.*, "A Financial Time-Series Prediction Model Based on Multiplex Attention and Linear Transformer Structure", *Appl. Sci.* 13(8)(2023), pp.14-15.

43) 이에 대하여는 Edmond Lezmi. Jiali Xu, "Time Series Forecasting with Transformer Models and Application to Asset Management"(2023) 참조〈https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4375798〉.

44) Tuna Tuncer *et al.*, "Asset Price and Direction Prediction via Deep 2D Transformer and Convolutional Neural Networks", Proceedings of the Third ACM International Conference on AI

3. 다중모드(Multimodal) AI[45]

생성적 적대 신경망, 변형 자동 인코더, 확산 모델, 트랜스포머 모델의 발전과 범용성이 있는 대형 언어 모델의 출현 등을 기반으로 다중모드 AI가 개발되었다. 다중모드 AI는 이미지, 음성, 문자 등 여러 유형의 데이터를 결합하여 더 정확한 예측을 하거나 통찰력 있는 결정을 내리는 모델이다. 다중모드 AI와 기존의 단일모드 AI의 차이점은 학습하는 데이터 유형이다.[46] 예를 들어, 단일모드인 금융 AI는 거시경제 데이터와 산업 데이터 및 금융 데이터만을 활용하여 금융시장을 예측하거나 분석하는 단일한 업무를 한다. 반면 다중모드 AI는 금융시장의 흐름에 영향을 미치는 객관적인 지표 외에도 투자자들의 감정, 감각 등도 수집 및 처리하여 특정한 조건이나 환경에서 더 자세하고 정확한 결과를 낼 수 있다.

다중모드 AI는 입력 모듈과 출력 모듈 외에 융합 모듈이 따로 있고 위 융합 모듈에서 이미지, 음성, 문자, 동영상 등의 각 데이터를 하나의 데이터 세트로 결합, 정렬 및 처리하는 기능을 담당한다. 이에 따라 음성 데이터만으로 일정한 이미지를 생성하거나 특정 이미지에 나타난 풍경, 감성 등을 문자로 설명하는 등 서로 다른 데이터 간 가로지르기(Crossmodal)가 가능해진다. 다중모드 AI에는 텍스트 분석기술,[47] 자연어 처리기술(Natural language processing),[48] 이미지 및 동영상 데이터에 대한 컴퓨터 시각기술, 여러 유형의 데이터에 대한 통합 시스템 기술 등이 필요하다.

금융 분야에서 다중모드 AI를 활용하는 방법은 다음과 같다. ① (정확한 투자 판단) 앞서 나온 예시와 같이 주식시장의 금융 분석을 함에 있어 객관적인 금융지표 외에도 상황 포착 및 인식에 탁월한 성능이 있어서 투자자들의 감정 및 정서 분석을 도입하여 금융기관의 정확한 투자 판단에 도움을 줄 수 있다.[49] ② (고객 상담에

---

in Finance(November 2022), pp.79-86.

45) 이 외에 확산 모델(Diffusion model)도 금융에서 중요한 역할을 하는 생성형 AI이나 여기서는 생략한다.

46) 다중모드 AI는 이미지 생성기술과 대형언어모델을 접목한 문자-이미지 생성 모델(주어진 문자로 이미지를 생성하는 AI)이 대표적이고, 이를 계기로 GPT-4와 같은 대화형 인공지능의 입력 프롬프트 다변화(음성, 이미지, 문자 등)가 시작되었다[채명식·조유리, "2023 인공지능", KISTEP 한국과학기술기획평가원(2023), 13쪽].

47) 이를 통하여 서면에 나타난 문서의 의도와 목적을 이해할 수 있게 해준다.

48) 자연어 처리기술은 음성 출력 및 인식 기능, 음성-문자 변환 기능 등을 제공한다.

49) 이에 대한 연구로 Yu-Fu Chen, Szu-Hao Huang, "Sentiment-influenced trading system based on

활용) 상담을 진행하는 금융소비자의 반응을 정확하게 판단할 수 있다. 예를 들어 "아주 잘하네요"라고 말하는 고객을 가정해 보자. 위 내용은 칭찬의 뜻을 내포할 수도 있는 반면에 비꼬는 표현이 될 수도 있는데, 기존 AI는 그 문구 자체만 인식을 하나, 다중모드 AI는 말투나 얼굴 표정과 같은 다른 유형의 데이터도 수집을 하여 정확한 반응을 구별할 수 있다. ③ (회사 및 개인의 신용 분석에 활용) 회사의 신용등급, 개인의 신용점수 등에 대하여 다중모드 AI를 활용하여 데이터를 융합하면 더 우수하고 정확한 결과를 도출할 수 있다.[50] ④ (금융업무의 간소화) 간단한 설명을 기초로 문서, 이미지, 동영상 등을 생성할 수 있으므로 내부 보고서, 엑셀파일, 광고 동영상 등 여러 업무를 쉽고 간편하게 처리할 수 있다.

Ⅳ. 금융법상 쟁점과 과제

앞서 본 바와 같이 생성형 AI는 금융 분야에서 다양하게 활용될 것으로 보인다. 그럼에도 불구하고 생성형 AI의 사용에 있어 ⓐ 조작 위험(딥페이크), ⓑ 금융안정성의 위험(플래시크래쉬, 금융시스템 리스크), ⓒ 투자자보호 관련 위험, ⓓ 데이터 유출 위험, ⓔ 불공정의 위험(데이터 편향, 자동화된 의사결정) 등과 같은 법적 문제들이 있을 것으로 예상되므로 아래에서 살펴보기로 한다.

1. 조작 위험: 딥페이크

1) '딥페이크'(Deepfake)란 AI 등 기계 학습 기술을 활용하여 생성하거나 수정된 실제 또는 가상의 동영상, 이미지, 음성 및 문자를 말한다. 딥페이크를 만드는 방법은 여러 가지가 있지만 최근에 활용되는 것은 얼굴 교환 기술을 사용하는 생성형 AI를 이용한 것이다. 특히 생성적 적대 신경망은 딥페이크의 결함을 감지하고 개선하여 딥페이크 탐지기가 그 출처를 추적하기 어렵게 만든다.[51] 아울러 다중모드 AI

multimodal deep reinforcement learning", *Applied Soft Computing* 112(4)(2021) 참조.

50) 관련 연구로 Mahsa Tavakolia *et al.*, "Multi-Modal Deep Learning for Credit Rating Prediction Using Text and Numerical Data Streams"(2023)이 있다〈https://arxiv.org/abs/2304.10740〉.

51) TC Helmus, "Artificial intelligence, deepfakes, and disinformation: A primer", *Rand*(2022), p.3.