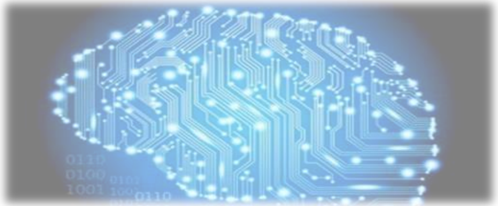
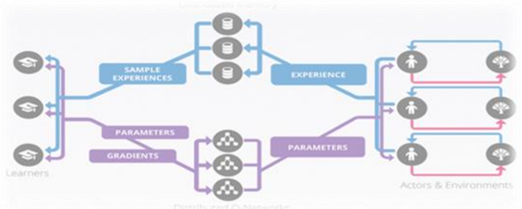




기계학습자동화 연구실

1차 정기 세미나

문아성, 이태원, 윤건일, 이한용

2022.03.22

Outline

- Individual Studies
  - Multimodal Learning Research, A-Seong Moon
  - Stock Price Prediction, Tae-Won Lee
  - 2-Way Inference on Embedded Board (DOOSAN), Geonil Yun
  - Restoration of Homoglyph Attack with BERT, Hanyong Lee

Multimodal Learning Research

A-Seong Moon

TO DO List

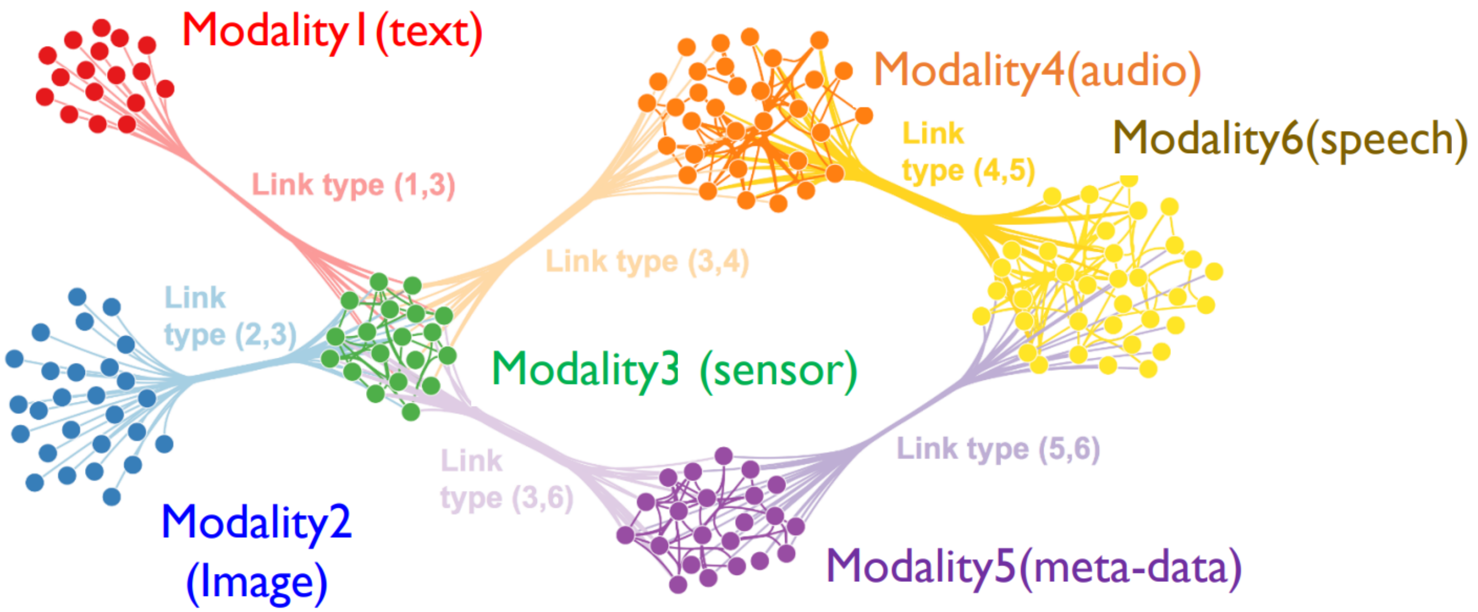
- Last week
  - ☑ Multimodal Text and Image Classification

- This week
  - ☑ Multimodal Image Classification: Image + @
  - ☑ Master's thesis: An efficient neural network specialized for sparse CT Slice images (가칭)

Multimodal Learning Research

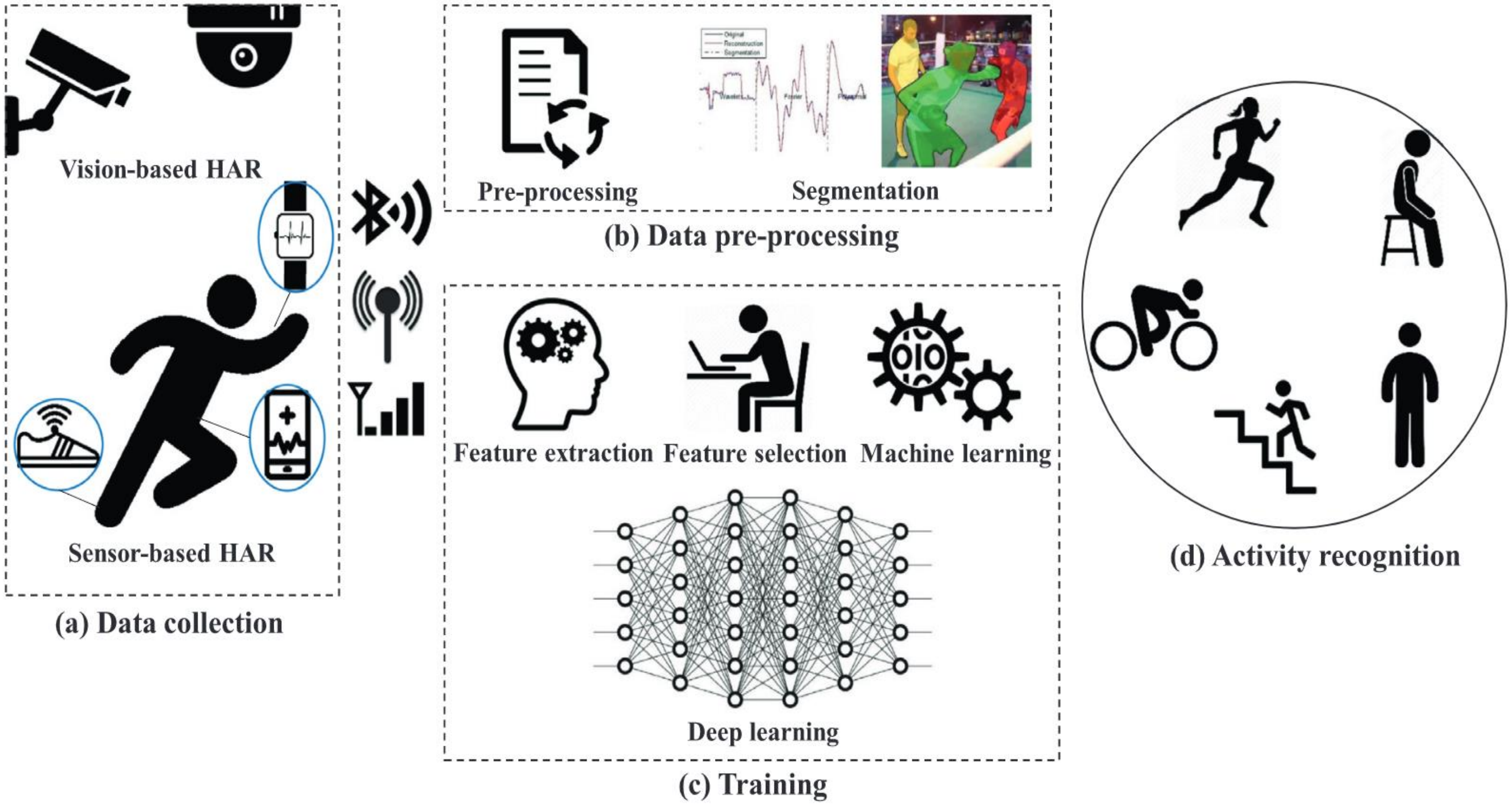
"Multimodal" 이란?

- **Multimodal**: Modality가 여러 개 존재
- **Modality** (양식): 특정 자원으로부터 수집된 데이터 표현 형식
- **Multimodal Learning**: **다양한 형태(Modality)의 데이터**를 사용하여 모델을 학습하는 것



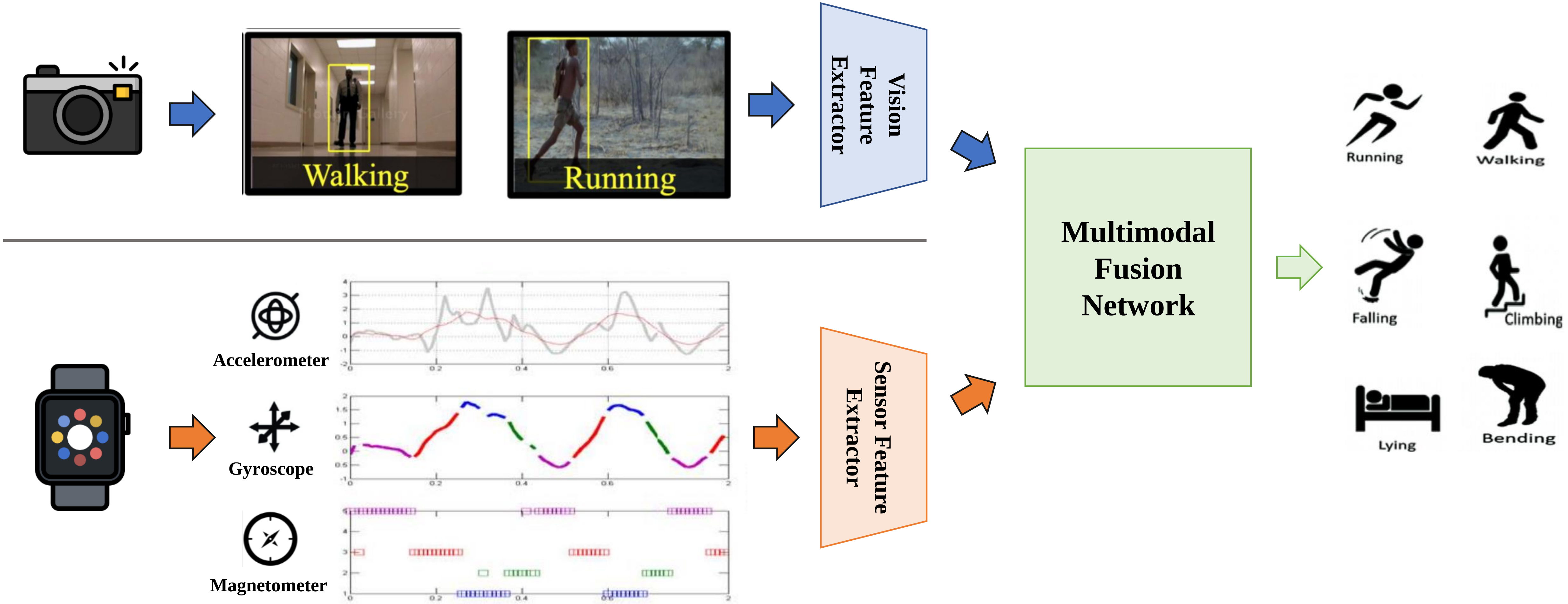
Human Activity Recognition

Identify **human activities** (such as walking, jogging, cycling, etc.)



Multimodal Learning Research

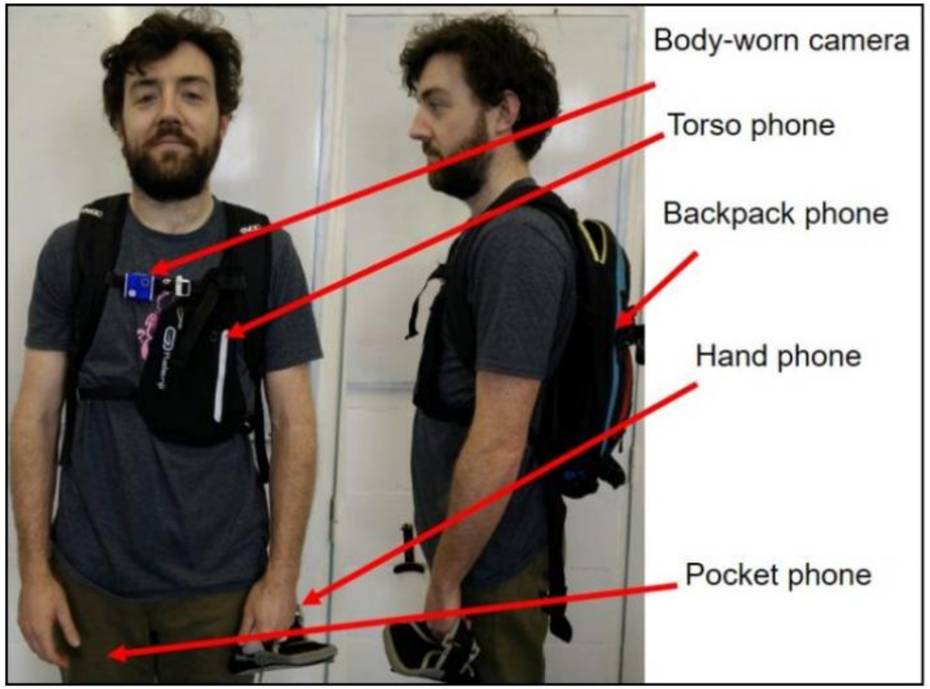
Multimodal Human Activity Recognition



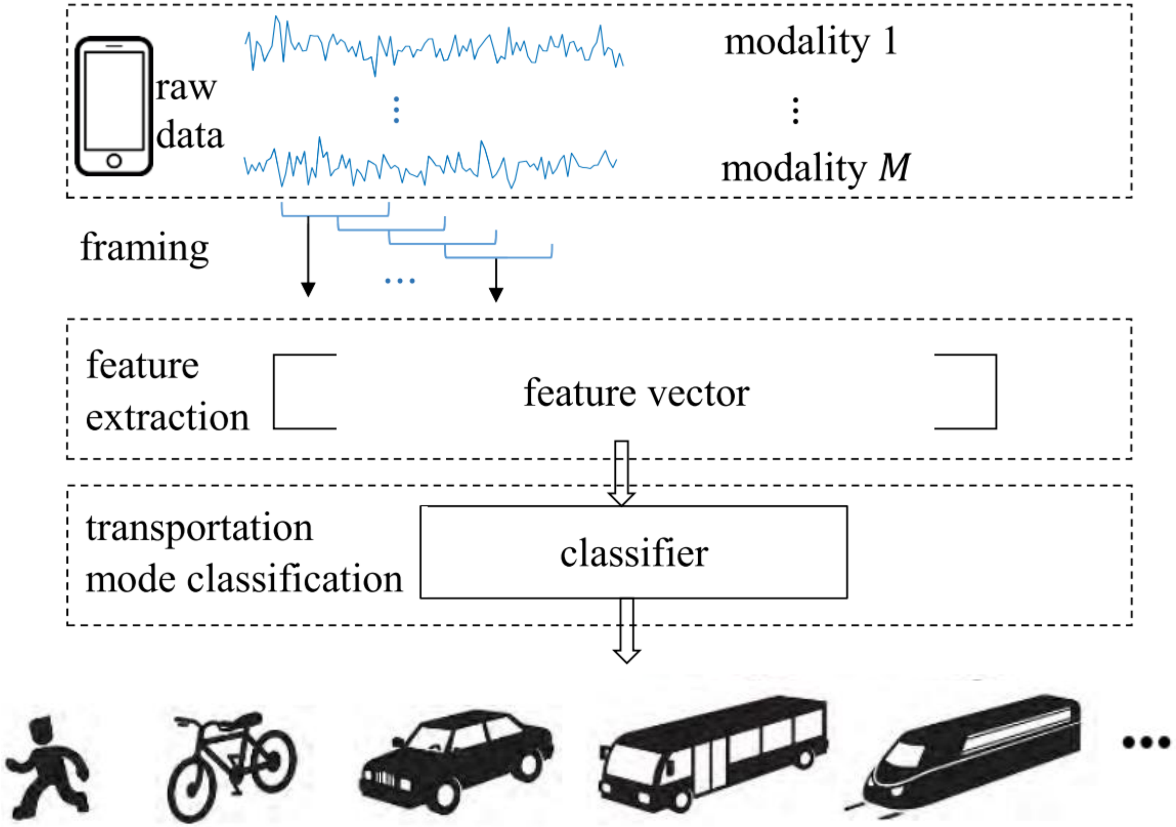
Multimodal Learning Research: *Human Activity Recognition*

Sussex-Huawei Locomotion Dataset, SHL Dataset

To recognize 8 modes of **locomotion and transportation**



A participant wearing the four smartphones
and a camera during data collection



Multimodal Learning Research: *Human Activity Recognition*

SHL Dataset: Multimodal Data

Modality	File	Train (B/T/Hi)	Validation (B/T/Hi/Ha)	Test (Ha)
Accelerometer	Acc_x.txt Acc_y.txt Acc_z.txt	✓	✓	✓
Gyroscope	Gyr_x.txt Gyr_y.txt Gyr_z.txt	✓	✓	✓
Magnetometer	Mag_x.txt Mag_y.txt Mag_z.txt	✓	✓	✓
Linear accelerometer	LAcc_x.txt LAcc_y.txt LAcc_z.txt	✓	✓	✓
Gravity	Gra_x.txt Gra_y.txt Gra_z.txt	✓	✓	✓
Orientation	Ori_w.txt Ori_x.txt Ori_y.txt Ori_z.txt	✓	✓	✓
Pressure	Pressure.txt	✓	✓	✓
Label	Label.txt	✓	✓	✕

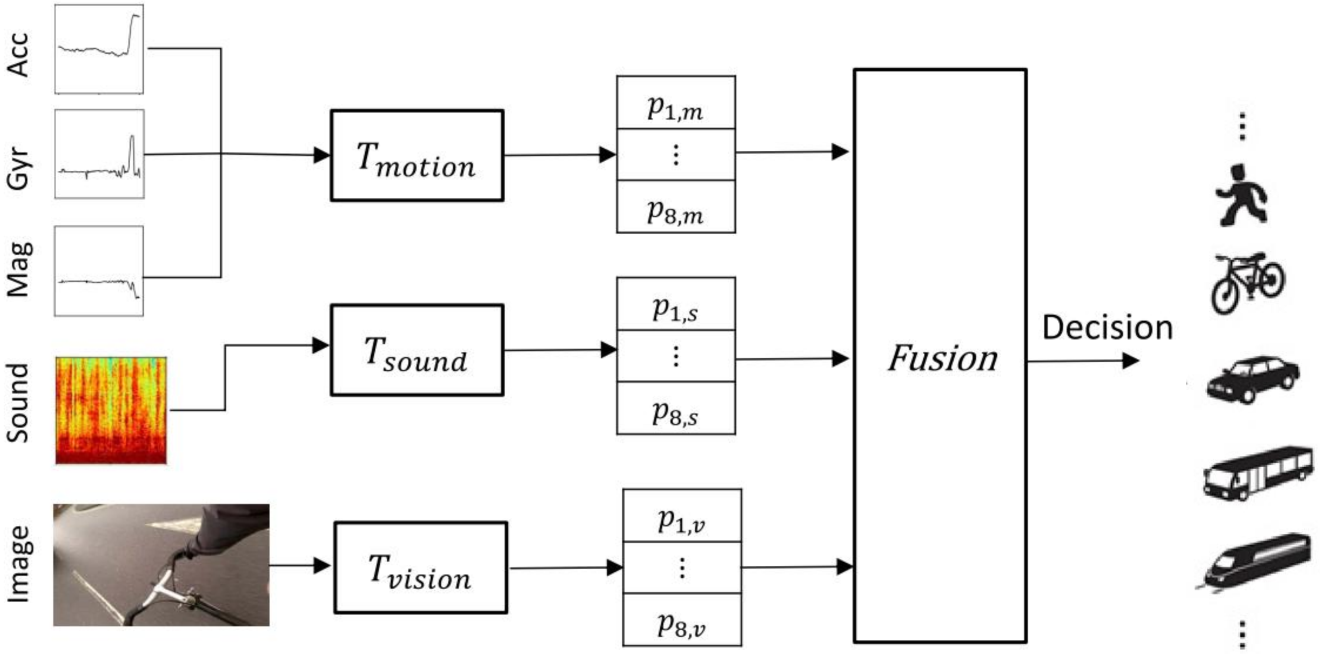
Data files provided by the SHL recognition challenge.
Position: B - Bag; T - Torso; Hi - Hips; Ha - Hand.

A participant filmed in real life with a body cam

Multimodal Learning Research: *Human Activity Recognition*

SHL Dataset: Multimodal Learning

Richoz, Sebastien, et al. "Transportation mode recognition fusing wearable motion, sound, and vision sensors." *IEEE Sensors Journal* 20.16 (2020): 9314-9328.



Proposed pipeline of multimodal fusion for transportation mode recognition

Modality	motion	sound	vision
F1 [%]	79.4	82.1	72.8

F1-Score of Mono-modal Classifier

Method	motion sound	sound vision	motion vision	motion vision sound
Ensemble Decision [Product]	91.5	91.0	89.2	94.5
Adaptive Fusion [Neural Network]	90.7	90.4	88.3	94.6

F1-Score of Multimodal Classifier

Multimodal Learning Research: *Vision Techniques*

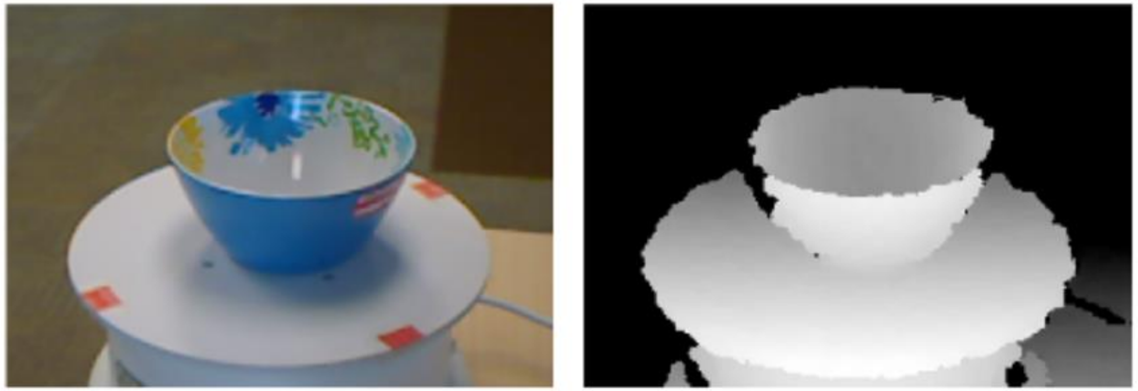
RGB Image and Vision Sensors

Modality

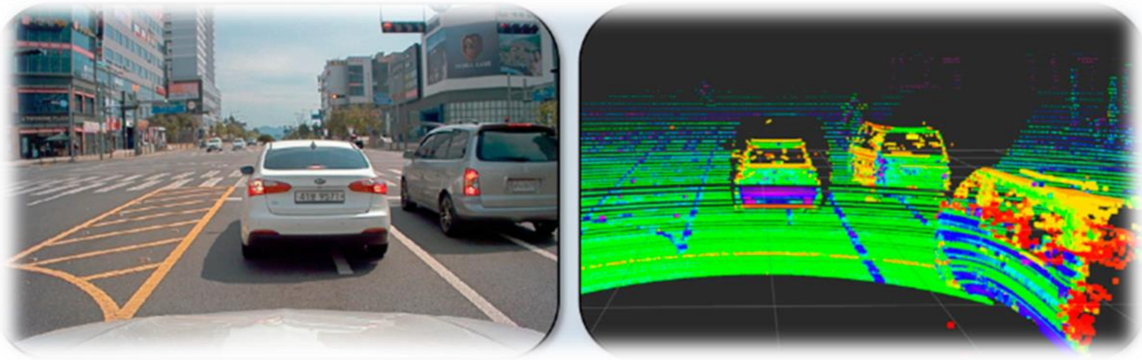
RGB, RGB-D, LiDAR Point Cloud, Radar, etc.

Task

Object Detection, Depth Estimation, Semantic Segmentation, etc.



RGB Image and RGB-D Image



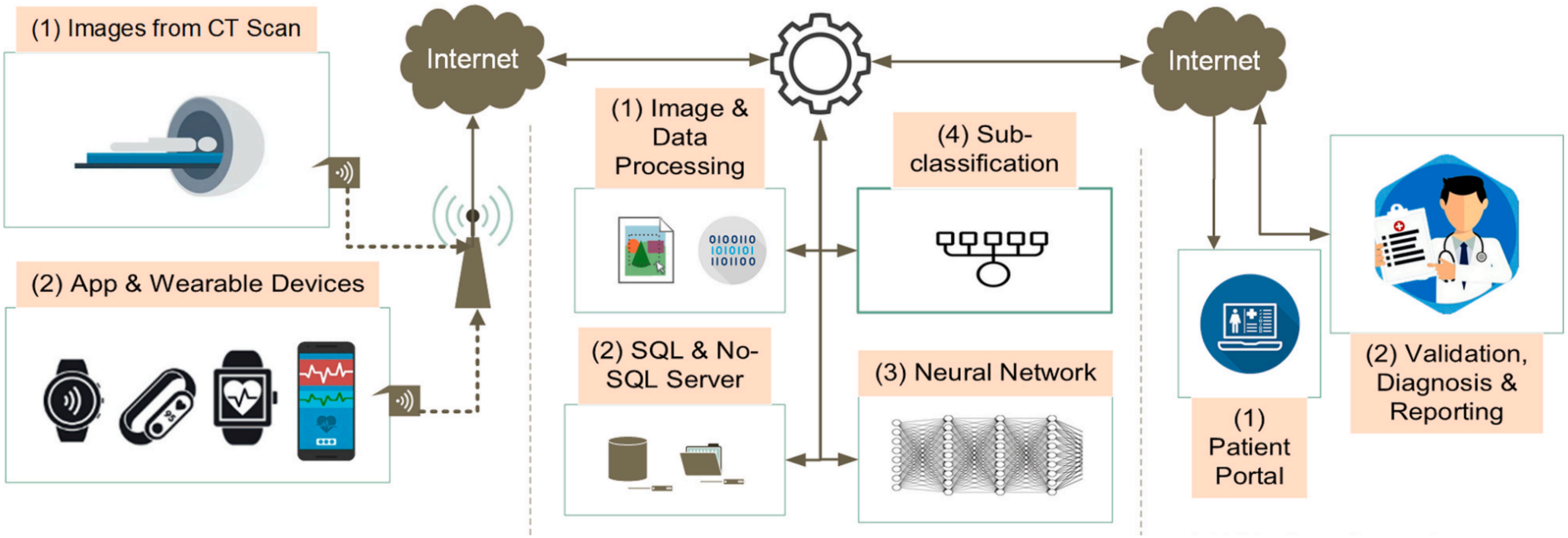
RGB Image and LiDAR data

Master's thesis: An efficient neural network specialized for sparse CT Slice images

연구 배경

최근 Medical IOT 기술을 이용한 원격진료 과정에서 CT, MRI 등 원격의료기기를 통해 데이터 전송 및 재구성

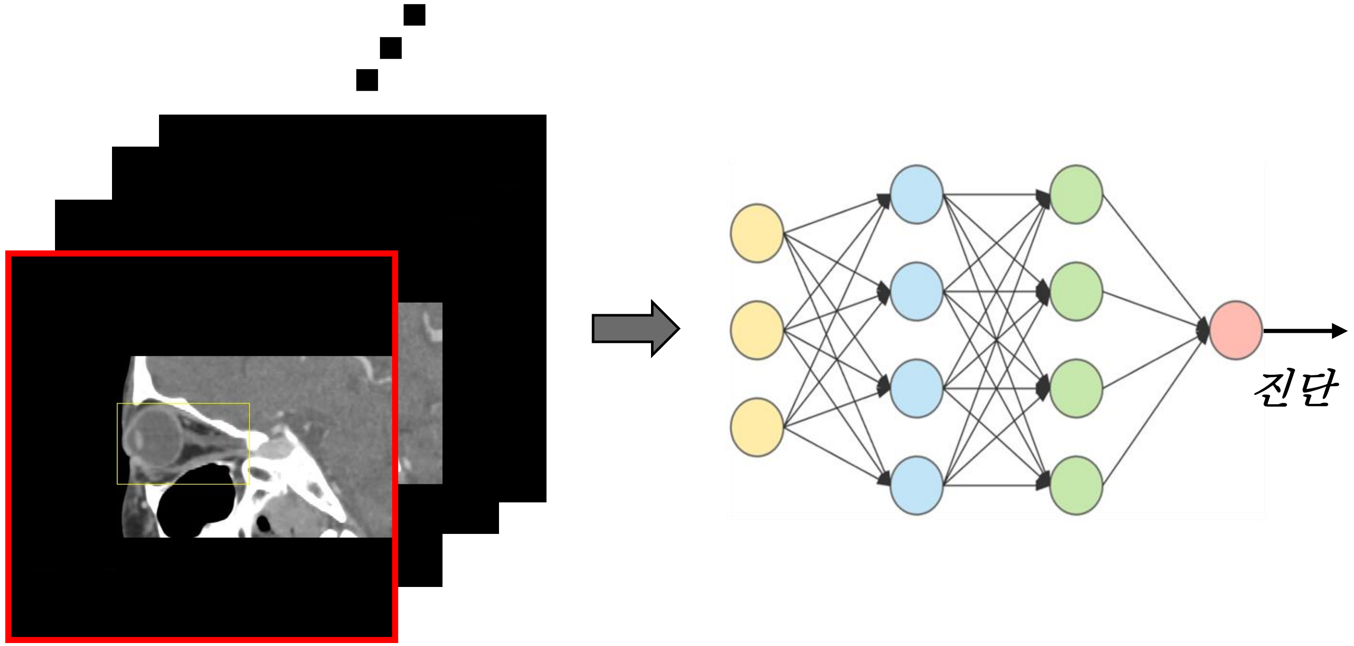
➡ 원활한 원격 실시간 진단을 위해 **비용이 적고 빠른 데이터 분석이 요구**



연구 배경

희소 CT 이미지 영상은 2D 시퀀스 이미지로 구성

환자 1명에 대해 많은 CT 영상으로 구성되어 있지만,
진단하는데 필요한 데이터는 극히 적음



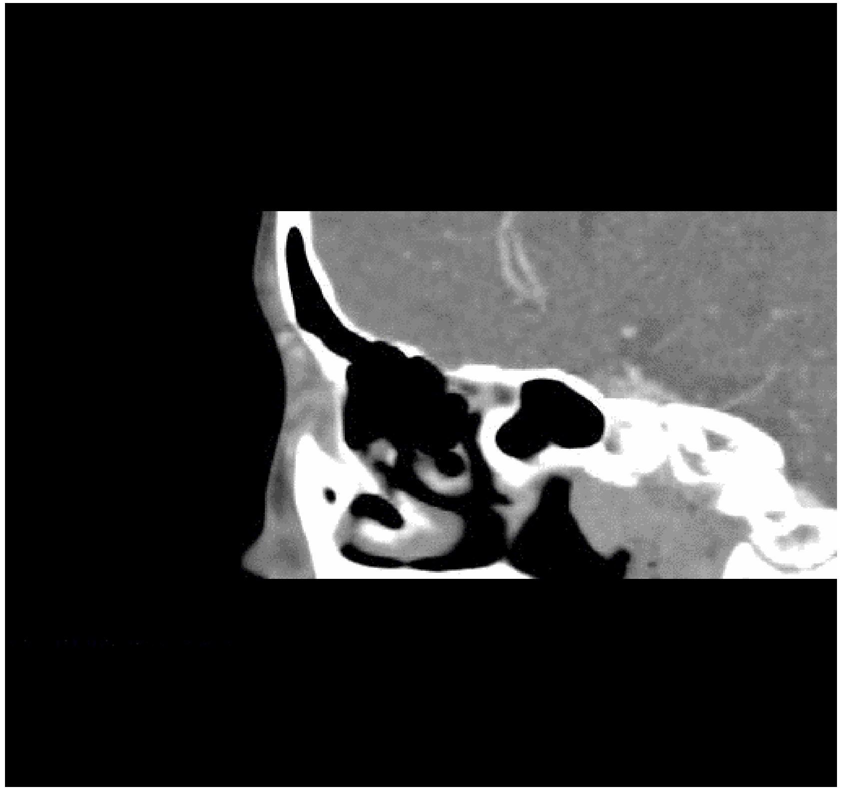


그림 1: Sagittal-view CT 이미지 영상

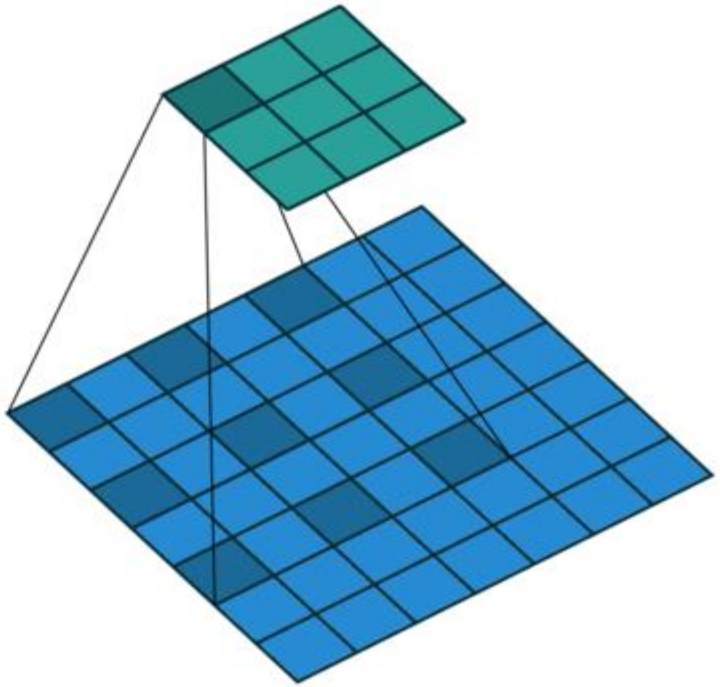
관련 연구 [1] : 효율적인 인공신경망

- 스마트폰이나 임베디드 시스템과 같이 자원이 한정된 공간에서 딥러닝을 적용하기 위함

- 효율적인 컨볼루션 레이어

  Spatial wise: *Dilated convolution*

  Channel wise: *Point-wise convolution*, *Group convolution*



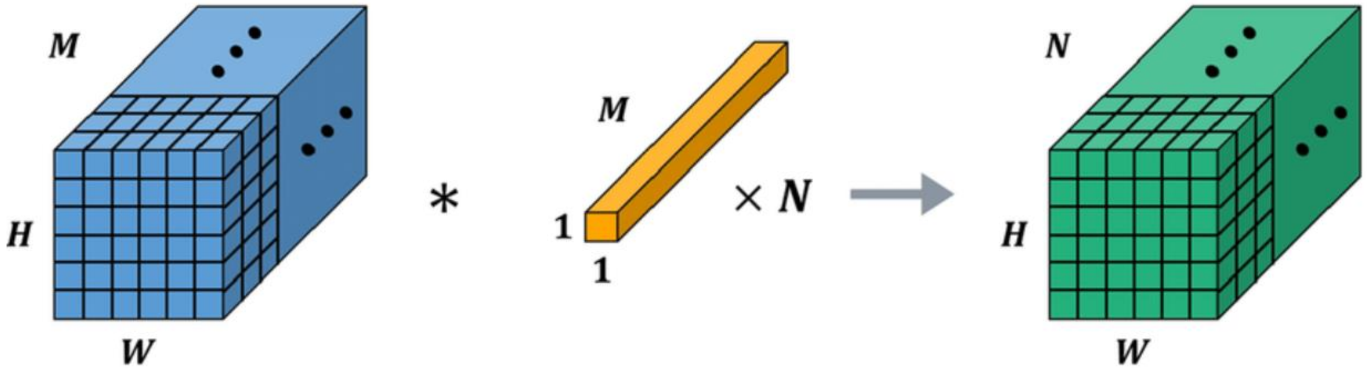
관련 연구 [1] : Pointwise Convolution Layer

Channel-wise Convolution

Kernel size: (1 x 1 x C)

많은 채널 입력 이미지를 더 적은 채널 이미지로 압축 가능

Channel compression trade-off: Operation speed ⟺ Information loss

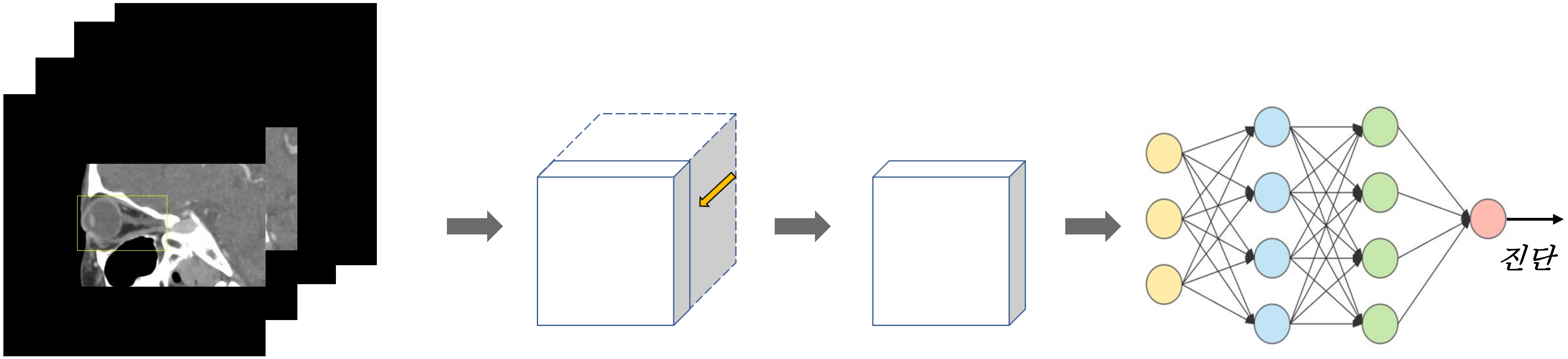


Master's thesis: An efficient neural network specialized for sparse CT Slice images

Early Compression of Sparse CT Slice Images

- CT 영상 각각의 이미지가 입력 데이터의 채널에 매핑
- 진단하는데 불필요한 채널은 적은 값으로 구성되어 계산 결과에 영향을 미치지 않음

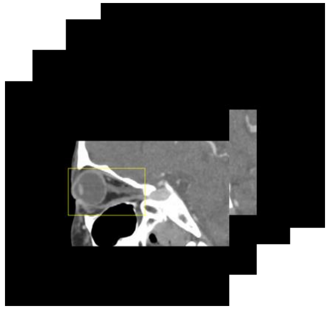
➡ Pointwise Convolution을 사용하여 **중요한 정보 손실 없이 작은 네트워크로 압축이 가능**하면서 성능을 유지



Sparse CT Slice images

Master's thesis: An efficient neural network specialized for sparse CT Slice images

Model Architecture



Inputs

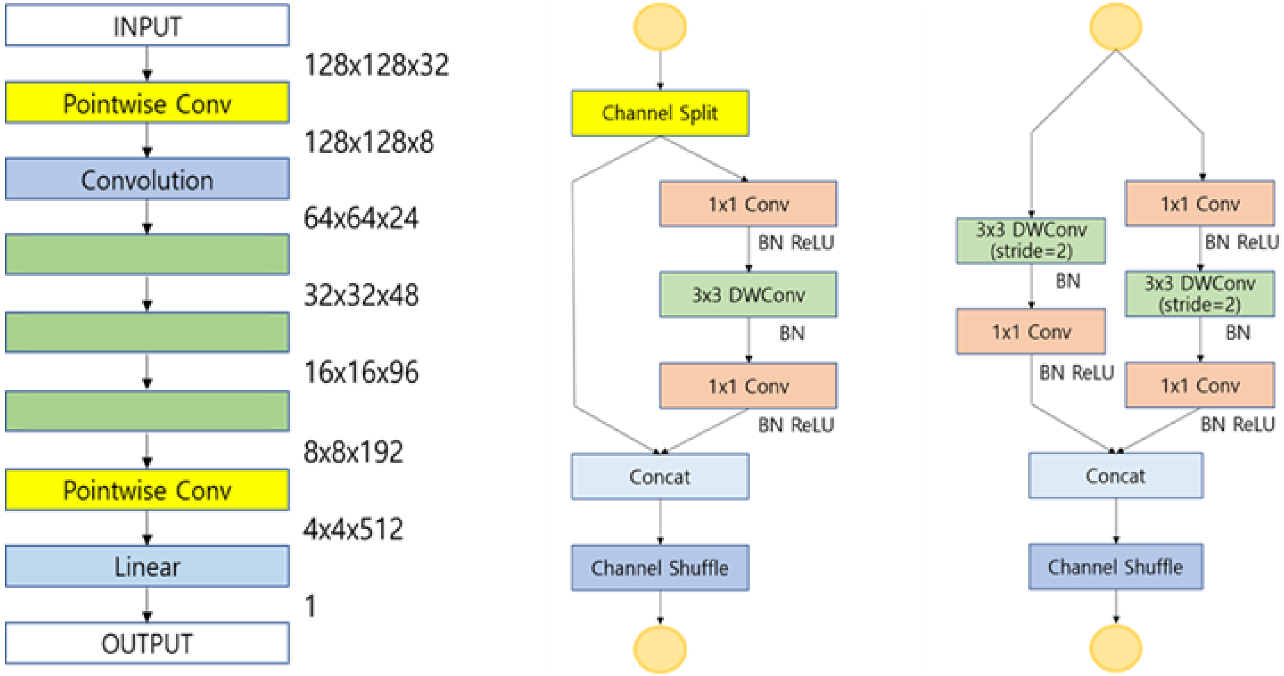
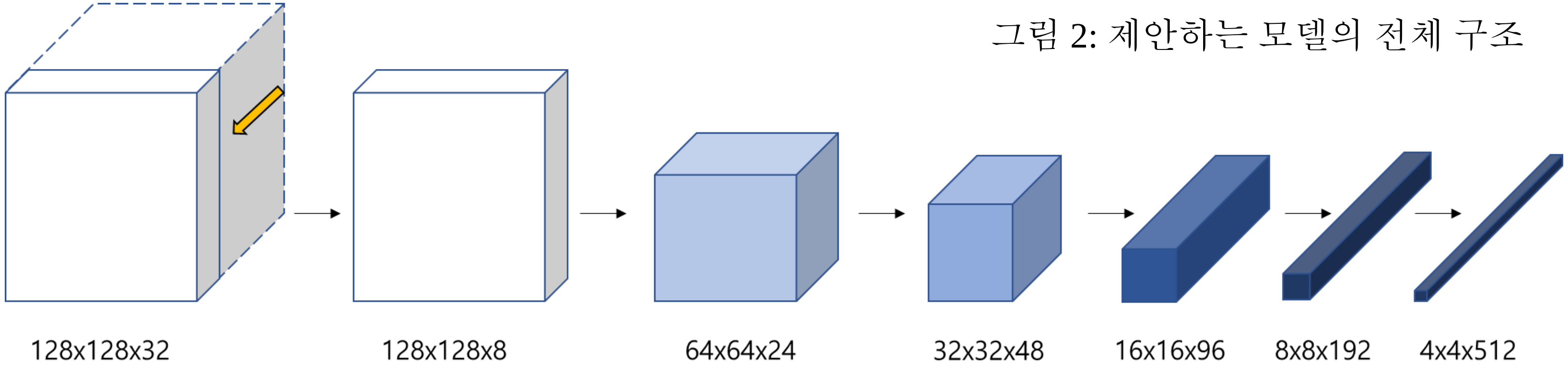


그림 2: 제안하는 모델의 전체 구조



Master's thesis: An efficient neural network specialized for sparse CT Slice images

Experiment settings

Disease name: Thyroid-associated ophthalmopathy

- ***Dataset***
  - 261 patient
  - active : 129 people, inactive : 132 people
- ***Input image***
  - Orbital Sagittal 2D CT images *(Consists of 32 slices per patient)*
- ***Train & Test set***
  - 8,352 datasets
  - Train Set : 209 people (6688 sheets)
  - Test Set: 52 people (1664 sheets)

Master's thesis: An efficient neural network specialized for sparse CT Slice images

Experiment results

Table 1: Performance of the classification models

Model	Parameters (M)	MACs (M)	AUC	Accuracy	Sensitivity	Specificity
Resnet	23.60	1717.7	0.86±0.039	0.77±0.050	0.78±0.085	0.77±0.100
GoogleNet	5.69	864.5	0.85±0.061	0.77±0.058	0.78±0.092	0.76±0.096
ShuffleNet-v2	1.26	74.5	0.91±0.042	0.83±0.049	0.82±0.081	0.84±0.079
Proposed Model	0.24	21.3	0.90±0.039	0.81±0.053	0.81±0.099	0.80±0.071

AUC, area under the curve
MACs, Multiply Accumulate operation per second

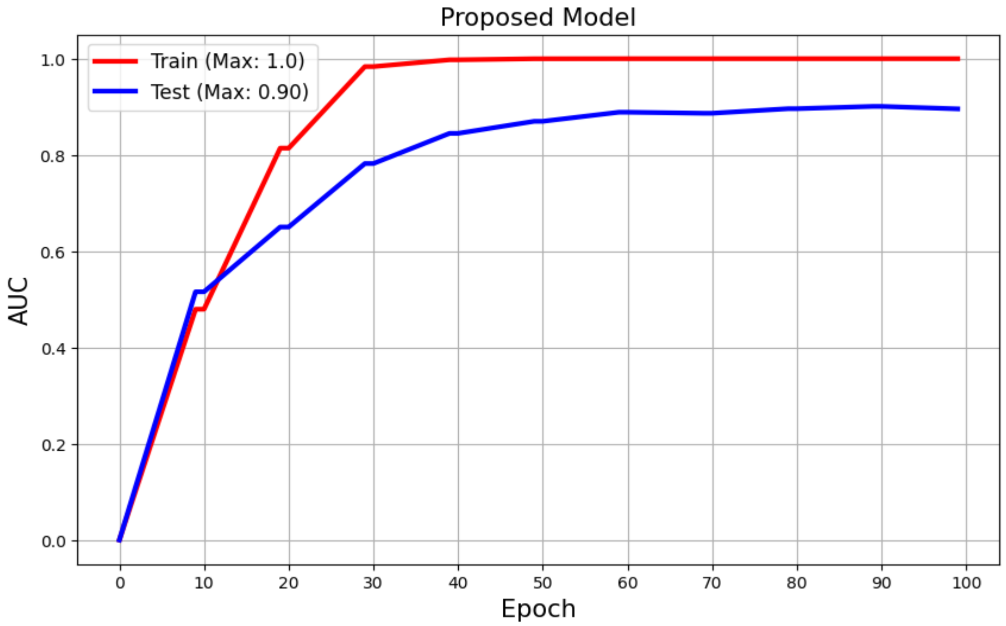


Fig 3- The learning curves of the proposed Neural Network

Conclusion

Problem

Overwhelmed by useless CT slices, resulting in wasted calculations.

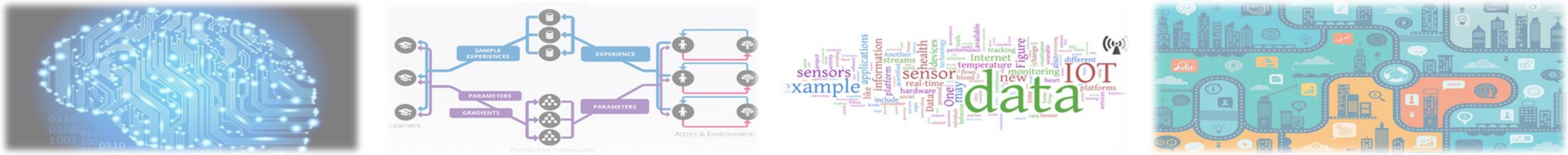
Objective

Learning from sparse data as quickly as possible

Performance

Accuracy: Similar to ShuffleNet-v2 *(AUC: 90%)*

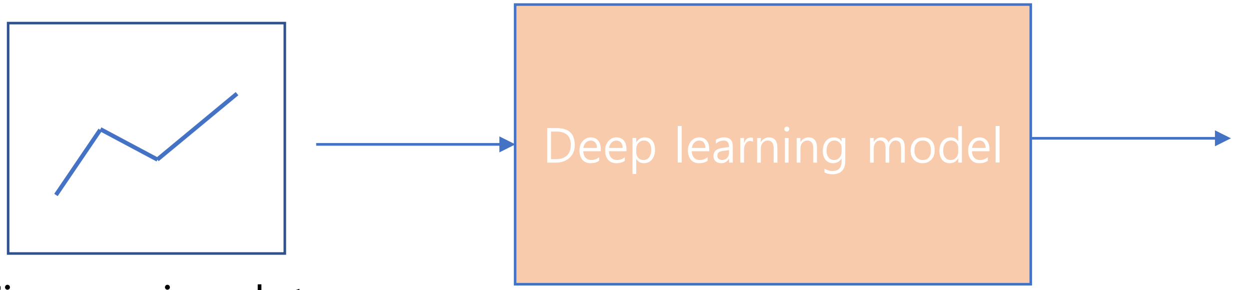
Efficiency: **3.5x speed improvement** compared to ShuffleNet-v2 *(MACs: 74.5 -> 21.3 M)*



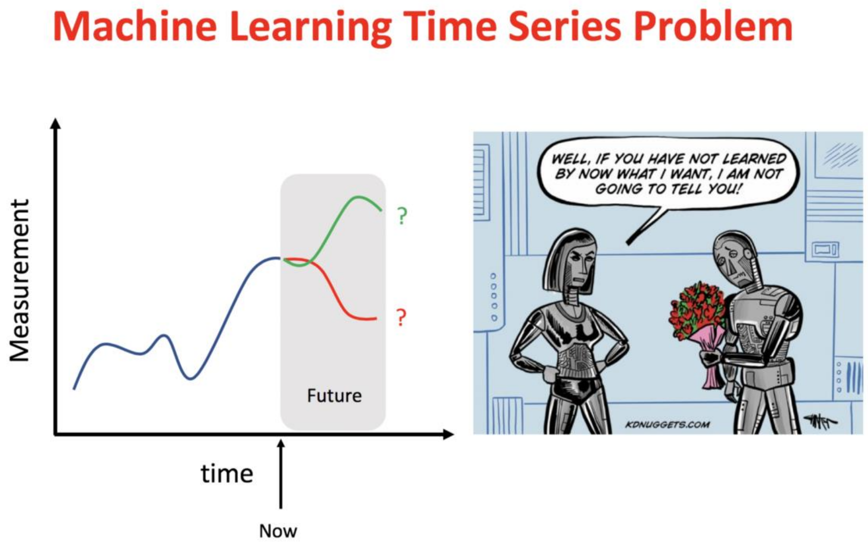
Stock price prediction

Tae-Won Lee

Stock price prediction



<Time series data>



- Time series prediction은 **주가 예측, 수요 예측** 등의 문제에서 이용되는 중요한 문제임.

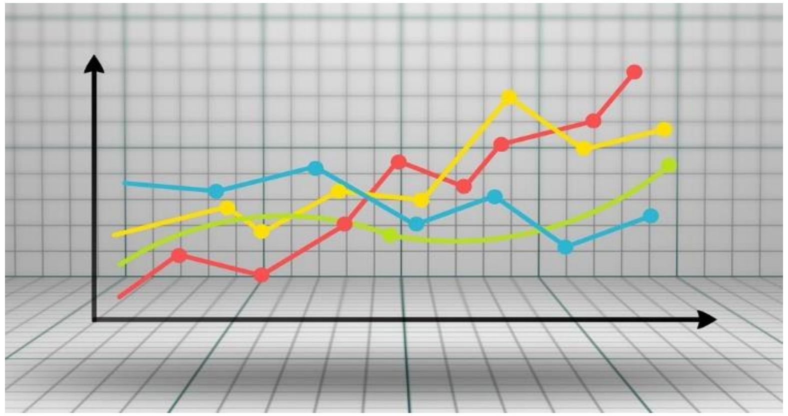
- 딥러닝을 활용하여 시계열 데이터의 미래 값을 예측

Stock price prediction

- 시계열 예측의 종류

- Univariate time series
  - 하나의 time-dependent variable
  - 이전의 정보(Seasonality, Tendency, cycle)만을 이용해 다음 시점의 예측을 진행

- Multivariate time series
  - 두개 이상의 time-dependent variables
  - 이전의 정보를 이용하는 것에 더하여
  - 연관성이 있다고 판단되는 time series data간의 Correlation을 추가적으로 이용할 수 있음.



< Multivariate time series 의 예시>

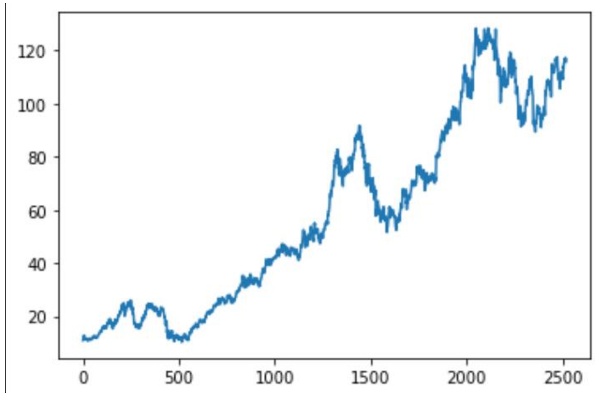
Stock price prediction

- KDD 17 (2007-01-01~2016-12-31)
  - Data 개수 : 2518
  - Feature : 6개 (Open, High, Low, Close, Volume, Adj Close)
  - Data description (AAPL, 애플)

	Open	High	Low	Close	Volume	Adj Close
count	2518.000	2518.000	2518.000	2518.000	2.518000e+03	2518.000
mean	61.547	263.469	257.844	260.719	1.330721e+08	58.142
std	36.273	176.835	173.889	175.363	9.902299e+07	35.661
min	11.341	82.000	78.200	78.200	1.142440e+07	10.175
25%	26.130	114.522	112.102	113.459	6.200998e+07	23.765
50%	57.858	181.624	175.489	179.080	1.067185e+08	53.027
75%	94.639	403.920	395.595	400.277	1.751029e+08	90.270
max	134.460	705.070	699.569	702.100	8.432424e+08	128.520

* 하루를 기준으로 데이터가 추출 됨

  - Data Graph(AAPL[‘Adj Close’])



* 수정종가 (Adj Close): 주식가격을 분석에 적용하기 위해 필수적으로 사용되는 feature

Stock price prediction

- 주식 예측을 위한 Deep learning Models using Multivariate time series data
  - CNN-BiLSTM-AM

    - CNN

    - Bidirectional LSTM

    - Attention Mechnism

  - AdvLSTM (Adversarial Training)

    - Attention LSTM

    - Adversarial Training

  - DTML (Data-Axis Transformer with Multi-Level Contexts)

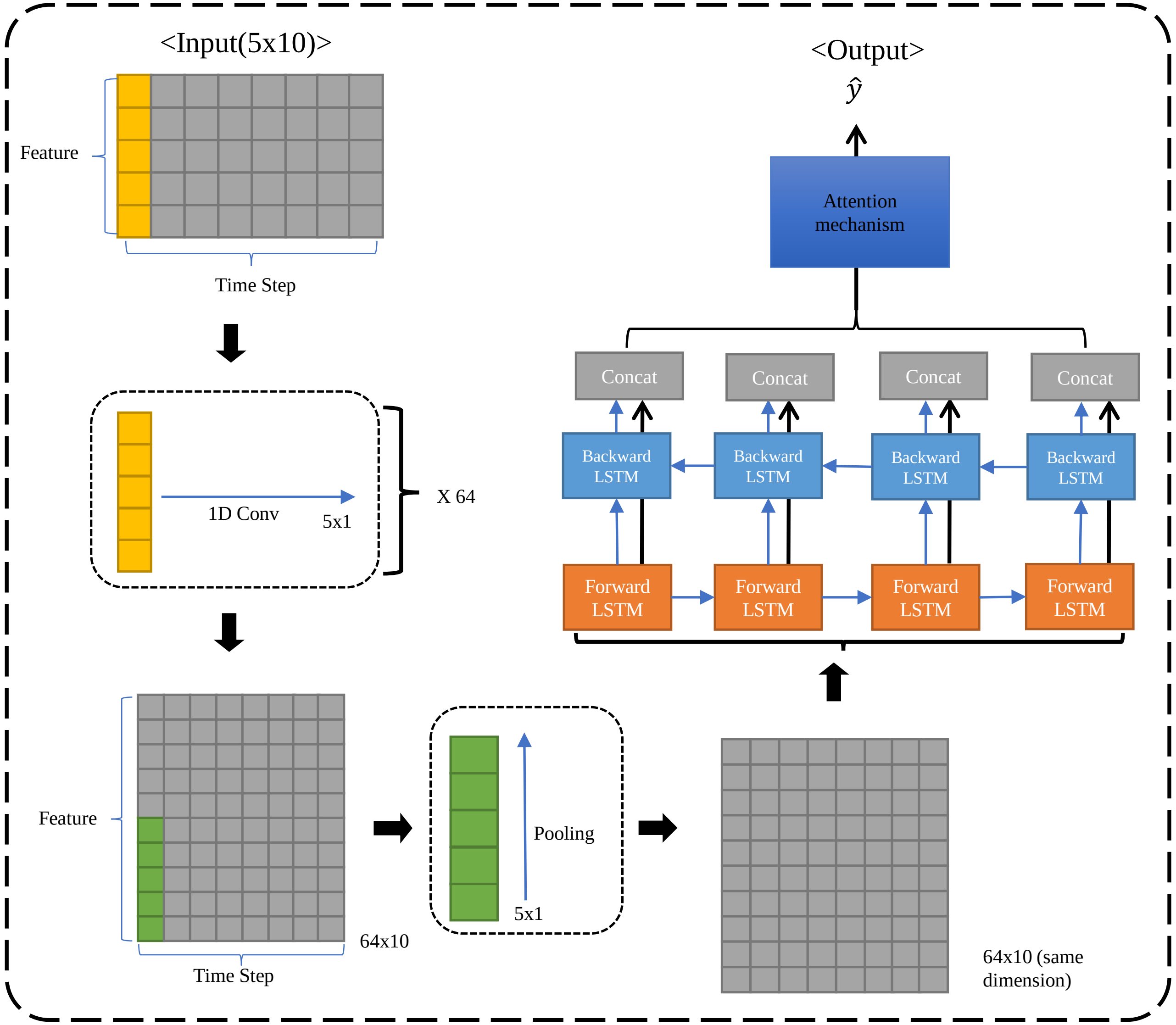
    - Attention LSTM

    - Transformer

    - 다양한 주식 종목 간의 상관관계를 학습

Stock price prediction

- **CNN-BiLSTM-AM**



- CNN을 사용하여 주식의 Feature를 학습하여 LSTM의 Input을 사용
- 시계열의 Time Dependency를 효과적으로 학습할 수 있는 양방향(bi Directional) LSTM
- LSTM에서 하나의 값을 예측하려고 할 때 일어날 수 있는 손실을 방지하기 위해 과거의 정보를 효과적으로 이용할 수 있는 Attention mechanism 이용

Stock price prediction

- **AdvLSTM**

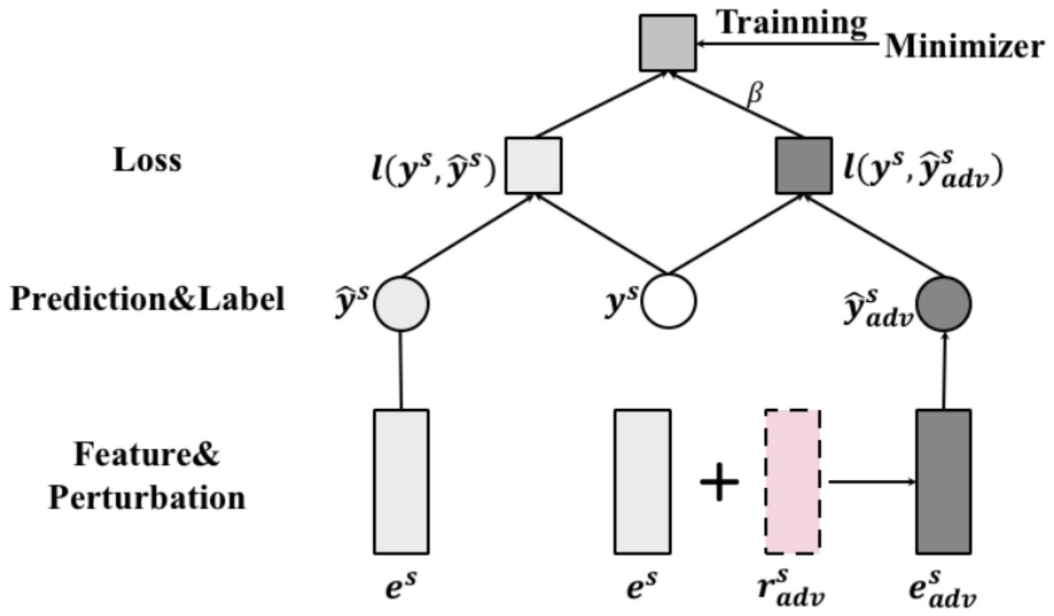
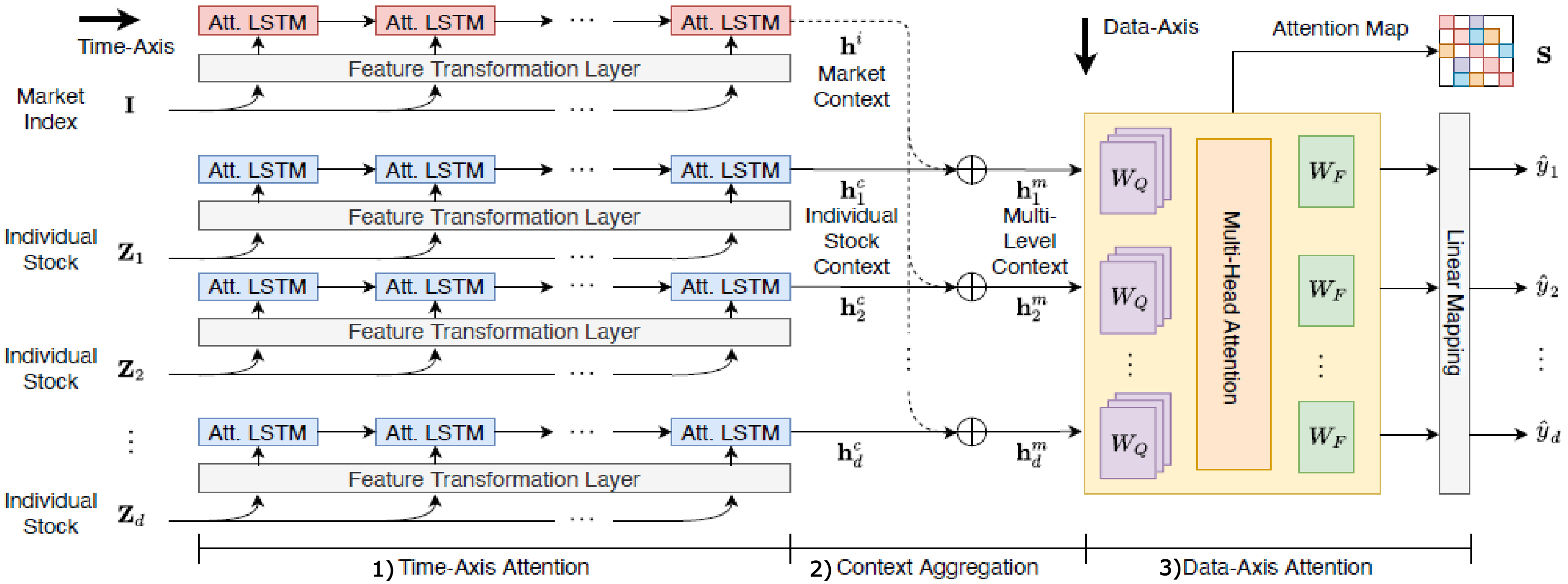


Figure 3: Illustration of the *Adversarial Attentive LSTM*.

- 금융 시계열 데이터는 시간에 따라 임의로 변하는 특성 때문에 학습 과정에서 Overfitting이 빈번하게 발생
- Adversarial Training 방법을 Model에 적용
- 아주 작은 값인 Perturbation을 생성하여 **overfitting을 방지함**

Stock price prediction

- **DTML**



- 전체 모델 구조는 크게 3가지로 나뉨

1) Time-Axis Attention -> 시계열 데이터의 feature를 추출
2) Context Aggregation -> 추출된 feature를 Matrix 형태로 Concatenate
3) Data-Axis Attention(Transformer) -> 서로 다른 종목 간의 <u>**상관관계 학습**</u>

TO DO list

- 지난주

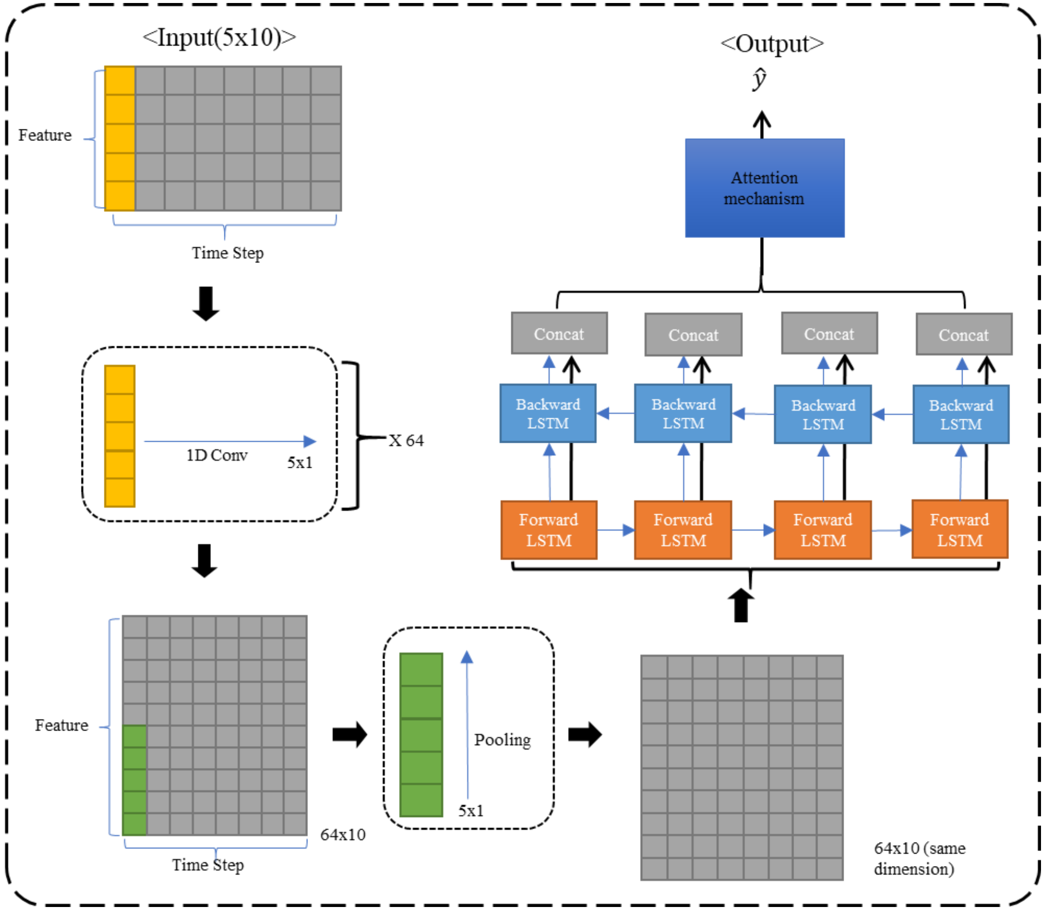
 - 논문의 모델에서 Technical Indicator를 추가 입력으로 넣은 모델 실험

- 이번주

 - 논문에서 특정 구조를 제외 시킨 후 실험

Comparison results

- CNN-BiLSTM-AM 모델에서 특정 구조 제거



- 논문에서 저자는 CNN Module을 시계열 데이터에 사용하는 이유를 찾아보기 어려움
- BiLSTM만으로 시계열 데이터의 Time dependency를 효과적으로 학습 가능

"CNN Module 제거 후 실험"

Comparison results

- 순위 평균 (KDD17 Datasets)

** 순위 평균: Appendix 성능 테이블 기반*

Model	Accuracy 순위 평균
DTML (-correlation module)	3.3
DTML [2]	(실험 예정)
AdvLSTM [7]	3.3
CNN-BiLSTM-AM (original) [8]	2.88
CNN-BiLSTM-AM+Technical Indicator	2.8
BiLSTM-AM+Technical Indicator ***(Proposed)***	**2.5**
BiLSTM-AM+Technical Indicator + (Correlation module)	(실험 예정)

- CNN을 제거한 BiLSTM-AM+ Technical Indicator 에서 가장 높은 성능을 보임 (2.88 -> 2.5)
- 이전 실험에서 Technical Indicator 를 Input에 추가한 후 실험 진행하여 소폭 높아진 정확성 확인 (2.88 -> 2.8)
- DTML구조의 경우 이전 실험에서 종목간 상관관계를 학습하는 모듈을 제외하여 구현

=> 추가 실험을 통해 종목간 상관관계 학습 성능 분석

Comparison results

- 향후 진행방향
  - Model
    - BiLSTM-AM+Technical Indicator 구조가 현재까지 가장 좋은 결과를 보임 (순위평균: 2.5)
    - 종목간 상관관계 구조를 학습하지 않은 DTML을 완전히 구현 후
    - 성능 향상된 BiLSTM-AM+TI 모델에 종목간 상관관계를 학습시키는 모듈을 추가하여 두 가지 모델을 비교 분석
  - Data
    - 현재 실험중인 KDD17 Dataset은 다른 논문에서도 성능 향상 폭이 적음
    - 다른 논문에서 앞선 KDD18 Dataset보다 성능향상 폭이 크다고 알려진 ACL18 Datasets에 대한 추가 실험 분석

Comparison results

- 순위 평균 (ACL18 Datasets)

model	순위 평균
DTML (-correlation module)	(실험 예정)
DTML [2]	(실험 예정)
AdvLSTM [7]	(실험 예정)
CNN-BiLSTM-AM [8]	(실험 예정)
CNN-BiLSTM-AM+Technical Indicator	(실험 예정)
BiLSTM-AM+Technical Indicator (Proposed)	(실험 예정)
BiLSTM-AM+Technical Indicator + (Correlation module)	(실험 예정)

Appendix

Experiment Setting

- KDD 17 (2007-01-01~2016-12-31)

  - **주식 데이터 코드 목록** : 'AAPL', 'AMZN', 'BA', 'BAC', 'BHP', 'BRK-B', 'CHL', 'CMCSA', 'CVX', 'D', 'DCM', 'DIS', 'DOW', 'DUK', 'EXC', 'GE', 'GOOGL', 'HD', 'INTC', 'JNJ', 'JPM', 'KO', 'MA', 'MMM', 'MO', 'MRK', 'MSFT', 'NGG', 'NTT', 'NVS', 'ORCL', 'PEP', 'PFE', 'PG', 'PTR', 'RDS-B', 'RIO', 'SO', 'SPY', 'SYT', 'T', 'TM', 'TOT', 'UNH', 'UPS', 'VALE', 'VZ', 'WFC', 'WMT', 'XOM', **총 50개.**

Experiment Setting

- ACL 18 (2014-01-01~2015-12-31)

- **주식 데이터 코드 목록** : 'AAPL', 'ABB', 'ABBV', 'AEP', 'AGFS', 'AMGN', 'AMZN', 'BA', 'BABA', 'BAC', 'BBL', 'BCH', 'BHP', 'BP', 'BRK-A', 'BSAC', 'BUD', 'C', 'CAT', 'CELG', 'CHL', 'CHTR', 'CMCSA', 'CODI', 'CSCO', 'CVX', 'D', 'DHR', 'DIS', 'DUK', 'EXC', 'FB', 'GD', 'GE', 'GOOG', 'HD', 'HON', 'HRG', 'HSBC', 'IEP', 'INTC', 'JNJ', 'JPM', 'KO', 'LMT', 'MA', 'MCD', 'MDT', 'MMM', 'MO', 'MRK', 'MSFT', 'NEE', 'NGG', 'NVS', 'ORCL', 'PCG', 'PCLN', 'PEP', 'PFE', 'PG', 'PICO', 'PM', 'PPL', 'PTR', 'RDS-B', 'REX', 'SLB', 'SNP', 'SNY', 'SO', 'SPLP', 'SRE', 'T', 'TM', 'TOT', 'TSM', 'UL', 'UN', 'UNH', 'UPS', 'UTX', 'V', 'VZ', 'WFC', 'WMT', 'XOM', **총 87개.**

Comparison results

- Accuracy (Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
AAPL		0.52031	0.47656	0.48281	0.47500	0.50469
AMZN		0.51250	0.53125	0.49688	0.52031	0.51719
BA		0.50625	0.51563	0.52188	0.53438	0.50938
BAC		0.51563	0.50781	0.48438	0.50938	0.47500
BHP		0.47813	0.50000	0.48125	0.48594	0.49688
BRK-B		0.47188	0.50000	0.49219	0.50156	0.51094
CHL		0.52344	0.50781	0.50938	0.48750	0.54531
CMCSA		0.49063	0.48750	0.52031	0.51406	0.52500
CVX		0.48125	0.49688	0.50313	0.50469	0.48438
D		0.51094	0.50313	0.52813	0.50625	0.52500
DCM		0.52656	0.48438	0.48906	0.53594	0.50625
DIS		0.48750	0.51094	0.51250	0.54219	0.50156
DOW		0.50000	0.48281	0.46406	0.47031	0.49688
DUK		0.48281	0.47344	0.55469	0.52969	0.53125
EXC		0.49531	0.46875	0.50781	0.50781	0.50781
GE		0.51563	0.52188	0.50469	0.51250	0.50156
GOOGL		0.52969	0.50938	0.52813	0.52344	0.48906
HD		0.50469	0.52813	0.52031	0.51094	0.52344

Comparison results

- Accuracy(Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
INTC		0.51094	0.48594	0.53125	0.51563	0.49375
JNJ		0.52500	0.48281	0.49219	0.51719	0.52031
JPM		0.50156	0.50313	0.50625	0.47813	0.50313
KO		0.47344	0.47969	0.52344	0.52344	0.49063
MA		0.51250	0.49219	0.50156	0.51250	0.54688
MMM		0.47969	0.51250	0.46875	0.49375	0.50469
MO		0.48906	0.51250	0.55469	0.53281	0.52344
MRK		0.49375	0.49375	0.49844	0.51875	0.50469
MSFT		0.53438	0.49531	0.51250	0.52031	0.52344
NGG		0.53750	0.51563	0.51406	0.51563	0.51875
NTT		0.56719	0.51563	0.49063	0.49531	0.50000
NVS		0.49375	0.50781	0.51250	0.53281	0.52188
ORCL		0.50938	0.50469	0.52969	0.48438	0.54375
PEP		0.48750	0.50313	0.48906	0.50000	0.50625
PFE		0.48594	0.47813	0.50625	0.48281	0.49531
PG		0.48438	0.52500	0.47344	0.47500	0.47969
PTR		0.52188	0.48438	0.52500	0.52656	0.53594
RDS-B		0.48750	0.49688	0.51719	0.51250	0.51406

Comparison results

- Accuracy(Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM -AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
RIO		0.52344	0.51719	0.49375	0.52188	0.50625
SO		0.50000	0.51719	0.51406	0.52813	0.52344
SPY		0.47813	0.50313	0.52344	0.51719	0.53438
SYT		0.51250	0.50469	0.49688	0.47656	0.45313
T		0.53750	0.50938	0.50469	0.50625	0.50000
TM		0.48125	0.50000	0.47188	0.47031	0.48906
TOT		0.48438	0.52031	0.52188	0.51875	0.50313
UNH		0.46406	0.51563	0.51406	0.48750	0.51406
UPS		0.51094	0.49844	0.47813	0.51875	0.50625
VALE		0.49688	0.49219	0.51875	0.49375	0.50156
VZ		0.46406	0.51406	0.52813	0.51719	0.52031
WFC		0.52188	0.47656	0.48750	0.52188	0.54219
WMT		0.47656	0.51563	0.50000	0.47969	0.50000
XOM		0.44844	0.48906	0.51563	0.50469	0.50156

Comparison results

- Execution time (Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
AAPL		161.645	335.396	143.048	161.645	138.432
AMZN		156.504	328.434	136.950	156.504	136.052
BA		160.705	330.712	139.597	160.705	138.824
BAC		162.407	328.612	138.406	162.407	135.258
BHP		158.183	330.041	140.970	158.183	138.292
BRK-B		158.586	332.573	138.586	158.586	143.079
CHL		158.181	332.028	136.008	158.181	140.466
CMCSA		156.620	331.780	141.750	156.620	138.003
CVX		155.816	333.798	140.223	155.816	138.322
D		165.908	336.750	138.927	165.908	139.784
DCM		165.795	337.952	140.254	165.795	141.325
DIS		161.550	334.185	141.032	161.550	135.541
DOW		158.448	332.393	141.182	158.448	136.658
DUK		161.425	336.730	136.732	161.425	137.079
EXC		157.998	332.582	140.514	157.998	138.058
GE		158.958	332.274	143.013	158.958	139.719
GOOGL		160.384	332.088	140.976	160.384	139.862
HD		160.310	332.761	139.349	160.310	137.079

Comparison results

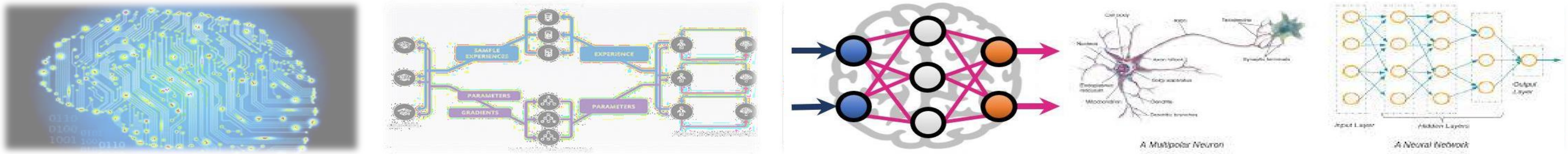
- Execution time (Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
INTC		160.211	330.783	141.906	160.211	147.325
JNJ		159.952	335.776	141.024	159.952	140.351
JPM		162.304	330.591	138.626	162.304	145.941
KO		162.545	333.906	139.024	162.545	147.448
MA		161.891	330.546	139.100	161.891	149.846
MMM		167.212	333.485	141.080	167.212	145.615
MO		165.240	334.212	144.793	165.240	150.964
MRK		160.905	331.877	141.920	160.905	141.089
MSFT		166.390	330.538	138.532	166.390	145.814
NGG		166.530	333.775	141.567	166.530	146.562
NTT		161.551	331.578	143.728	161.551	151.485
NVS		169.513	333.148	140.598	169.513	151.040
ORCL		162.770	330.996	140.703	162.770	145.556
PEP		161.694	334.158	138.646	161.694	145.832
PFE		164.992	332.247	138.961	164.992	151.621
PG		165.728	334.549	143.373	165.728	149.121
PTR		169.118	328.715	144.158	169.118	140.881
RDS-B		168.218	332.170	150.184	168.218	139.130

Comparison results

- Execution time (Index : NASDAQ)

Data	Proposed	DTML [2]	AdvLSTM [7]	CNN BiLSTM -AM [8]	CNN BiLSTM -AM+technical indicator	BiLSTM -AM+technical indicator
RIO		160.253	327.683	140.045	160.253	137.343
SO		156.863	334.877	145.188	156.863	141.181
SPY		159.452	335.157	141.829	159.452	142.038
SYT		156.946	331.131	140.390	156.946	136.391
T		157.791	332.567	139.805	157.791	141.352
TM		161.948	329.700	139.231	161.948	142.028
TOT		163.915	330.992	140.492	163.915	141.173
UNH		169.782	331.001	140.989	169.782	139.637
UPS		163.288	332.706	139.600	163.288	143.059
VALE		171.213	328.378	140.294	171.213	143.917
VZ		162.650	332.866	143.037	162.650	143.516
WFC		161.092	329.751	140.179	161.092	145.777
WMT		162.011	333.436	141.981	162.011	154.010
XOM		161.774	332.370	142.474	161.774	153.513



2-Way Inference on Embedded Board

Geonil Yun

Overview

- **2-Way Inference on Embedded Board**
  - Tasks – Pedestrian detection, Optical Character Recognition
  - Porting to embedded board
  - Framework – 2-Way Inference

2-Way Inference on Embedded Board

- **Task – Pedestrian Detection**

Detection Model

  - Detect pedestrian in image.
  - Labels : full, head, upper, lower
  - Use **Yolo v5 – nano** model to train.

2-Way Inference on Embedded Board

- **Task – Optical Character Recognition**

Nano
YOLOv5n

Recognition Model

TROIKA
VENE RESTORAN
JA TRAHTER

  - Detect and recognize text in image.
  - Label : only **Text**
  - Use **Yolo v5-nano** to train.

2-Way Inference on Embedded Board

- **Detection model & Recognition model**

Detection Model

Train the model using annotated data (full, head, upper, lower, text)

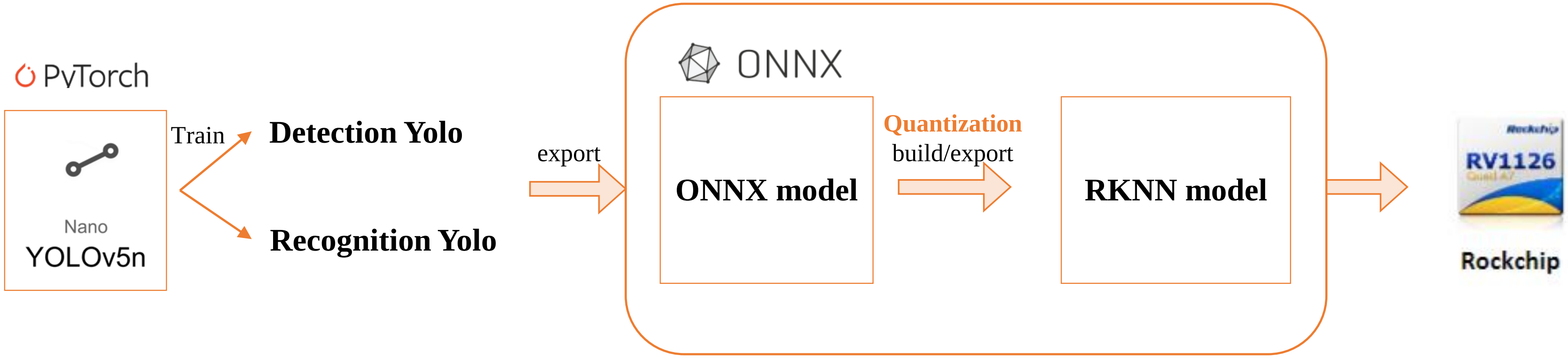
Recognition Model

Train the model using generated data (alphabets & digits)

- Detection model(**Phase-1 Yolo**) detects **full**, **head**, **upper**, **lower**, and **text** in image.
- Recognition model(**Phase-2 Yolo**) detects(recognizes) **alphanumeric characters** in image.

2-Way Inference on Embedded Board

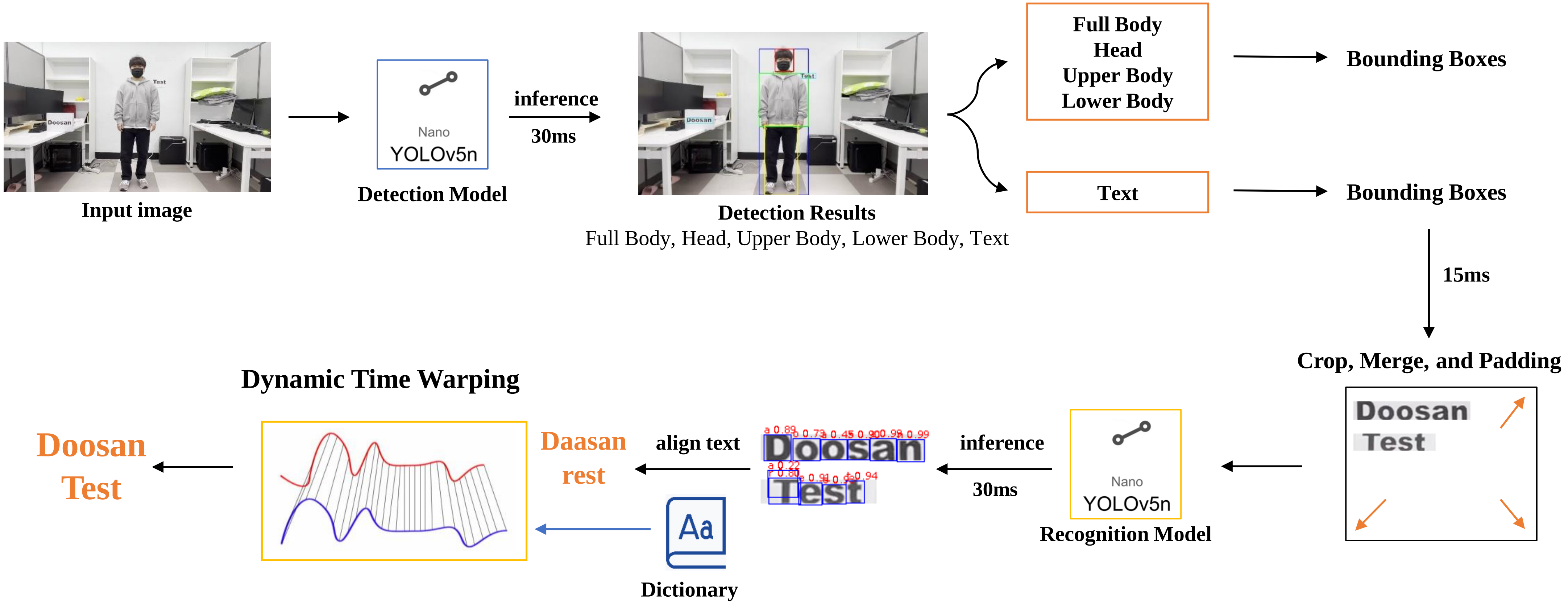
- **Porting model on Rockchip(Embedded board)**
  - Quantization is required to use Rockchip *NPU. (Rockchip NPU supported **UINT8/UINT16**)
  - For quantization, using rkknn library and export as RKNN model



* NPU : Neural Processing Unit

2-Way Inference on Embedded Board

- **Framework**

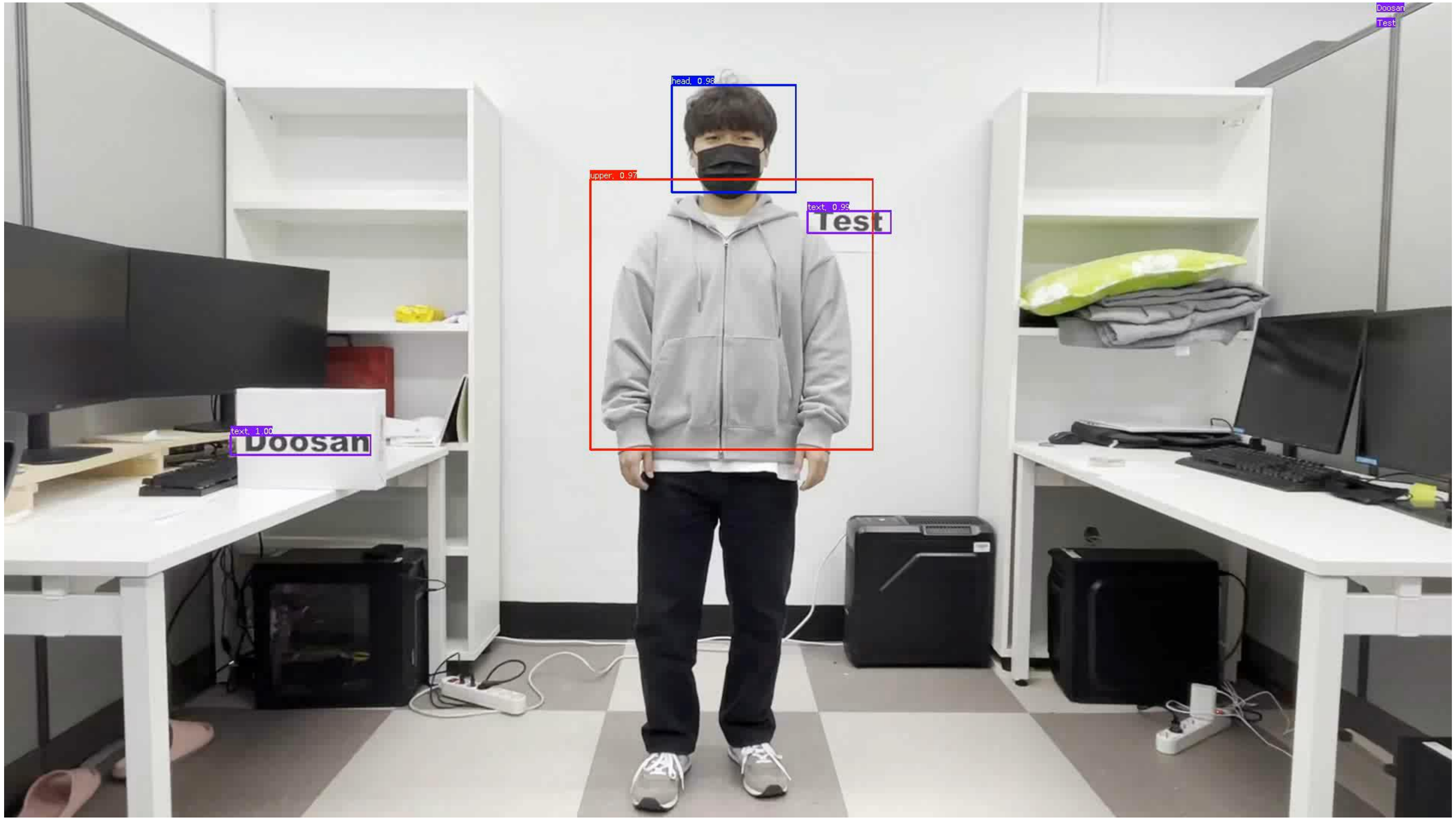


- Detection model(**Phase-1 Yolo**) detects **full, head, upper, lower,** and **text** bounding box in image.
- **Crop** and **merge** text bounding boxes and **padding** to input recognition model(**Phase-2 Yolo**) .
- Aligns text based on alphaneumeric bounding box coordinates.
- Use the ***DTW algorithm** to find the most similar word in dictionary.

* DTW : Dynamic Time Warping

2-Way Inference on Embedded Board

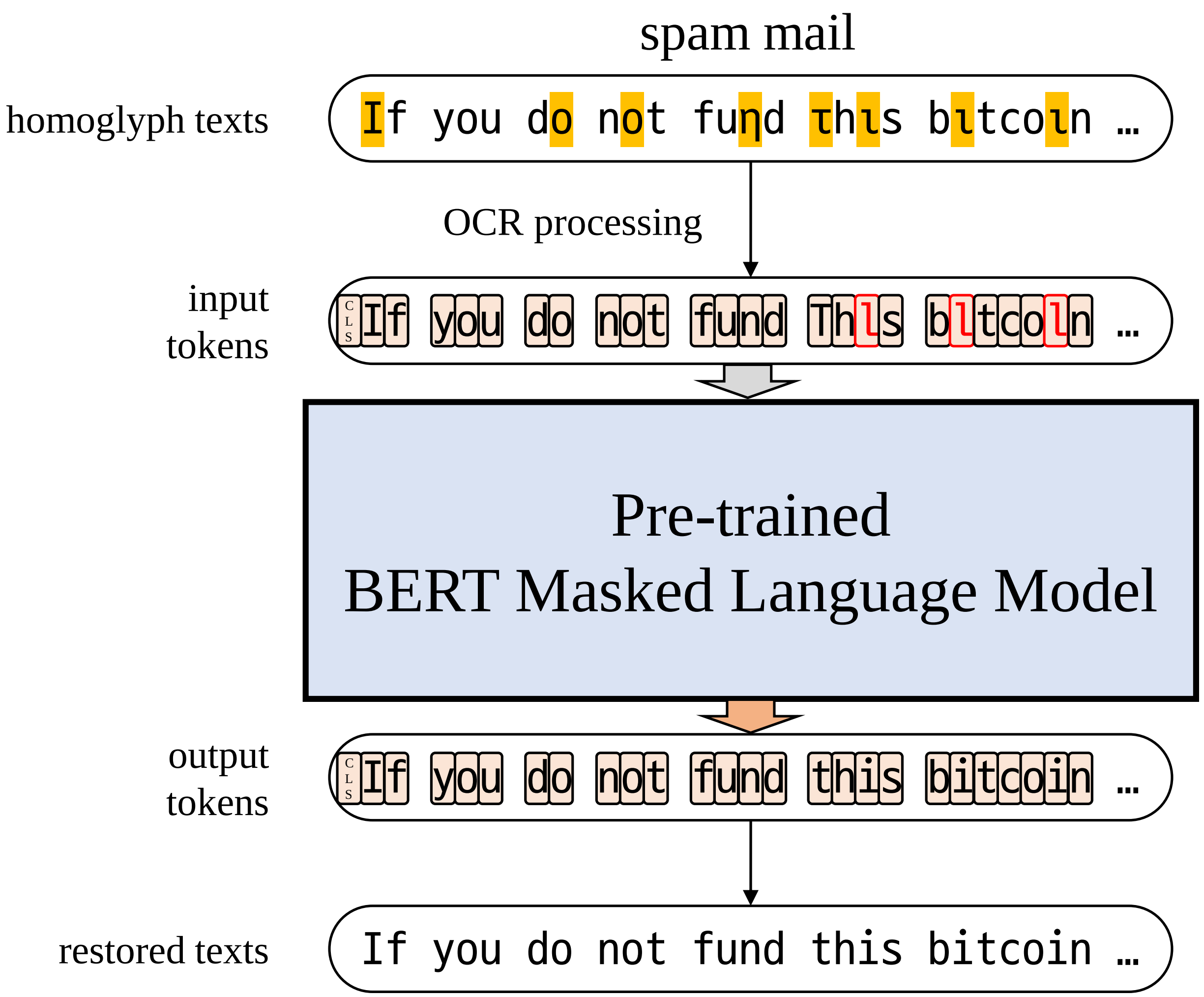
- **Demo video**



Restoration of Homoglyph Attack with BERT

Hanyong Lee

Restoration of Homoglyph Attack with BERT



Restoration of Homoglyph Attack with BERT

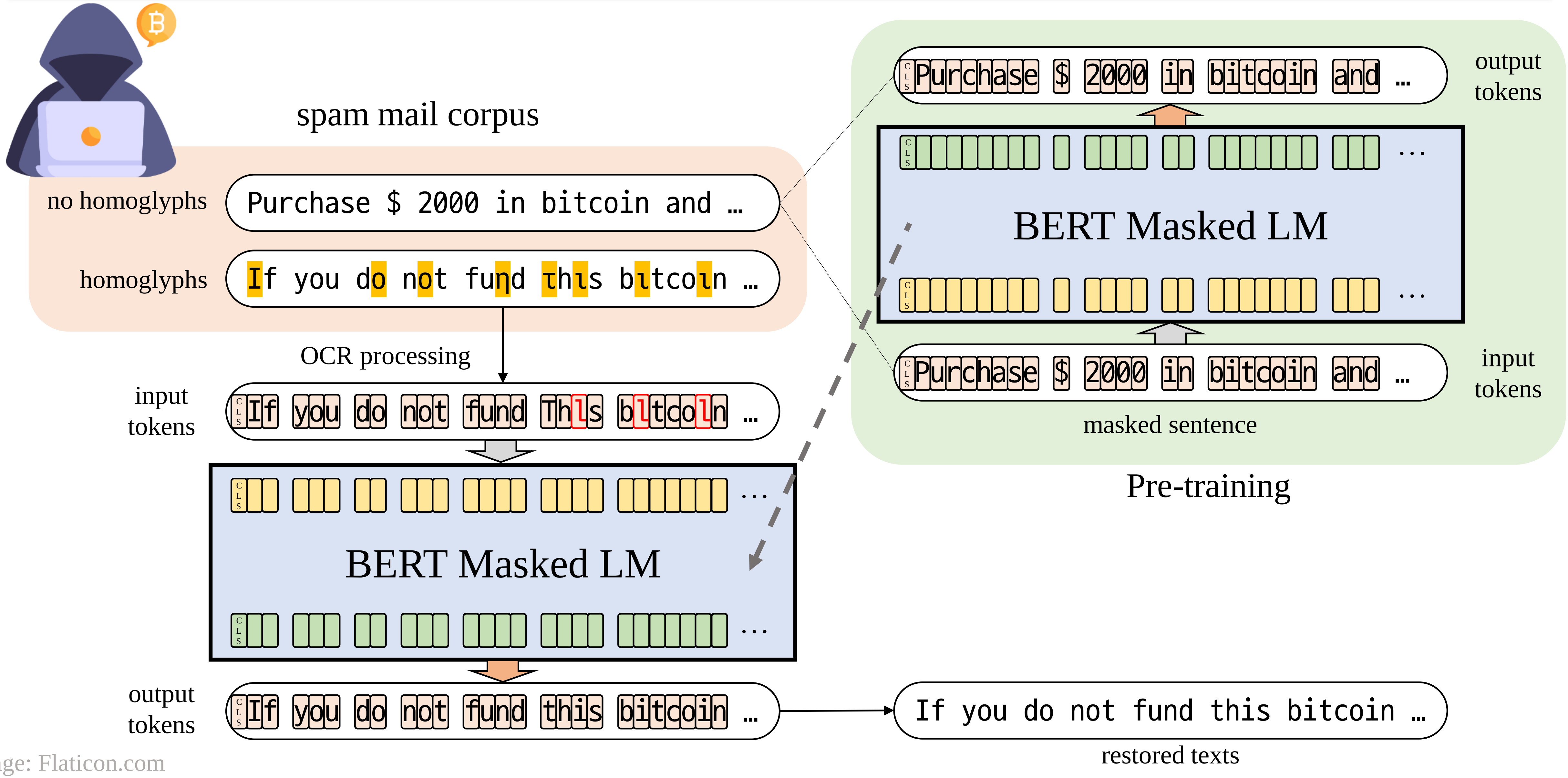


image: Flaticon.com

✓ To Do List

- Last Week
  1. Refining English data
  2. Splitting ASCII-only / homoglyph set

- This Week
  1. Making homoglyph dictionary for test dataset
  2. Annotating for homoglyph dataset.
  3. Removing junk data.

0. Overview

Collecting Homoglyph Words → Annotating Homoglyphs → Labeling Homoglyph Texts (→ Evaluation Set)

1. Making / Annotating homoglyph dictionary for test dataset

- Collection & Annotation of 41097 homoglyph words.
- Dictionary file Examples

```
"bitcoín": "bitcoin",
"bitcoĩn": "bitcoin",
"bitcoĩn'": "bitcoin'",
"bitcoīn": "bitcoin",
"bitcoīn'": "bitcoin'",
"bitcoǐn": "bitcoin",
"bitcoǐn'": "bitcoin'",
"bitcoȋn": "bitcoin",
"bitcoȋn'": "bitcoin'",
"bitcoĺn": "bitcoin",
"bitcoĺn'": "bitcoin'",
"bitcoin": "bitcoin",
```

```
"emaіls": "emails",
"emails,": "emails,",
"emails,": "emails,",
"emaìl": "email",
"emaìls": "emails",
"emaìl": "email",
"emaíl": "email",
"emaıl": "email",
"emaỉl": "email",
"emaỉls,": "emails,",
"emaỉl": "email",
"emaỉl": "email",
```

```
"hacked": "hacked",
"hacker": "hacker",
"hackers": "hackers",
"hackèd": "hacked",
"hackéd": "hacked",
"hackíng": "hacking",
"hackîng": "hacking",
"hacked": "hacked",
"hacked": "hacked",
"hacker": "hacker",
"hacÂked": "hacaked",
"hacķers": "hackers",
```

2. Removing Junk Data

- Junk Data examples
  - HTML Codes
    - “.u0bcea8b7ca1::before { content: ...”
  - No Meaning Texts
    - “asdasdfasdfasdfasdfa”
    - “ffg fg fgfgf gfgfgf”
  - User-Reported IP Lists
    - “IP list: 103.140.xx.xx 103.198.xx.xx 103.81.xx.xx …”
  - Unexcluded non-English texts

3. Dataset Split Information

- Total Examples: 178,203
  - one or more sentences per one example
- Homoglyph Examples: 6,912
- Non-homoglyph Examples: 171,291