A.I. on Digital Forensics

2024. 8. 6.

Chanhwi Lee

Cybersecurity Research Center of KNPU

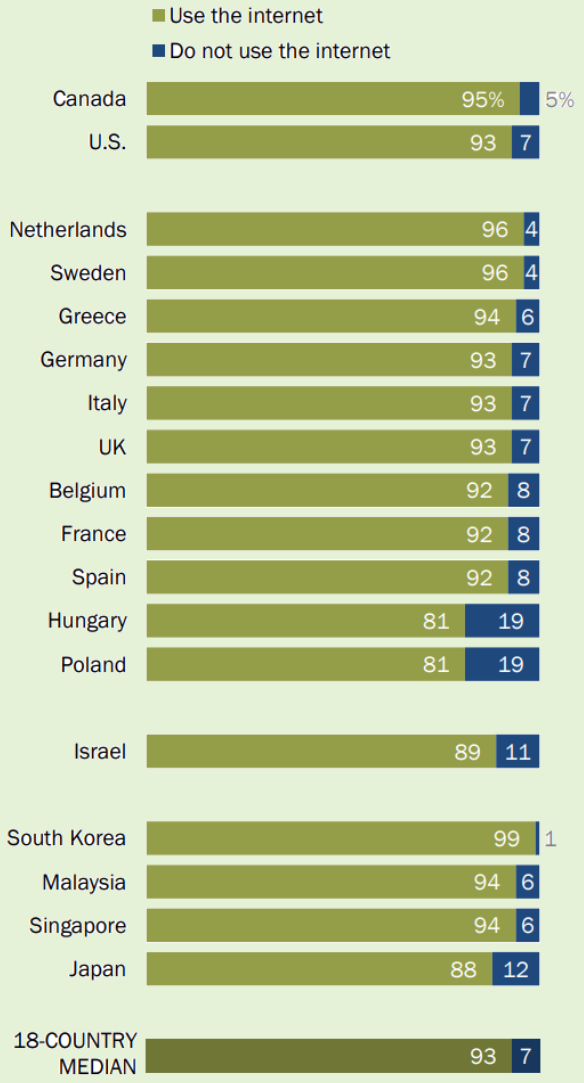
About Lecturer

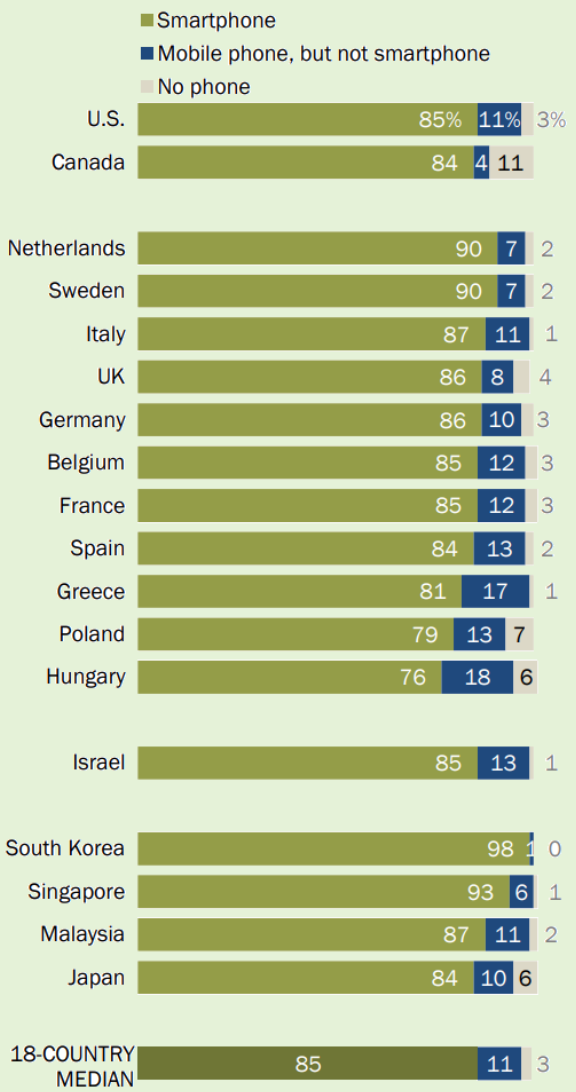
- B.L. in K.N.P.U.(2019)
- Investigator(2021-2023)
- KNPA CTF(2022, 2023)
- Whitehat Conference(2024)
- Interested in Vulnerability Analysis, Digital Forensics

Table Of Contents

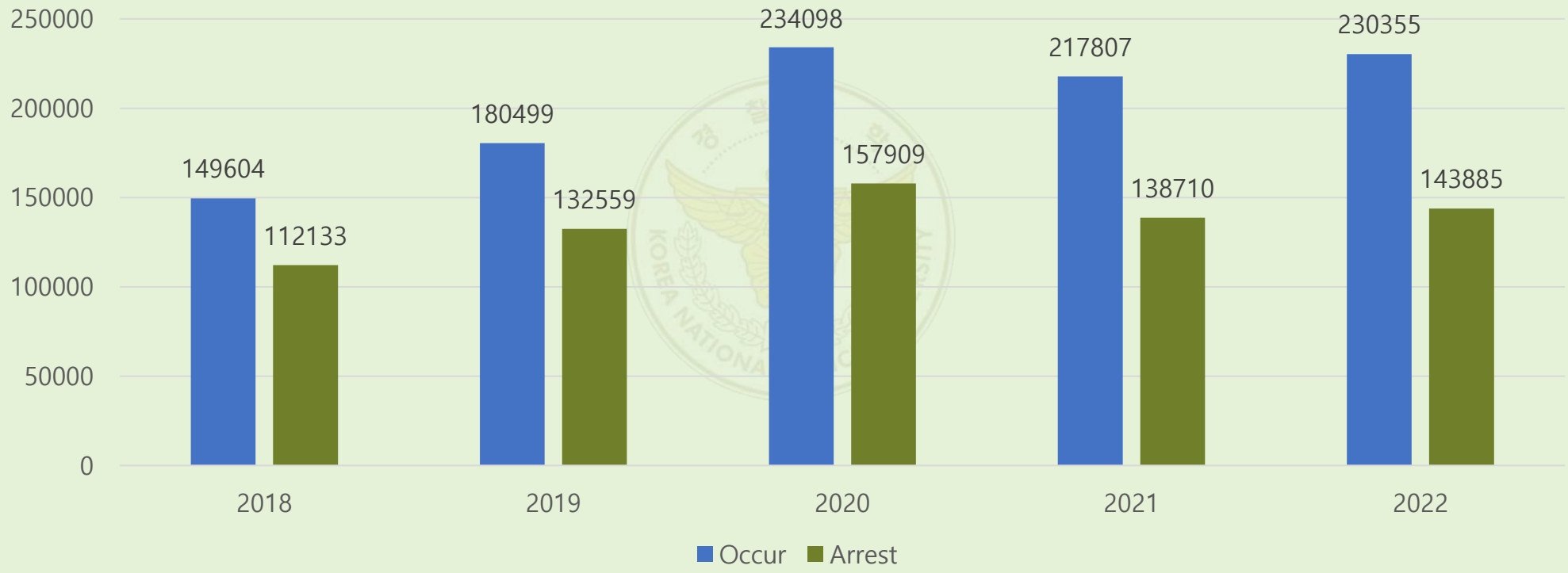
1. The Nature of Digital Evidence

Penetration Rate of Internet & Smartphone

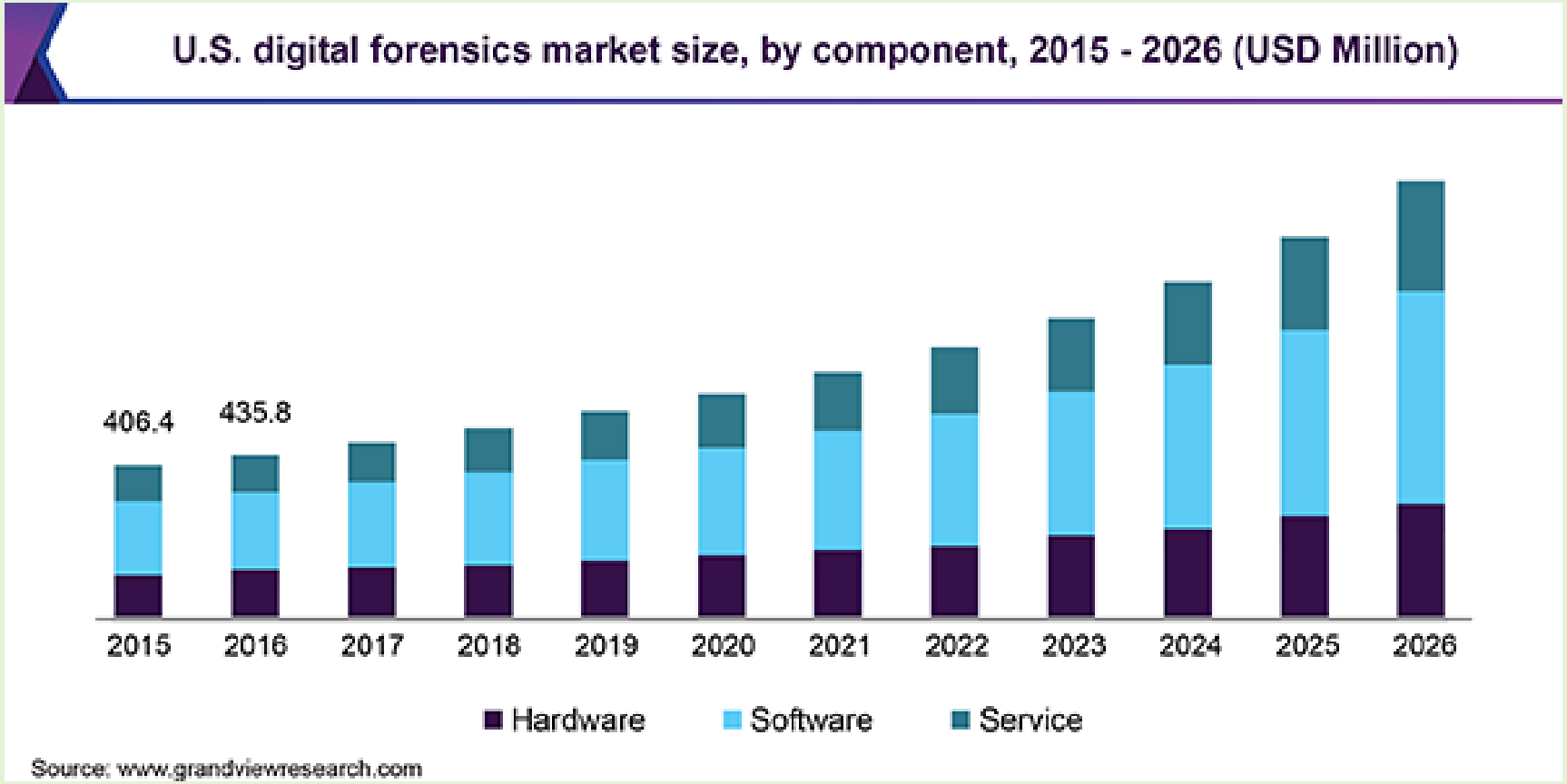




Cybercrime Stats



Growth in Digital Forensic Market



Need for breakthrough

- The increasing number of cases and devices seized is further compounded with the growing size of storage devices (Garfinkel, 2010).
- Existing forensic software solutions have evolved from the first generation of tools and are now beginning to address scalability issues. However, a gap remains in relation to analysis of large and disparate datasets(Roussev et al., 2013).

2. About AI Technology

CNN(Convolution Neural Network)

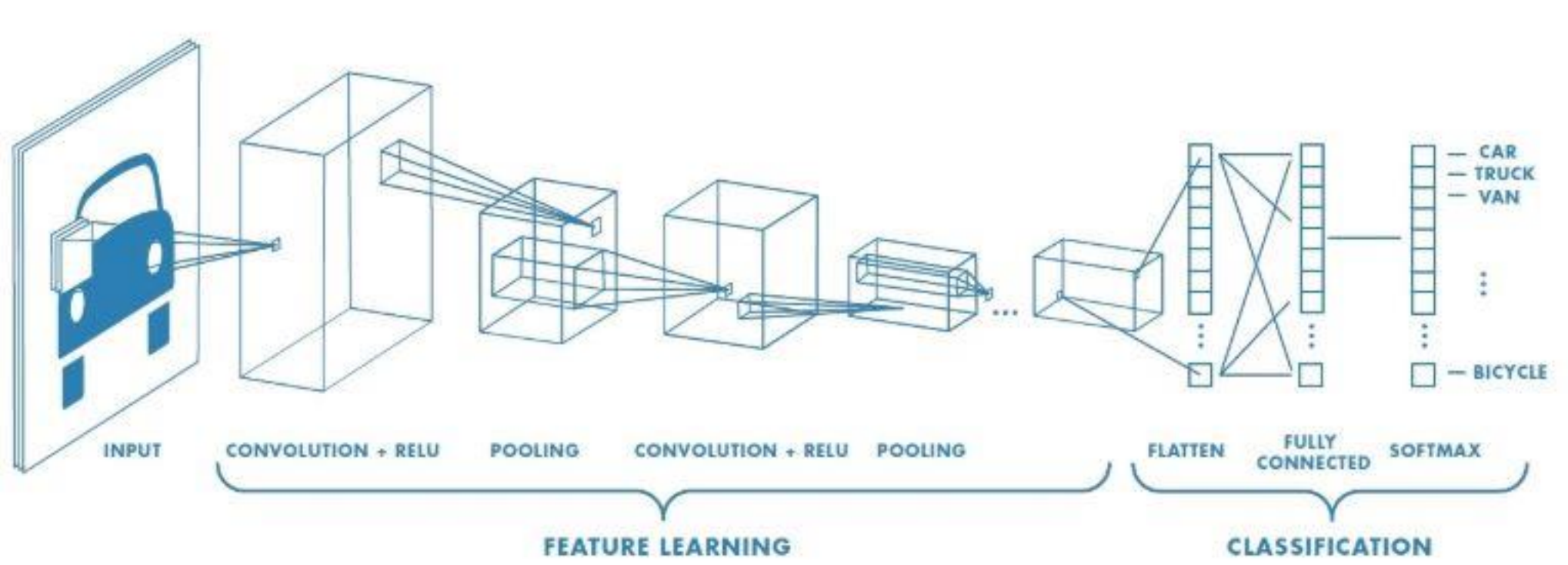
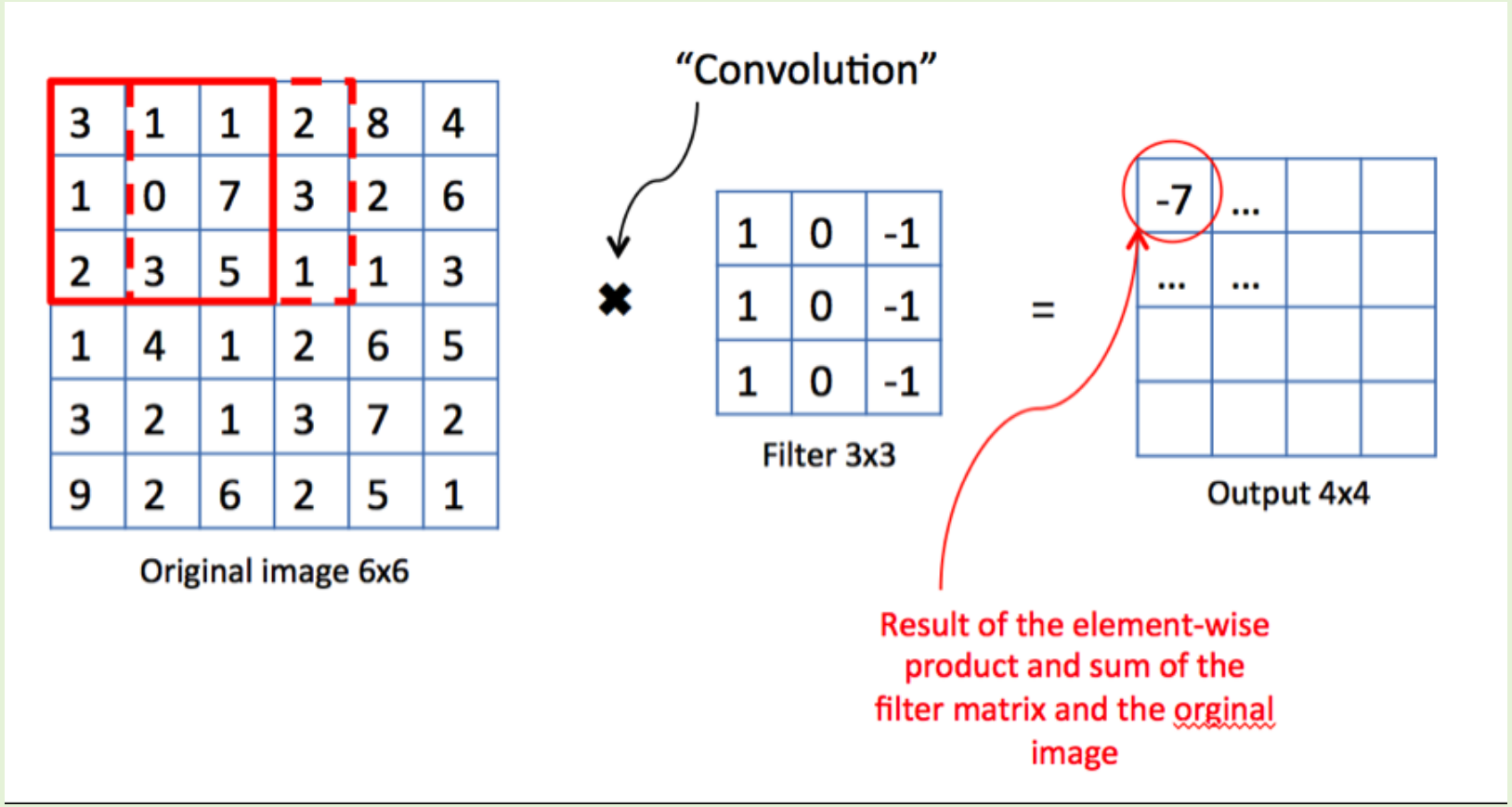


Image File

```
[[[  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   3  18  18  18 126 136 175  26 166 255 247 127   0   0   0   0]
  [  0   0   0   0   0   0   0   0  30  36  94 154 170 253 253 253 253 253 225 172 253 242 195  64   0   0   0   0]
  [  0   0   0   0   0   0   0  49 238 253 253 253 253 253 253 253 253 251  93  82  82  56  39   0   0   0   0   0]
  [  0   0   0   0   0   0   0  18 219 253 253 253 253 253 198 182 247 241   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0  80 156 107 253 253 205  11   0  43 154   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0  14   1 154 253  90   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0 139 253 190   2   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0  11 190 253  70   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0  35 241 225 160 108   1   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0  81 240 253 253 119  25   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0  45 186 253 253 150  27   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0  16  93 252 253 187   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 249 253 249  64   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0  46 130 183 253 253 207   2   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0  39 148 229 253 253 253 250 182   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0  24 114 221 253 253 253 253 201  78   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0  23  66 213 253 253 253 253 198  81   2   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0  18 171 219 253 253 253 253 195  80   9   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0  55 172 226 253 253 253 253 244 133  11   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0 136 253 253 253 212 135 132  16   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]
  [  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0]]]
```

28 x 28(pixel) image file, The number indicates the brightness of each pixel

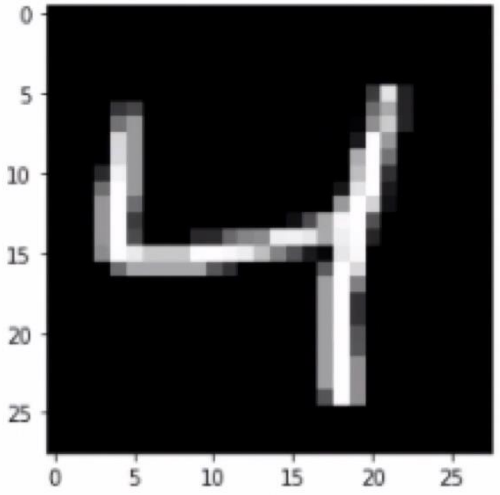
Convolution Layer

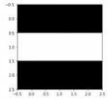


Convolution Layer

특정한 패턴의 특징이
어디서 나타나는지를 확인하는 도구

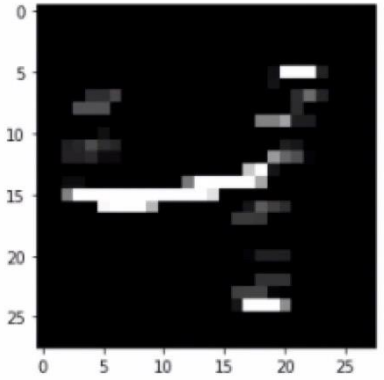
"Convolution"

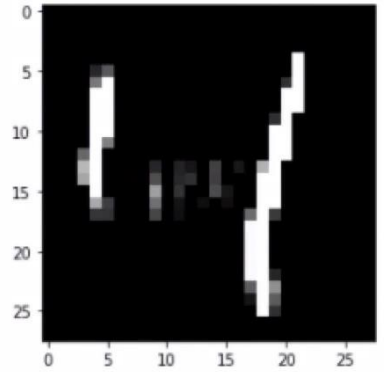




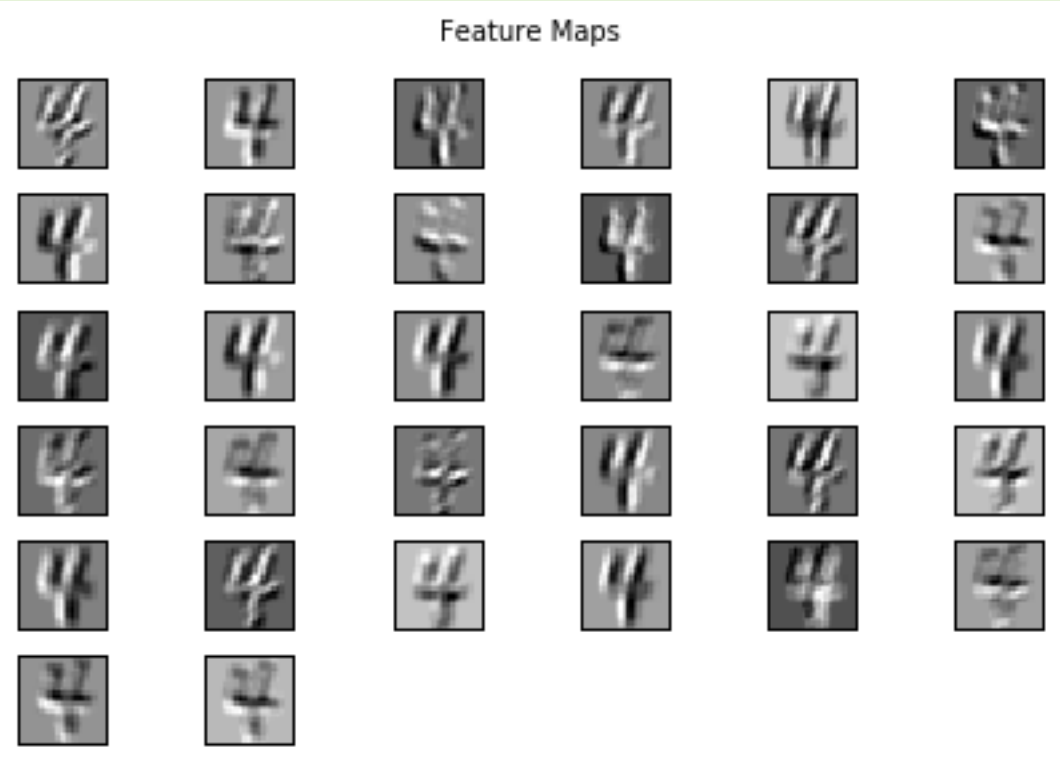
필터
Filters

특징맵 feature map

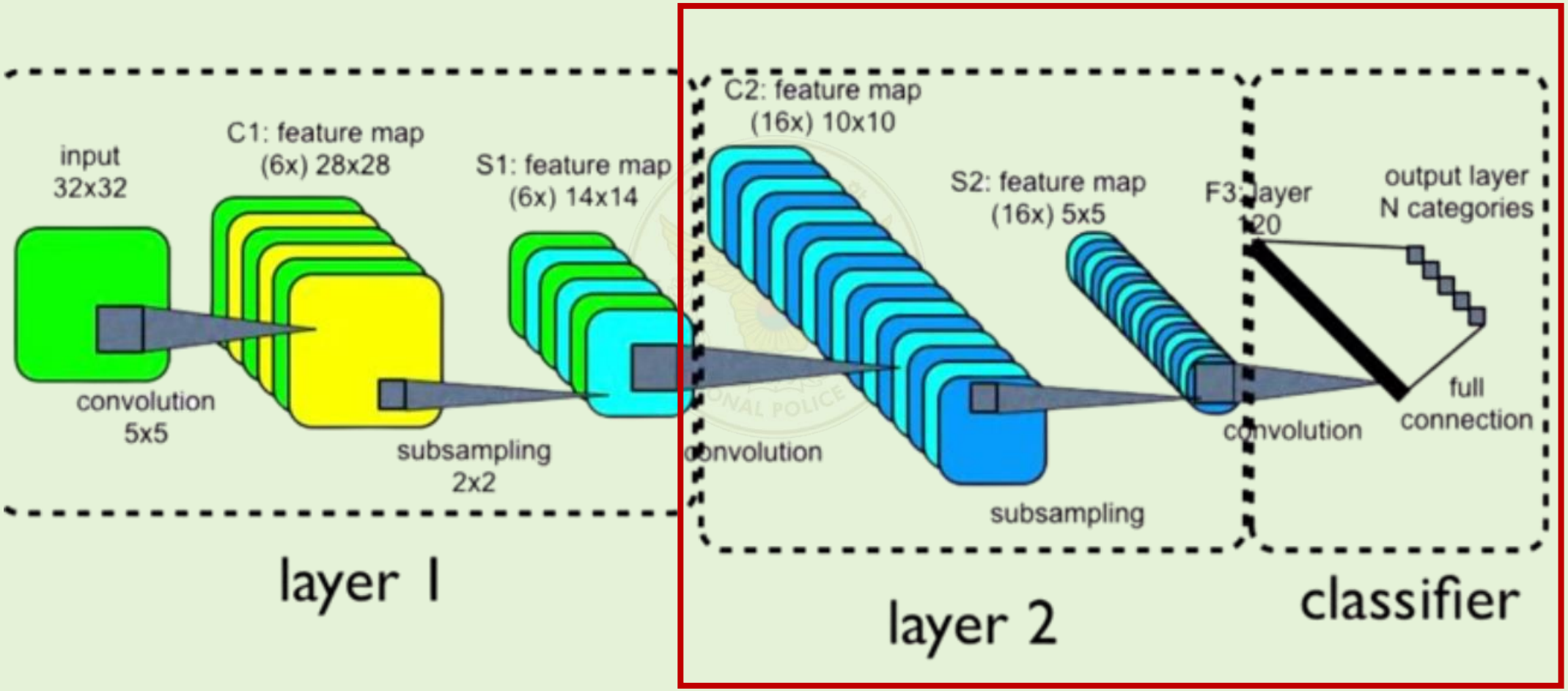




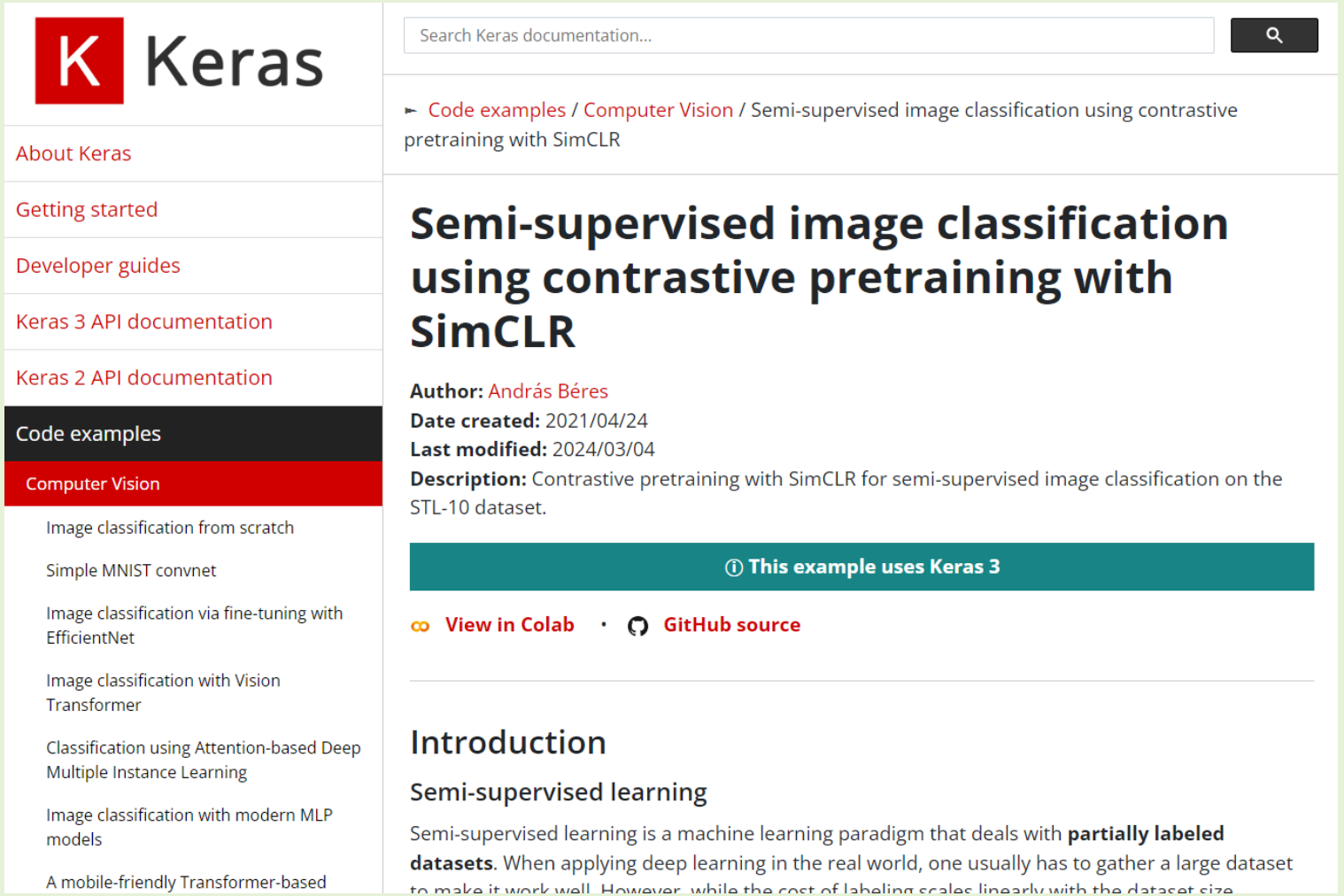
Convolution Output



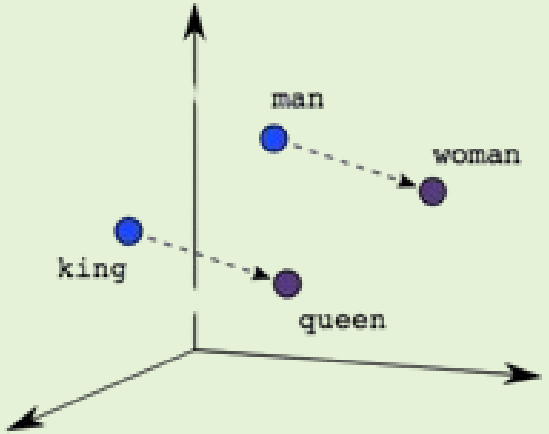
Convolution Output



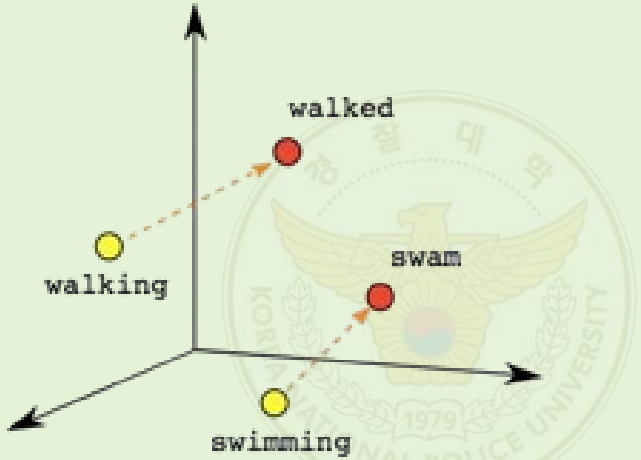
Keras


Keras
Search Keras documentation...
About Keras
Getting started
Developer guides
Keras 3 API documentation
Keras 2 API documentation
Code examples
Computer Vision
Image classification from scratch
Simple MNIST convnet
Image classification via fine-tuning with EfficientNet
Image classification with Vision Transformer
Classification using Attention-based Deep Multiple Instance Learning
Image classification with modern MLP models
A mobile-friendly Transformer-based
Code examples / Computer Vision / Semi-supervised image classification using contrastive pretraining with SimCLR
Semi-supervised image classification using contrastive pretraining with SimCLR
Author: András Béres
Date created: 2021/04/24
Last modified: 2024/03/04
Description: Contrastive pretraining with SimCLR for semi-supervised image classification on the STL-10 dataset.
This example uses Keras 3
View in Colab
GitHub source
Introduction
Semi-supervised learning
Semi-supervised learning is a machine learning paradigm that deals with partially labeled datasets. When applying deep learning in the real world, one usually has to gather a large dataset

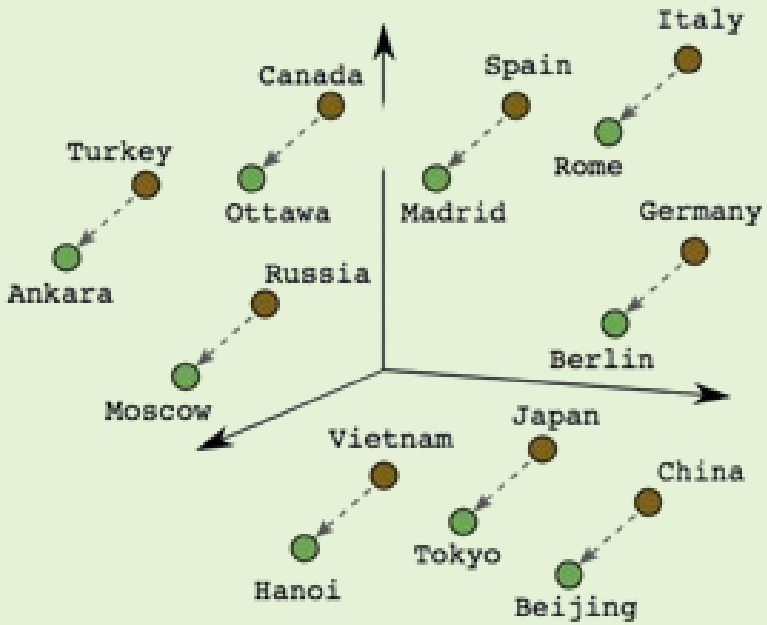
Word Embedding



Male-Female

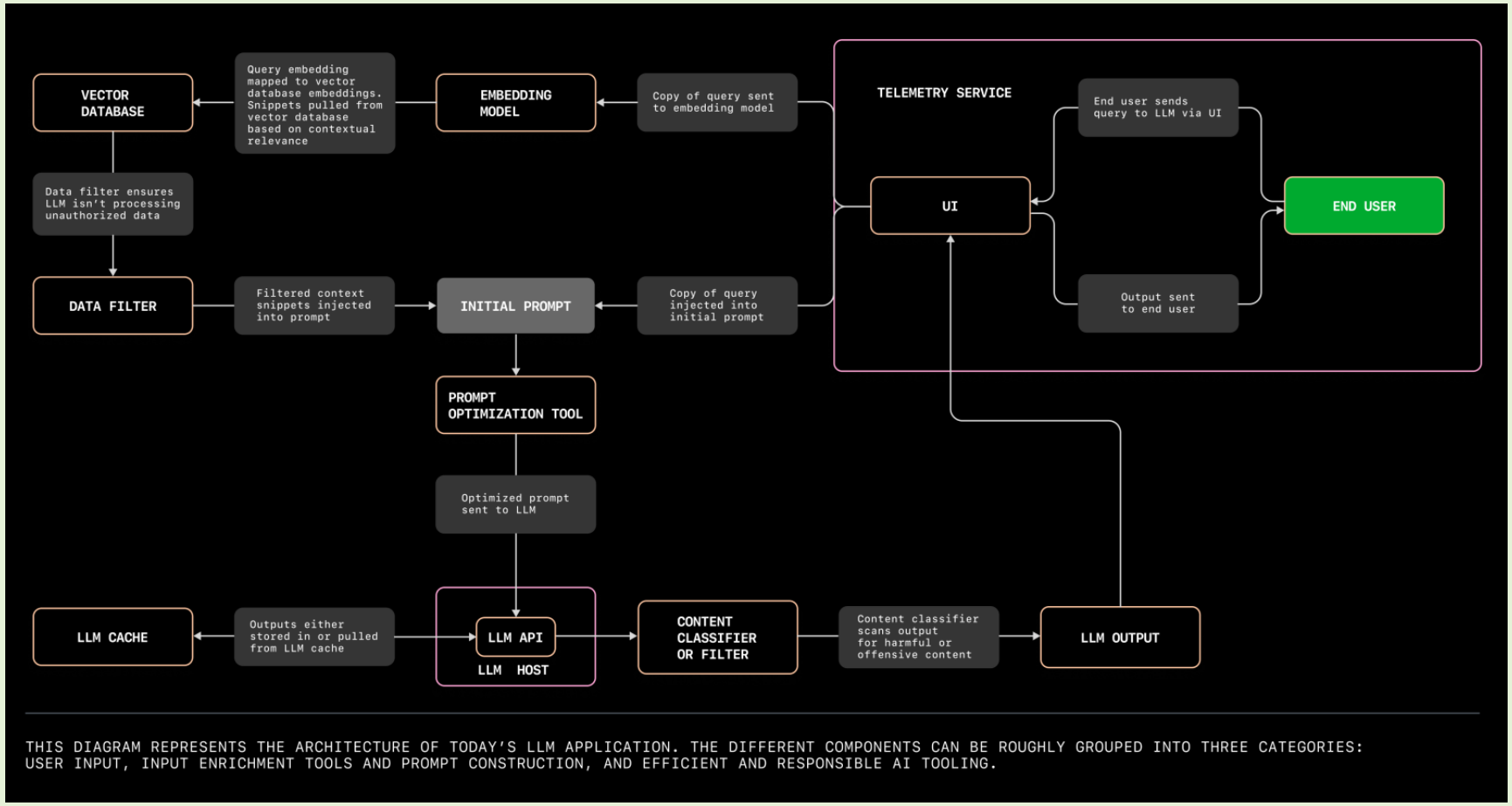


Verb Tense



Country-Capital

LLM(Large Language Model)



LLMs

1. Server-side Model(Need API call)
- GPT 4o, 4o-mini
- Claude 3.5 Sonnet
- Gemini 1.5
- etc

2. Local model
- Llama 3.1
- Phi 3
- Mistral

3. Application to Digital Evidence

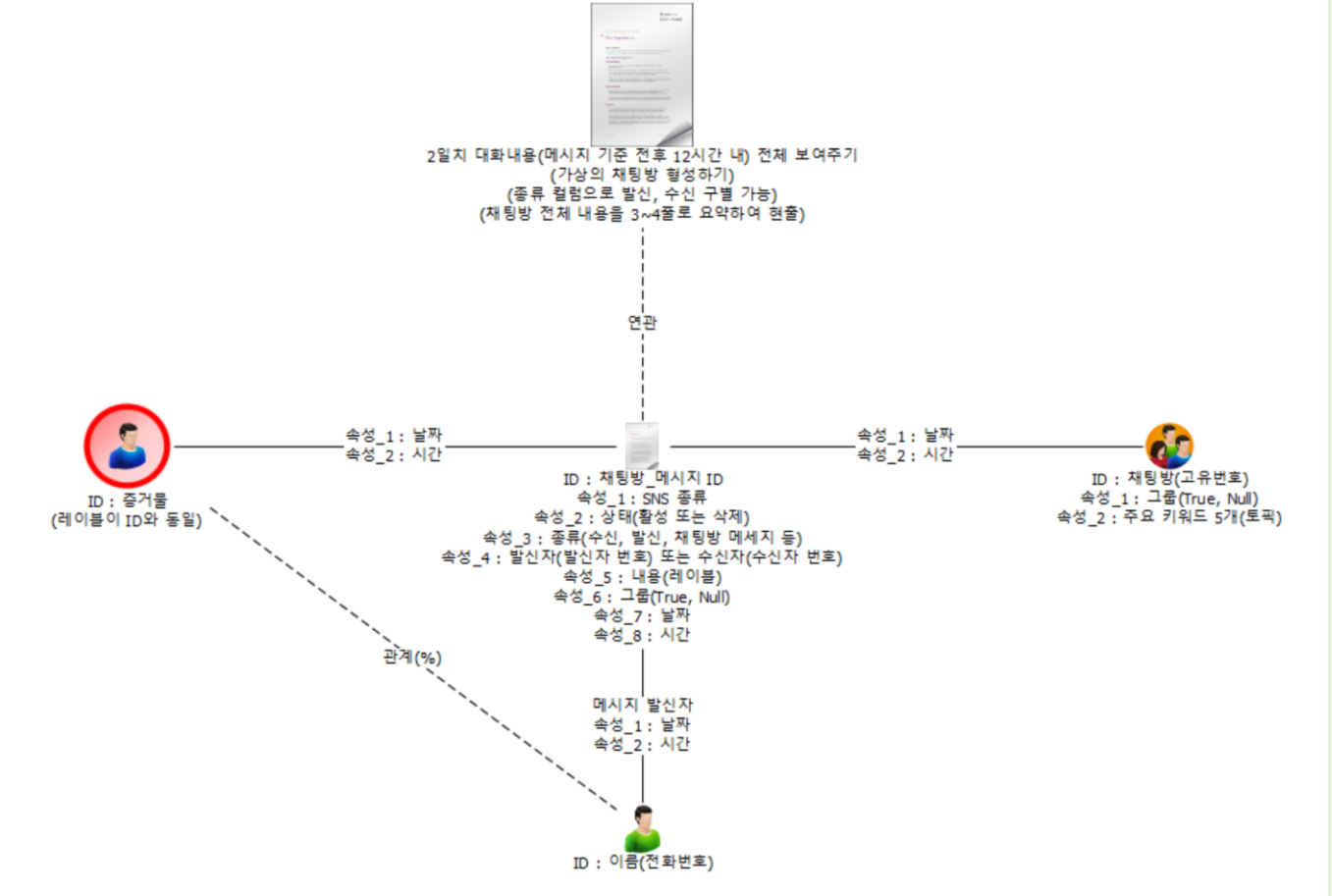
Types of digital Evidences

- Text : Email, Chats, Messages…

- Audio : Phone call, Music …

- Image : CCTV Footage, Google Streetview…

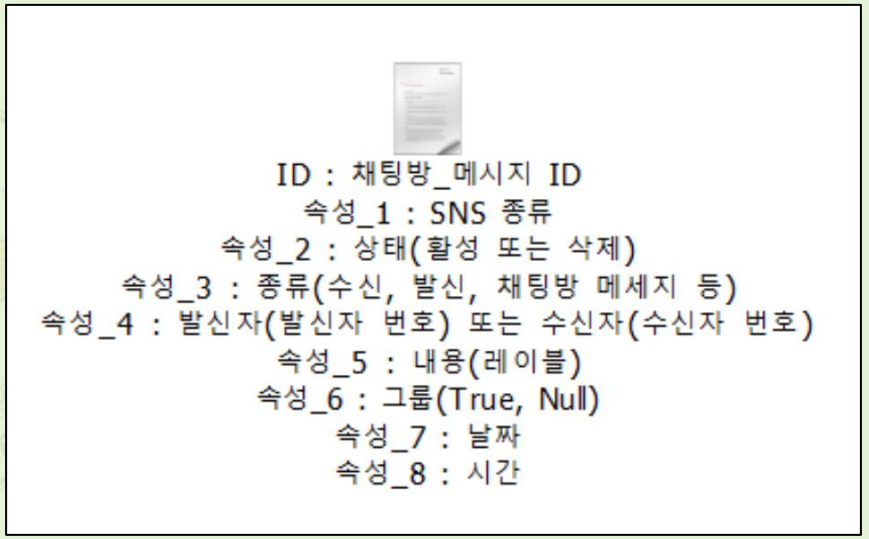
3. 1. AI on text-based evidences



3. 1. AI on text-based evidences

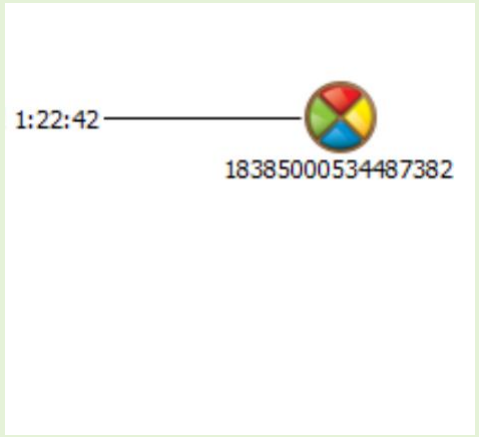
1. Scheme
- Message
- Chatroom
- Person

2. Using LLM with proper prompt



3. 1. AI on text-based evidences

3. 1. AI on text-based evidences



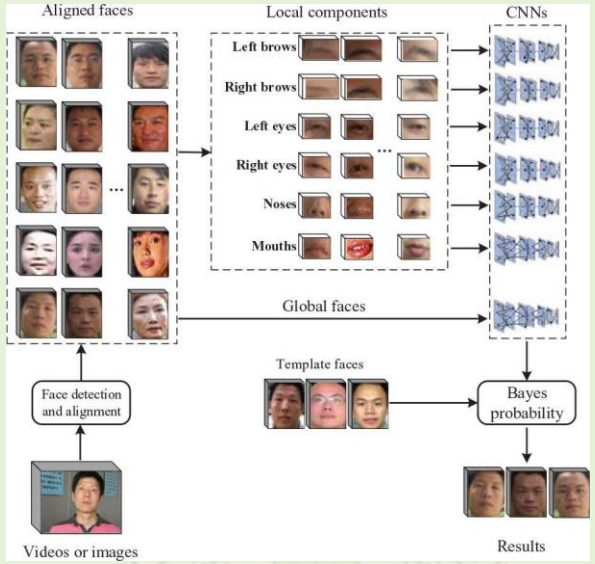
채팅방 ID 18385000534487382 에서 추출한 마약관련 대화입니다.

1. 한 대화에서는 "왜 형사가 너 찾아? 너 또 마약 팔았지?"라는 말이 나오며, 법 집행 기관이 마약 판매와 관련해 어떤 인물을 추적하고 있음을 나타냅니다.
2. 또 다른 대화에서는 "너 마약하지!!!"라고 질문하며, 응답자가 마약을 하지 않는다고 부인하는 내용이 포함되어 있습니다.
3. 추가적으로, "내가 이거 때문에 약을 먹는거였어"라는 문장도 있으며, 이는 특정 상황이나 스트레스로 인해 약물 사용을 하고 있음을 암시합니다.

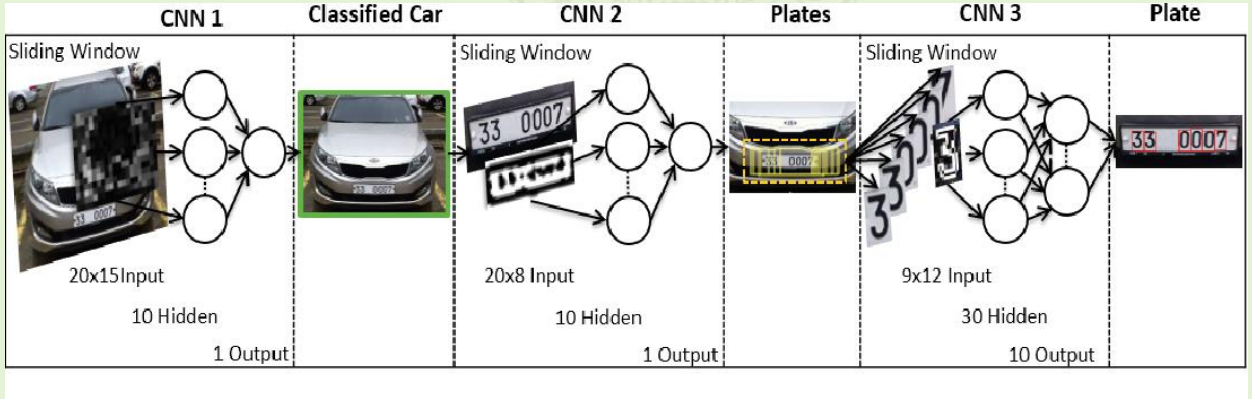
Context Grasp from multiple text messages.

3. 2. AI on image-based evidences

- Face detection

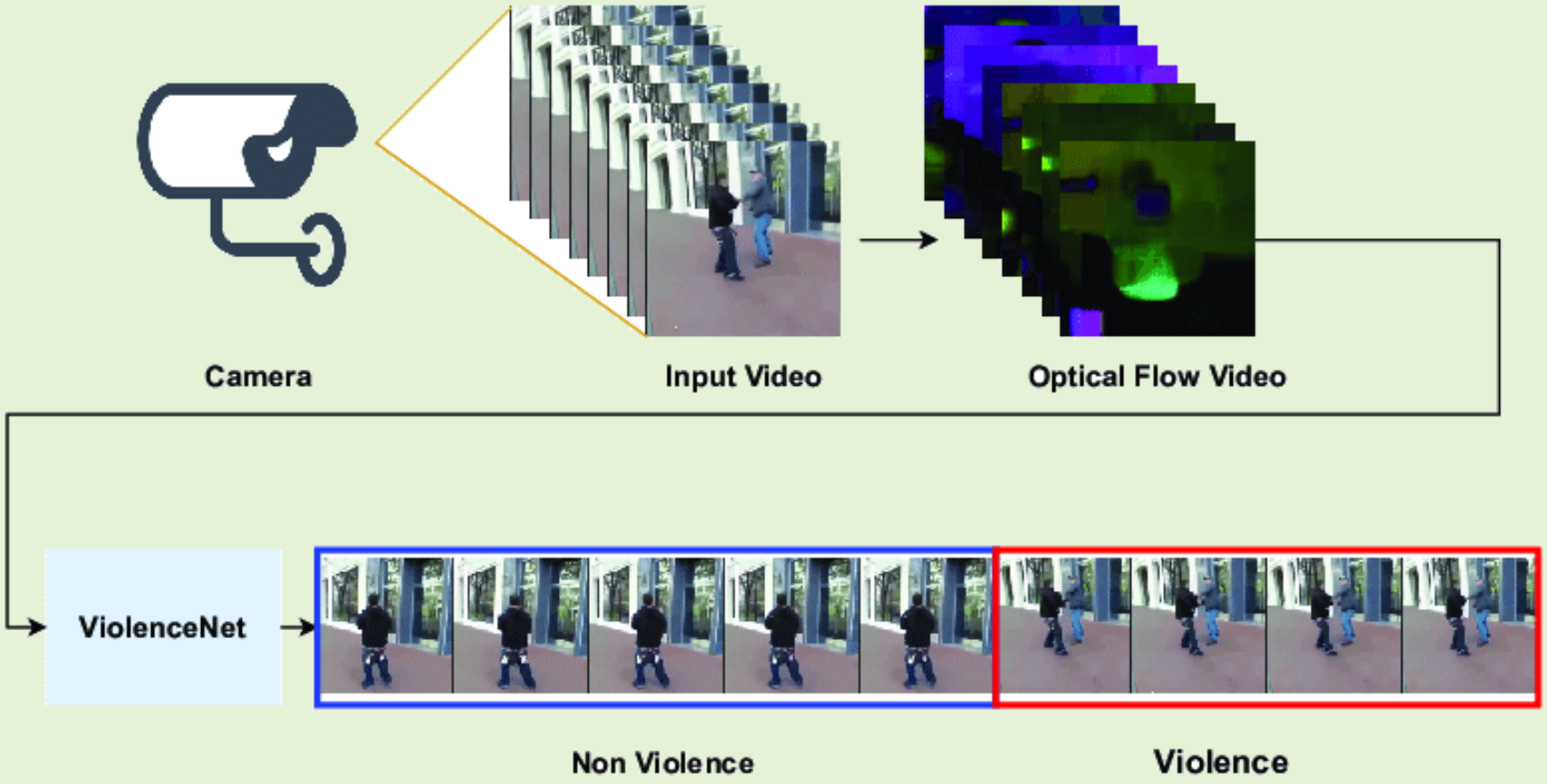


- Car number detection

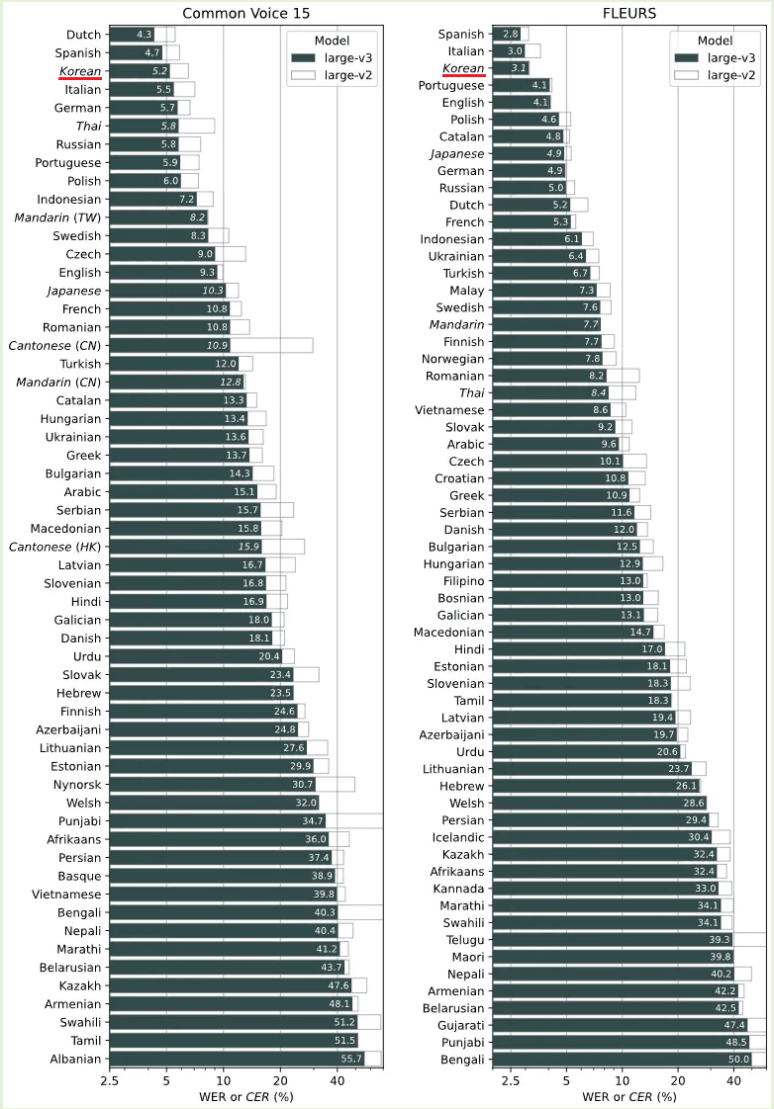


3. 2. AI on image-based evidences

- CCTV Violence Detection



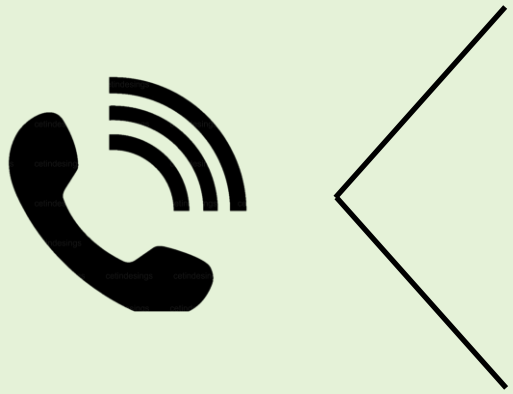
3.3. AI on audio-based evidences



3.3. AI on audio-based evidences

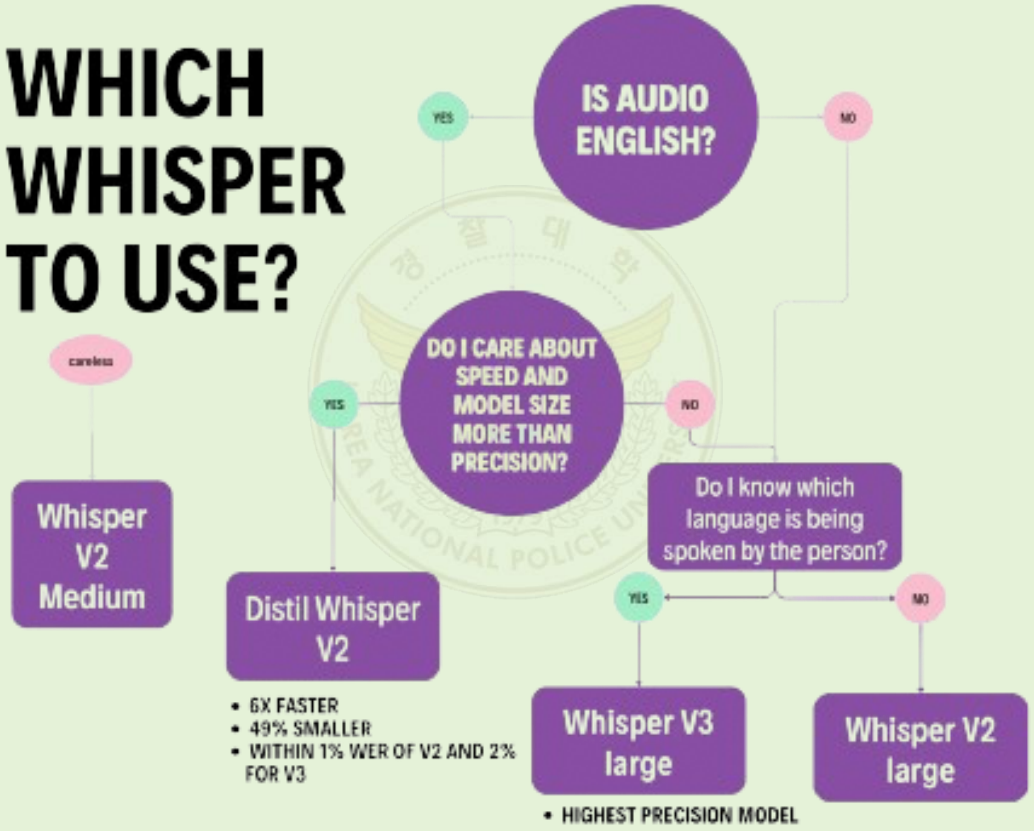
```
[1]: from lightning_whisper_mlx import LightningWhisperMLX

[2]: whisper = LightningWhisperMLX(model="distil-large-v3", quant=None)

     Error displaying widget: model not found
     Error displaying widget: model not found

[16]: whisper2 = LightningWhisperMLX(model="large-v3", quant=None)

     Error displaying widget: model not found
     Error displaying widget: model not found

[3]: output = whisper.transcribe(audio_path="./Sample.mp3")
```

3.3. AI on audio-based evidences



```
[8]: output['text']

[8]: " In early January 2024, Special Agent Mr. CIC from the National Cybercrime Investigation Bureau and his team received intelligence about an
elusive criminal mastermind known as Mr. Evil Noodle. Suspected of coordinating cybercrimes against major global corporations, Meister Evil N
oodle is linked to a covert, state-backed hacking group named the Evil Lizards. This group masquerades as a tech support service for global r
obotics companies, using this guise to implant malware, conduct, surveillance and harvest sensitive data. Their operations also involve manip
ulating compromised robots to function as tools in a global espionage network. Recent cyber attack. Incidents. A notable attack involved a so
phisticated email scam targeting employees with a malicious word attachment, leading to a ransomware outbreak that encrypted vital files. Con
currently, a massive leak of information from the company's servers was revealed by a national cert alert, tracing back company suppliers fou
nd on the darknet. Additionally, malware was discovered in the systems managing critical operational robot data, marking a multivector approa
ch to the cyber attacks. Case study South Korea Robotics Breach A breach at a leading South Korean robotics firm demonstrated the evil lizar
d's capacity to infiltrate and manipulate critical infrastructure, significantly impacting global national security. CIC team engagement. The
CIC team is alerted by the National Search. and immediately engages with a scenario involving complex cyber threats, requiring them to analyz
e attacks and develop strategies to mitigate damage and enhance cybersecurity. The CIC team begins their shift with an alert from the Nationa
l CERT and are immediately thrust into a scenario that challenges them to navigate through complex cyber threats, analyze attacks, and devise
strategic responses to mitigate damage and strengthen cybersecurity measures. Objective. Special Agent Mr. CIC and his team, team aimed to di
smantle Mr. Evil Noodles network and neutralize the threat posed by his group, the evil lizards. The operation focuses on cybercrime intertwi
ned with espionage, highlighting the need for cybersecurity vigilance and international collaboration. Mission. The team is investigating Mr.
Evil Noodle's involvement in trafficking banned items through the dark web. The primary tasks involve meticulously analyzing evidence to docu
ment key details, including cryptocurrency addresses used for transactions, and identities of suspects involved. Concurrently, the team must
activate the AI bot to locate and decryp the file with team members' credentials. Gaining access to this file is crucial for advancing to sub
sequent stages of the investigation. The focus shifts to investigating one of the most active APT groups tied to Mr. Evil Noodle, exploring t
he complexities of ransomware and cyber espionage. This mission highlights the indispensable role of cybersecurity professionals, known as Wh
ite Hats, combating sophisticated cyber threats. Good luck as you navigate these challenges and strive to protect national security."
```

3.3. AI on audio-based evidences



Reference

- https://velog.io/@rsj9987/%EB%94%A5%EB%9F%AC%EB%8B%9D-CNN-%EA%B8%B0%EB%B3%B8-%EA%B5%AC%EC%A1%B0
- https://www.pewresearch.org/global/2022/12/06/internet-smartphone-and-social-media-use-in-advanced-economies-2022/
- https://www.apple.com/kr/newsroom/2023/06/introducing-apple-vision-pro/
- https://platum.kr/archives/56307
- https://www.atlantis-press.com/journals/ijcis/125905637/view
- https://www.semanticscholar.org/paper/Number-Plate-Detection-with-a-Multi-Convolutional-Gerber-Chung/e015047bace9d909de956a9f3db70ab64a57d6a5
- https://x.com/osanseviero/status/1725122881384776023
- https://www.researchgate.net/figure/CCTV-scheme-for-detection-of-violence-scenes-In-a-CCTV-system-our-model-receives-the_fig3_353001089


Thank you!!
Q&A