

엣지 컴퓨팅 환경인 Raspberry Pi 5에서 가역 신경망 HiNet 이미지 은닉모델의 구현에 관한 연구

김정훈, 김세빈, 정준

동서울대학교

thdnfrhfem@gmail.com, sqlsbin@gmail.com, jj81271000@gmail.com

A study on the implementation of the HiNet image hidden model, a reversible neural network, on the Raspberry Pi 5, an edge computing environment.

JungHum Kim, SeBin Kim, Jun Jeong

DongSeoul Univ.

요약

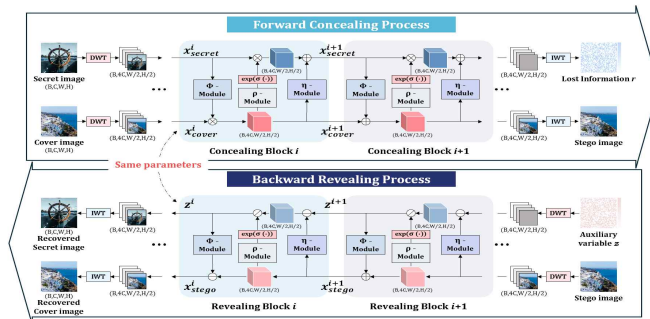
본 연구는 가역 신경망 구조의 HiNet 이미지 은닉 모델을 엣지 컴퓨팅 환경인 Raspberry Pi 5 상에서 원활히 동작하도록 기존 모델의 크기, 추론 시간, 품질·보안성을 고려한 최적화에 관한 것이다. 기존의 HiNet 모델의 경량화를 위해 PTQ(Post-Training Quantization)를 적용하여 일부 연산만을 INT(Integer) 8비트로 변환하고, 가역성에 민감한 계층은 FP(Float)32 비트로 유지하여 복원 성능 저하를 최소화하였다. 본 연구에서 제안한 방법을 모델의 경량화, 추론 시간, 품질·보안 부분에 대해서 기존 방식과 비교 평가하였다. 실험 결과, 제안 방식이 기존 방식에 비해 모델 크기는 57.3% 감소하였고, 추론 시간은 320[sec] 단축하였고 CPU 점유율, memory 사용량 또한 각각 51.1%, 24.9% 감소하였다. 품질 부분 측정치인 PSNR(Peak Signal-to-Noise Ratio)과 SSIM(Structural Similarity Index)은 각각 5%, 0.6% 만큼 감소하였다. 보안 부분의 측정치인 AUC(Area Under the ROC Curve)는 보안 성능이 9% 감소하는 결과를 얻었지만 엣지 컴퓨팅 환경인 Raspberry Pi 5에서 원활하게 동작하는 것을 확인하였다.

I. 서론

스테가노그래피(Steganography)와 워터마킹(Watermarking)은 디지털 이미지 내에 시크릿(Secret) 이미지를 삽입하거나 복원하면서도 원본의 가시적 품질을 유지하는 기술로, 저작권 보호와 프라이버시 보장에 중요한 역할을 한다[1]. 그러나 기존의 신경망 기반 접근법들은 주로 GPU가 탑재된 서버 환경에서 구동을 전제로 설계되었다. 메모리·연산 자원이 제한된 엣지 컴퓨팅 환경에서는 동작이 어렵다는 한계가 있다[2]. 본 연구에서는 가역 신경망 구조의 HiNet 모델을 Raspberry Pi 5와 같은 엣지 컴퓨팅에서 동작하도록 경량화하기 위한 양자화 기법인 PTQ(Post-Training Quantization)를 적용하였다. PTQ는 FP32로 학습된 모델을 추가 학습 없이 INT8로 변환해 모델 크기와 메모리 사용을 줄이는 방식이다[3].

II. HiNet

HiNet은 가역 신경망(INN)으로, 은닉(Conceal) 경로 (cover+secret → stego)와 복원(Reveal) 경로 (stego → cover, secret)가 구조적으로 동일하며 같은 파라미터를 사용한다. 이러한 가역성 덕분에 정보 손실을 최소화하고 복원(Reveal) 오차를 줄일 수 있다. HiNet 모델의 개요는 그림 1과 같다.



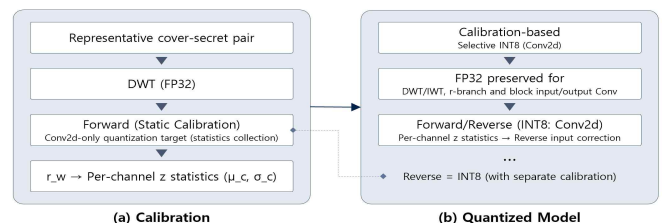
[그림 1] HiNet 전체 구조

III. PTQ(Post-Training Quantization)

엣지 컴퓨팅과 같이 리소스(Resource)가 제한된 환경에서 HiNet 모델을 활용하기 위해서는 모델 경량화가 필수적이다. PTQ는 부동소수점(FP32)으로 표현된 가중치와 연산을 더 낮은 정밀도의 정수(INT8)로 변환하여 모델 크기를 줄이고, 추론 속도를 향상시키는 대표적인 양자화 기법이다. 그러나 연산 효율을 높이는 동시에 은닉·복원 품질 저하가 발생할 수 있는 한계가 존재하며 이를 보완하기 위해 본 연구에서는 파인튜닝과 결합한 PTQ 방식의 양자화 기법을 제안하여 적용하였다.

IV. 제안한 방식

모델의 경량화를 위한 PTQ 과정은 대표 이미지 쌍을 이용한 정적 조정(Static Calibration)을 통해 Conv2d 레이어(Layer)만 FP32에서 선택적으로 INT8로 변환하여 정확도 손실을 최소화하였으며, 제안한 PTQ 과정은 그림 2와 같다. 본 연구에서는 원본 HiNet을 워터마크 데이터셋으로 소규모 미세 조정(Fine-tuning)하여 도메인 적응을 수행한 후, 해당 모델에 PTQ를 적용하였다. 이는 단순 PTQ 대비 정확도 손실을 완화하기 위해 활용된 방식이다. 제안한 PTQ 방식을 대상으로 모델 경량화(크기·메모리), 추론 시간, 은닉·복원 품질(SSIM, PSNR), 보안성(StegExpose ROC-AUC) 지표를 기준으로 비교평가를 수행하였다.



[그림 2] 제안한 PTQ방식

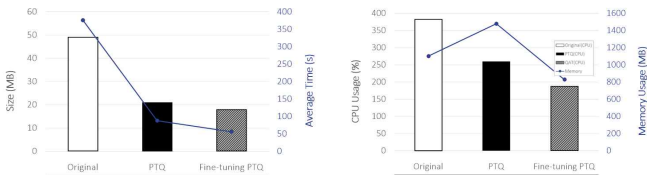
V. 실험 환경 및 성능 비교

실험에 사용된 기기의 사양과 소프트웨어의 버전은 표 1과 같다.

<표 1> 실험 환경 내용

구분	항목	운영체제
Hardware	Device	Raspberry pi 5 Model B Rev1.0
	CPU	ARM Cortex-A76 Quad-core
	RAM	8GB LPDDR4X
	GPU	Broadcom VideoCoreVII
Operating System	OS	Debian GNU/Linux 12
Software	Python	3.11.2
	PyTorch	2.7.4
	TorchVision	0.22.1

본 연구에서는 양자화를 통해 엣지 컴퓨팅 환경에서의 적합성을 검증하기 위하여 모델 경량화, 추론 시간, 은닉/복원 품질·보안성을 중점적으로 평가하였다. 품질 평가는 PSNR과 SSIM을 사용하여 시각적 유사성을 측정하였고, 보안 평가는 AUC 지표를 통해 은닉 이미지의 탐지 난이도를 분석하였다. 제안한 PTQ방식을 적용 결과, 모델 크기와 추론 시간이 각각 57.3%, 85.2% 감소하여 경량화와 연산 효율 향상이 확인되었으며 CPU 점유율, memory 사용량 또한 각각 51.1%, 24.9% 감소하였다. 이러한 결과는 그림 3과 같다.



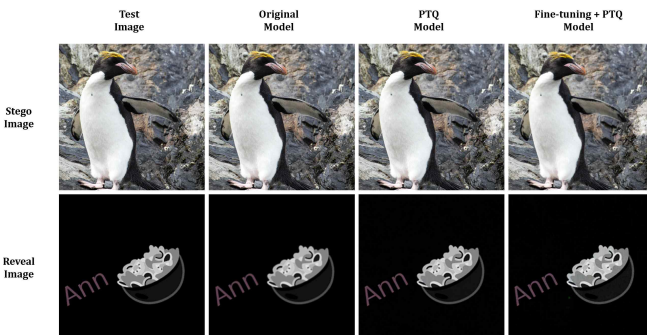
[그림 3] 모델 성능 비교

품질/보안은 은닉/복원 가시성(SSIM, PSNR)과 보안성(AUC)을 FP32와 대비 비교하였다. 가시성은 96% 내로 유지되었고, 결과는 표 2와 같다.

<표 2> PSNR, SSIM 비교

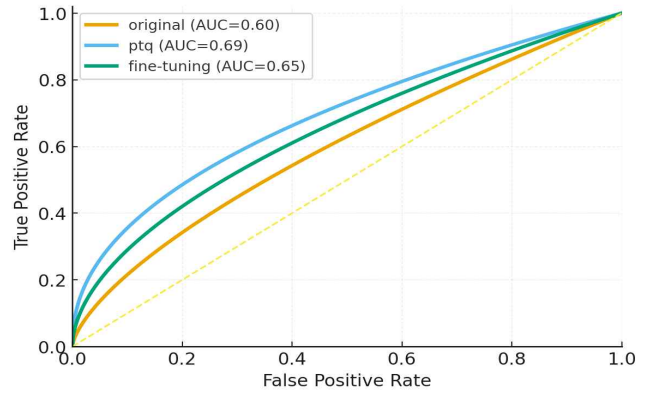
Model	Cover PSNR(dB)	Cover SSIM	Secret PSNR(dB)	Secret SSIM
Original	45.08	0.997	46.20	0.981
PTQ	41.92	0.987	44.86	0.975
Fine-tuning PTQ	<u>42.65</u>	<u>0.991</u>	<u>45.37</u>	<u>0.980</u>

세 모델 모두의 스테고(stego) 이미지의 왜곡은 미미하며, 복원은 양호하게 진행되었다. 결과는 그림 4와 같다.



[그림 4] 각 모델의 이미지 품질 비교 결과

AUC는 공개된 스테가 분석기를 사용해 산출했으며, FP32 대비 PTQ는 -15%, Fine-tuning+PTQ는 -9% 수준의 감소를 보였다. 공개된 스테가 분석기는 [StegExpose/https://github.com/b3dk7/StegExpose.git]를 활용하여 AUC를 측정하였다. 결과는 그림 5와 같다.



[그림 5] 각 모델의 AUC 비교

실험 결과, Fine-tuning+PTQ는 단순 PTQ 대비 우수한 성능을 보였다. PSNR과 SSIM 지표에서 Fine-tuning PTQ는 원본 대비 품질 저하가 거의 발생하지 않았으며, PTQ보다 은닉·복원 품질이 안정적으로 유지되었다. AUC 값에서도 Fine-tuning PTQ가 더 낮은 탐지율을 보여 스테고 탐지에 대한 보안성이 향상되었음을 확인하였다.

VI. 결론

본 연구는 고성능 이미지 은닉 모델인 HiNet을 Raspberry Pi 5와 같은 자원 제약적인 엣지 컴퓨팅 환경에서 실용적으로 운용하기 위한 양자화 기반 경량화 방안을 제시하고 그 효과를 검증하였다. GPU 서버 환경을 전제로 설계된 기존 딥러닝 모델의 한계를 극복하고자 새로운 PTQ 기법을 적용하여 모델 경량화의 최적화를 수행하였다. 특히 PSNR, SSIM과 같은 복원 품질 지표와 AUC 기반 스테고 탐지 저항성에서 모두 우수한 성능을 보여, 엣지 컴퓨팅 환경에서도 실용적 활용 가능성을 높였다. CPU 점유율, 추론 시간, 메모리 사용량이라는 세 가지 핵심 자원에서 모두 균형 잡힌 최적화 효과를 확인하였다. 결론적으로 본 연구는 HiNet 모델의 엣지 컴퓨팅 환경에서의 구동 가능성을 입증했다. 추후 자원 사용의 균형을 맞추는 최적화 연구가 더해진다면 엣지 컴퓨팅 기반의 실시간 디지털 저작권 보호 기술 상용화에 한 걸음 더 다가갈 수 있을 것으로 기대된다.

참 고 문 헌

- [1] J. Jing, X. Deng, M. Xu, J. Wang, and Z. Guan, "HiNet: Deep Image Hiding by Invertible Network," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, pp. 4733-4742.
- [2] B. M. Issac, S. N. Kumar, S. Zafar, K. A. Shakil, and M. A. Wani, "Deep learning steganography for big data security using squeeze-and-excitation with inception architectures," *Scientific Reports*, vol. 15, no. 31193, 2025.
- [3] J. Hasan, "Optimizing Large Language Models through Quantization: A Comparative Analysis of PTQ and QAT Techniques," *arXiv preprint arXiv:2411.06084*, 2024.