Anomaly Detection

Machine Learning Study

JinHo Kim

Contents

1. Introduction

Intro.

"Anomaly Detection!"

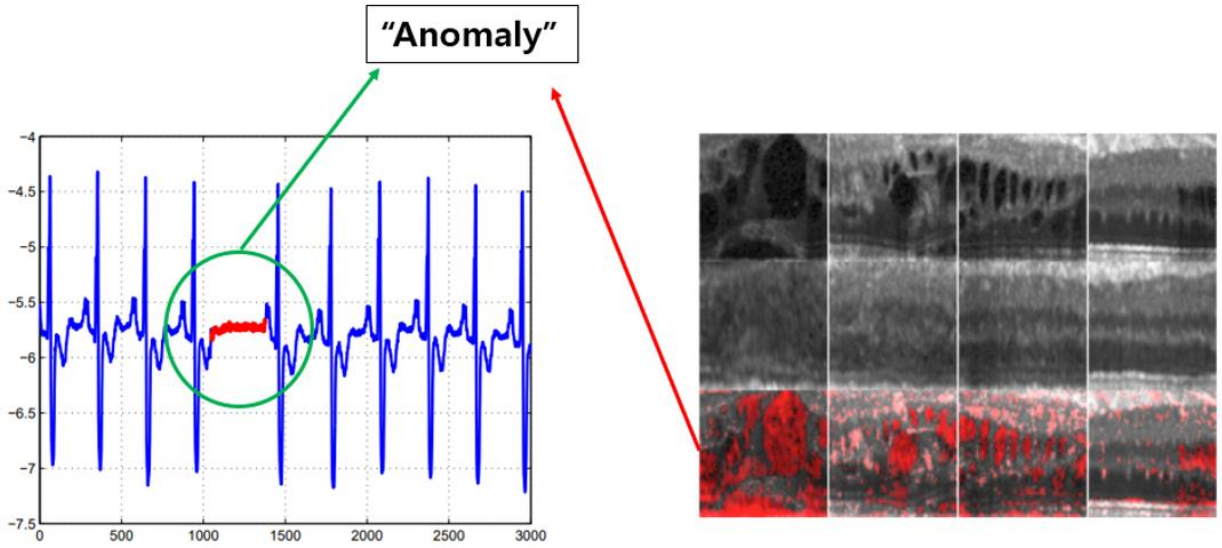
Intro.

Security

Defense

2. What is Anomaly?

What is Anomaly Detection?

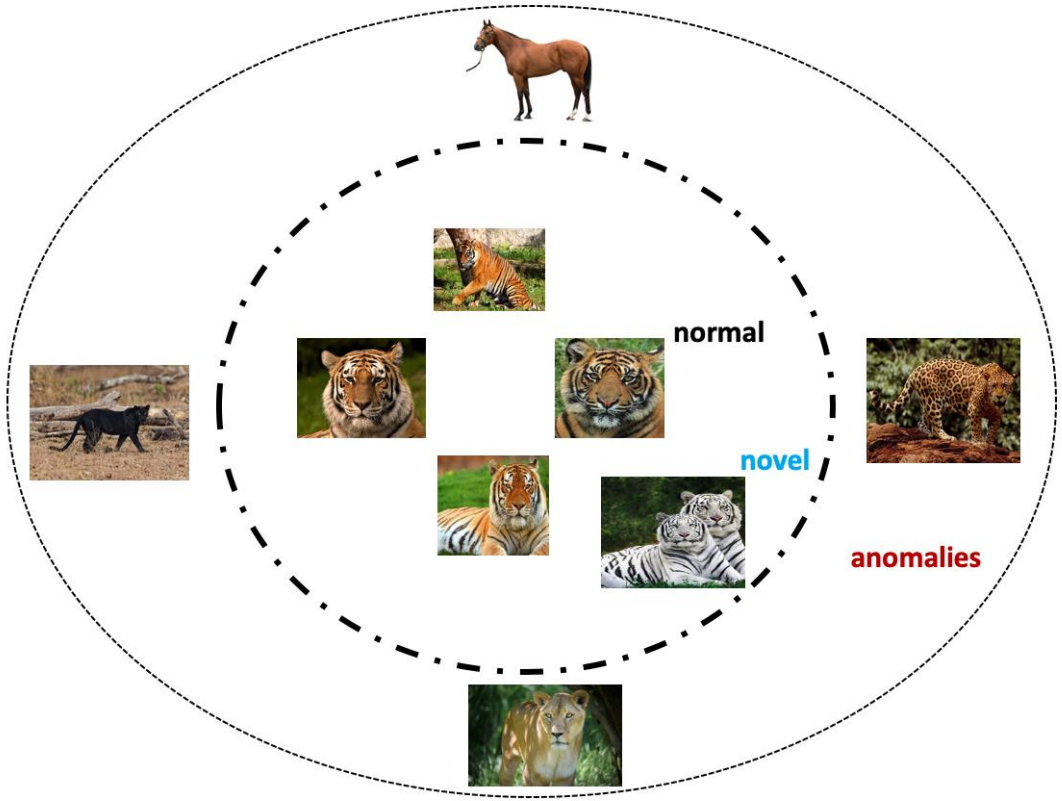


Reference
[1] Anomaly Detection of Time Series, 2010
[2] Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery, 2017

Anomaly Detection

Nomral(정상) sample과 Abnormal(비정상, 이상치, 특이치) sample을 구별해내는 문제

Anomaly VS Novelty

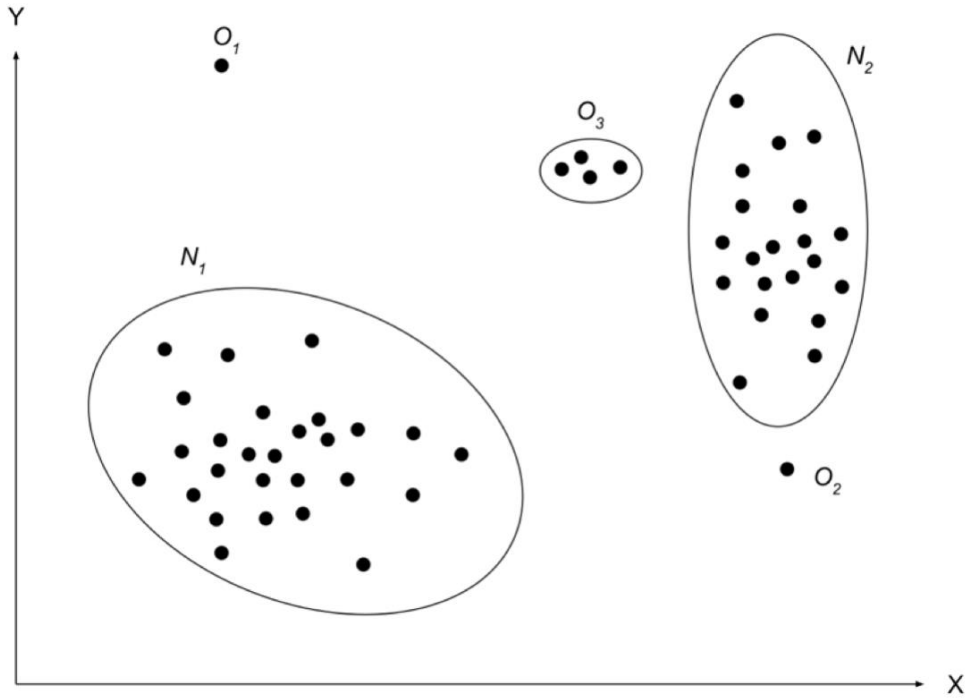


Anomaly = abnormality, deviant, outlier

Novelty = novel (new) or unobserved patterns

https://arxiv.org/pdf/1901.03407.pdf

Types of Anomaly Data



- Point
- Contextual or Conditional
- Collective or Group

https://arxiv.org/pdf/1901.03407.pdf

Anomaly Detection 연구 분야 용어 정리

1. 학습시 비정상 sample 사용여부 및 label 유무에 따른 분류
2. 비정상 sample 정의에 따른 분류
3. 정상 sample의 class 개수에 따른 분류

https://hoya012.github.io/blog/anomaly-detection-overview-1/

1. 비정상 sample 사용 여부 및 Label 유무에 따른 분류

- Supervised Anomaly Detection
- Semi-Supervised(=One-Class) Anomaly Detection
- Unsupervised Anomaly Detection

Supervised Anomaly Detection

데이터셋에 정상 sample과 비정상 sample이 모두 존재하는 경우에 사용 가능
비정상 sample이 다양하고 많이 보유할수록 더 높은 성능을 기대할 수 있음

But, 실제 상황에서는 비정상 sample의 발생빈도가 현저히 적기 때문에
'Class-Imbalance' 문제가 발생

장점 : 정상 / 비정상 판정 정확도가 높다.

단점 : 비정상 sample을 취득하는데 시간과 비용이 오래 걸림,
'Class-Imbalance' 문제를 해결해야 함

https://hoya012.github.io/blog/anomaly-detection-overview-1/

Semi-Supervised(One-Class) Anomaly Detection

Supervised 방식의 가장 큰 문제는
비정상 sample 확보하는데 많은 시간과 비용이 든다는 것!

이처럼 Class-Imbalance가 심하면
정상 sample만 이용해서 모델을 학습하기도 하는데,
이때, **One-class Classification** 방식을 사용 ex) One-Class SVM, Deep SVDD

장점 : 비교적 활발하게 연구가 진행되고 있으며,
정상 sample만 있어도 학습이 가능

단점 : Supervised 방법론과 비교했을 때 상대적으로 정확도가 떨어짐

https://hoya012.github.io/blog/anomaly-detection-overview-1/

Unsupervised Anomaly Detection

대부분의 데이터가 정상 sample이라는 가정을 하여
Label 취득 없이 학습을 시키는 Unsupervised Anomaly Detection

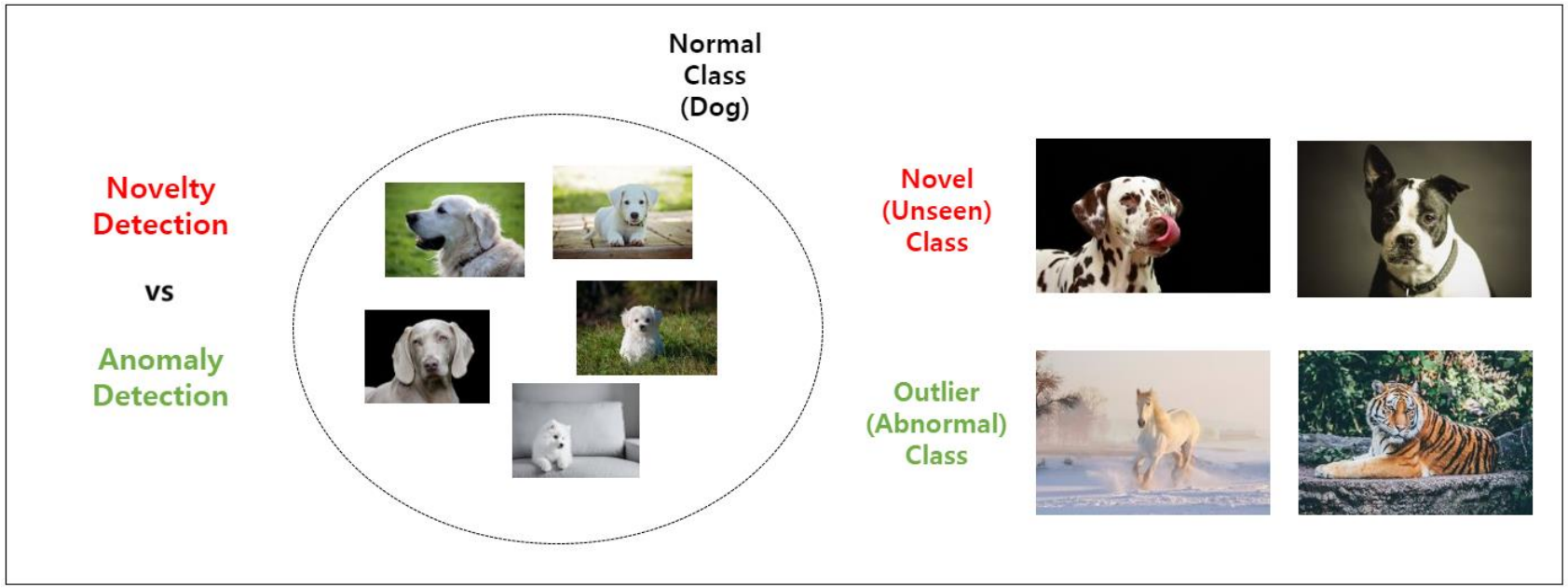
PCA or AutoEncoder를 사용하여 Unsupervised 진행

장점 : Labeling 과정이 필요하지 않음

단점 : 정확도가 그다지 높지 않고, hyper parameter에 매우 민감

https://hoya012.github.io/blog/anomaly-detection-overview-1/

2. 비정상 sample 정의에 따른 분류

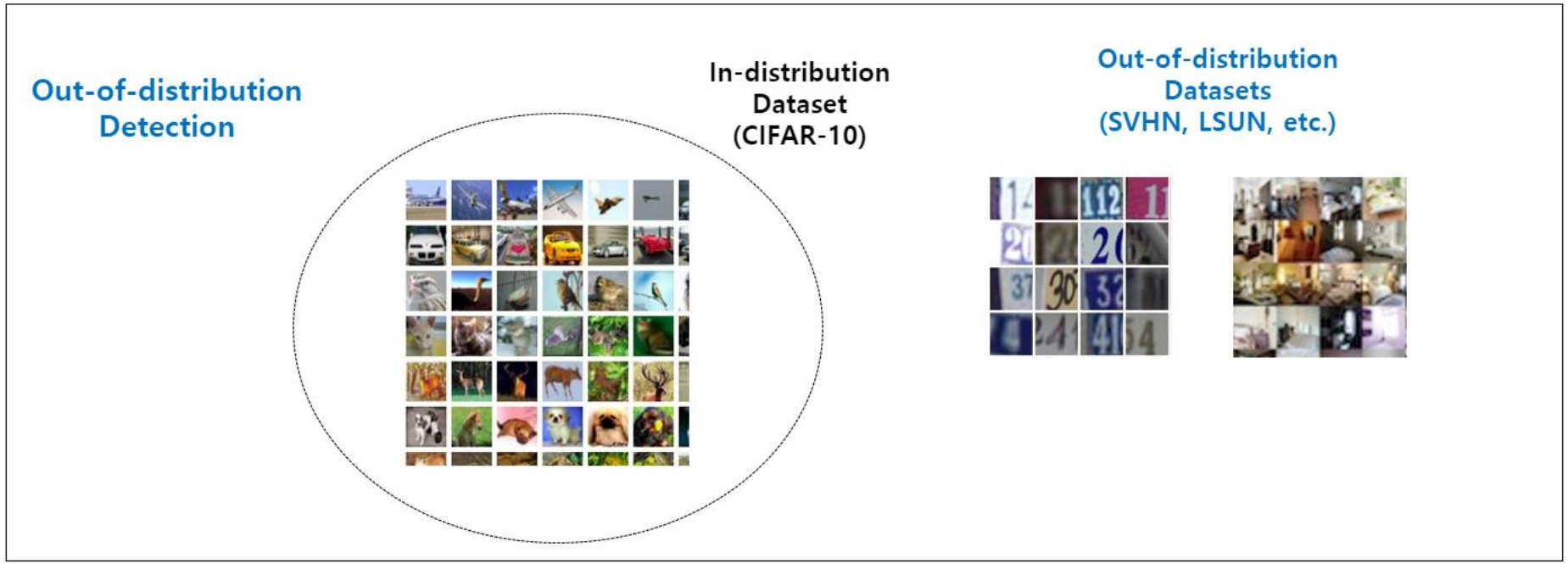


Novelty Detection은 현재 등장하진 않았지만, 충분히 등장할 수 있는 sample
Outlier Detection은 등장할 가능성이 거의 없는, 데이터 오염 가능성이 있는 sample

Anomaly Detection = Novelty Deteciton + Outlier Detection

https://hoya012.github.io/blog/anomaly-detection-overview-1/

3. 정상 sample의 class 개수에 따른 분류 (multi class인 경우)

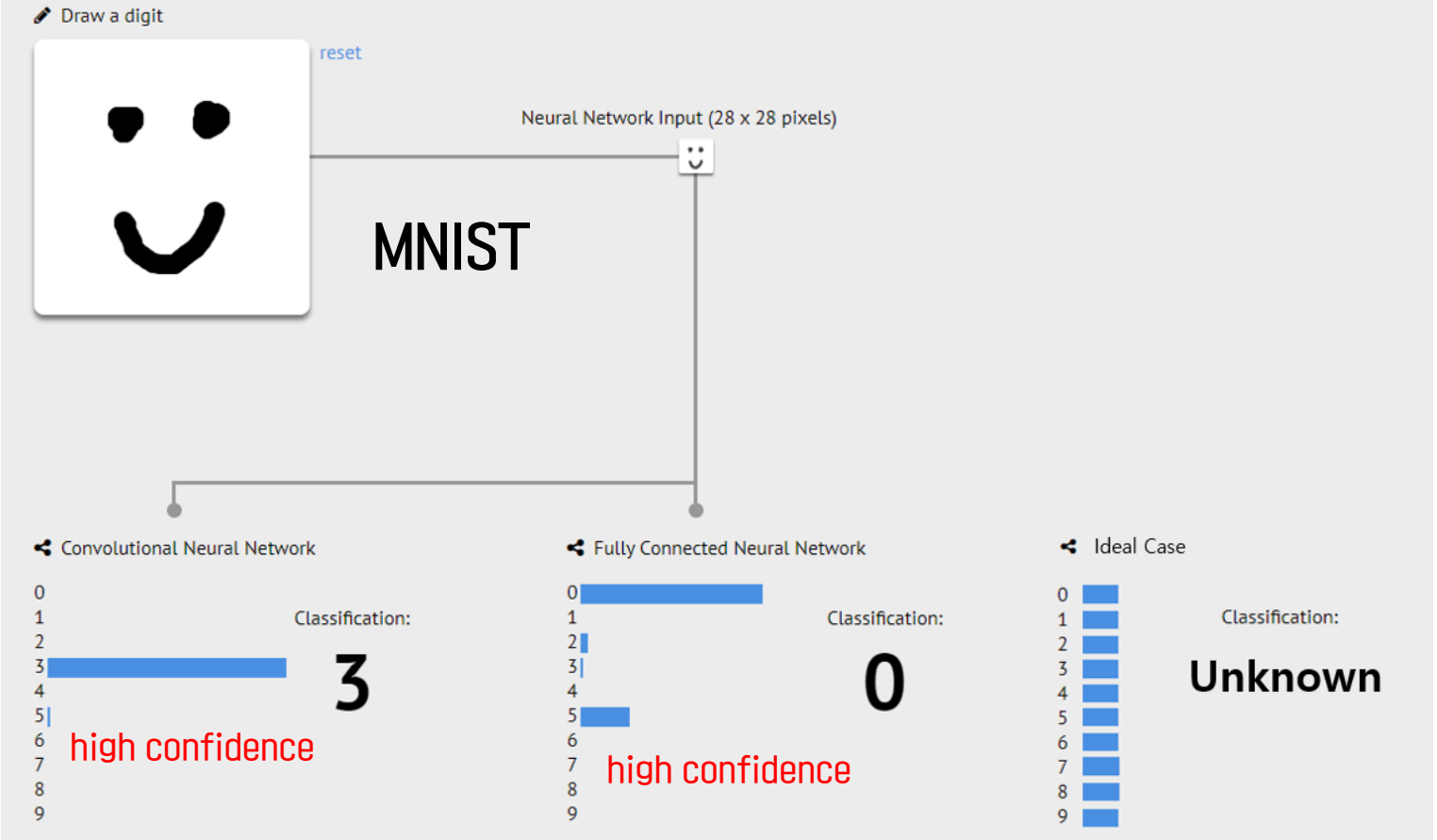


https://hoya012.github.io/blog/anomaly-detection-overview-1/

Out-of-Distribution

$$\sigma(\vec{z})_i = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}}$$

softmax



https://hoya012.github.io/blog/anomaly-detection-overview-1/

Out-of-Distribution

’Unknown Class’ Problem

1. 이미 학습된 모델을 다시 학습
2. 다양한 Unknown sample을 수집

So, Out-of-Distribution-detection 분야가 활발히 연구 진행중

https://hoya012.github.io/blog/anomaly-detection-overview-1/

3. Application

Anomaly Detection Model

- SVM (OC-SVM, SVDD)
- Isolation Forest
- Clustering
- AutoEncder
- Word2Vec
- GAN
- Deep SVDD

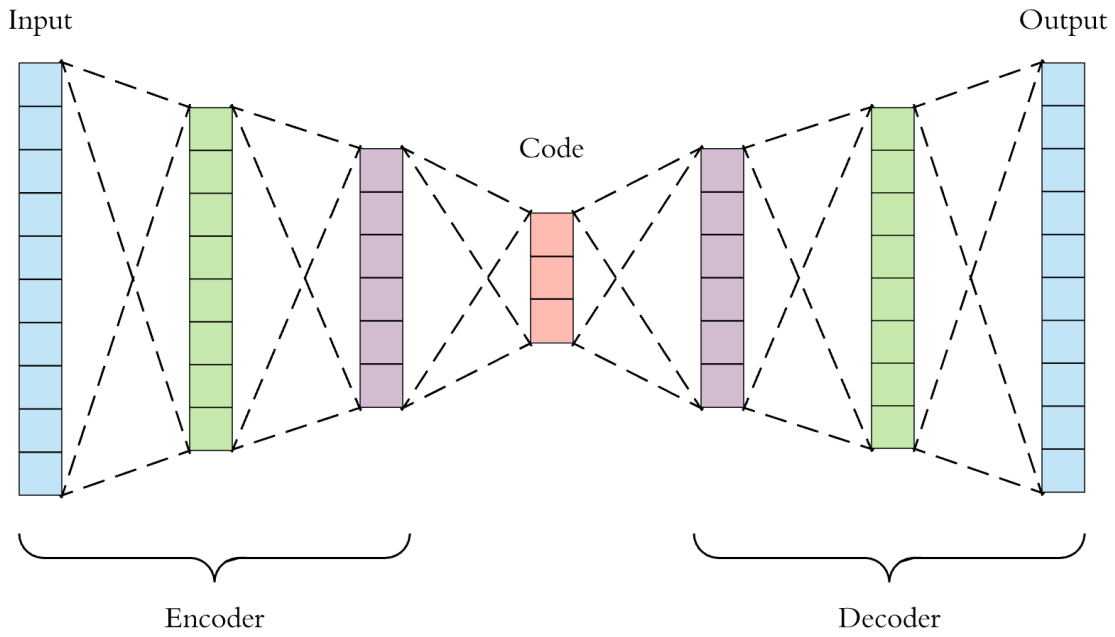
https://www.youtube.com/watch?v=wSgnhxZ3iQo

Anomaly Detection Model

- SVM (OC-SVM, SVDD)
- Isolation Forest
- Clustering
- AutoEncder
- Word2Vec
- GAN
- Deep SVDD

https://www.youtube.com/watch?v=wSgnhxZ3iQo

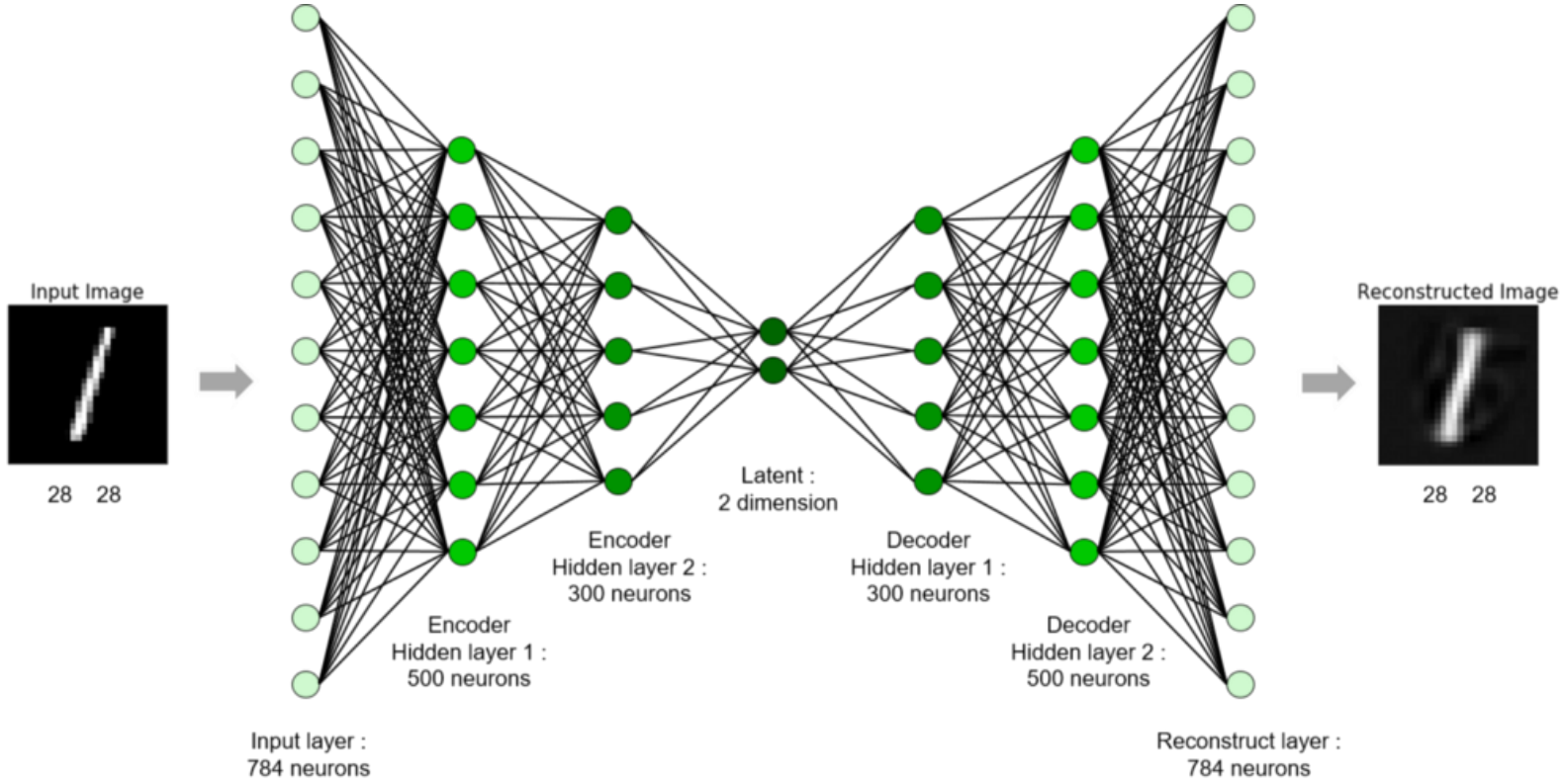
Anomaly Detection Model - AutoEncoder



Encoder와 Decoder로 구성되어 있는데,
Encoder 는 차원을 축소하여 Vector를 생성하고 Decoder는 Vector로부터 원본 데이터를 복원

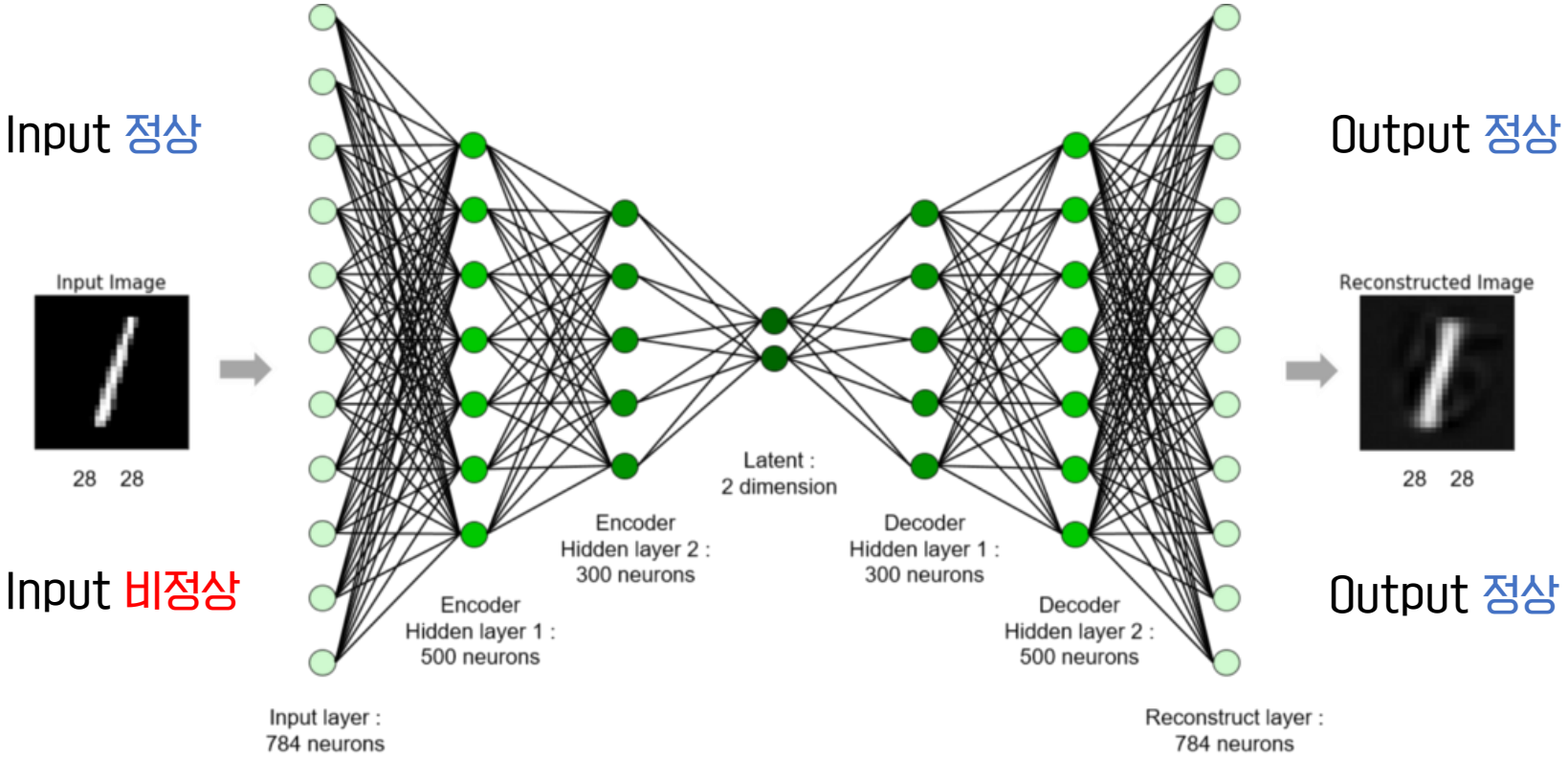
https://gaussian37.github.io/dl-concept-autoencoder2/

Anomaly Detection Model - AutoEncoder



https://techblog-history-younghunjo1.tistory.com/130

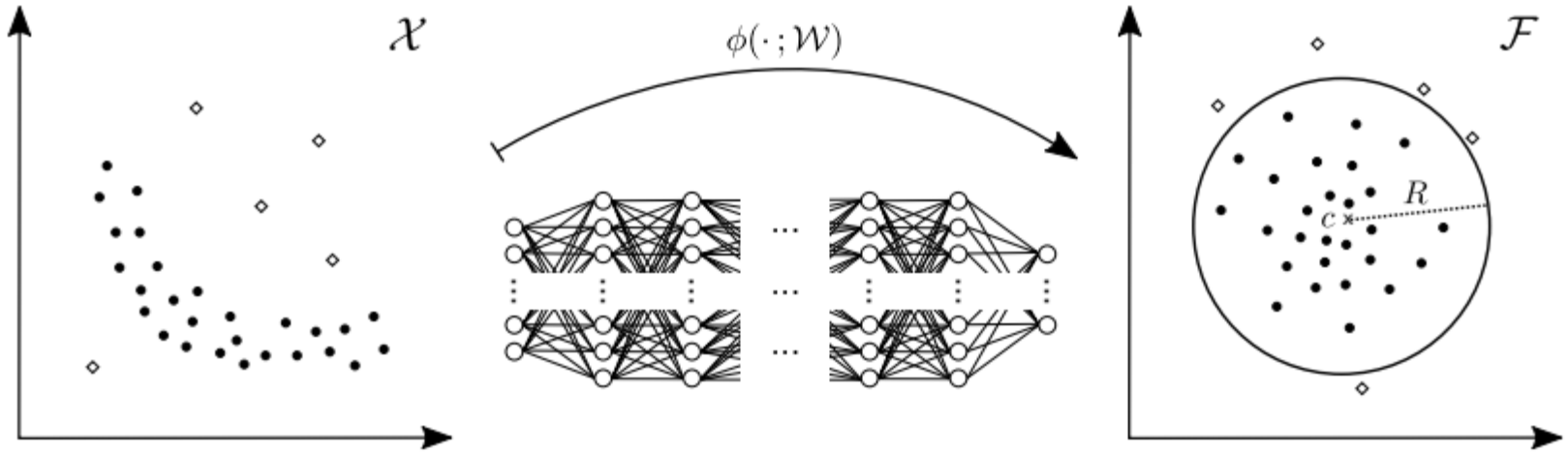
Anomaly Detection Model - AutoEncoder



Input 과 Output에서 차이가 발생 → 비정상 sample 검출!

https://techblog-history-younghunjo1.tistory.com/130

Anomaly Detection Model - Deep-SVDD

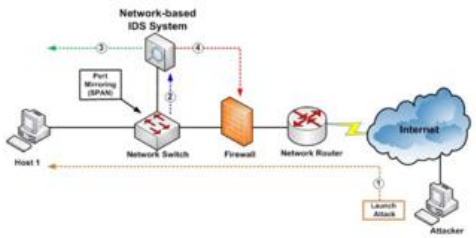


타 모델들과 달리, Anomaly Detection을 위하여 개발된 모델

http://proceedings.mlr.press/v80/ruff18a/ruff18a.pdf

Anomaly Detection Application

Cyber-intrusion

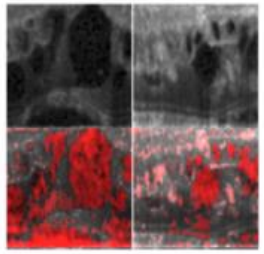


Log file

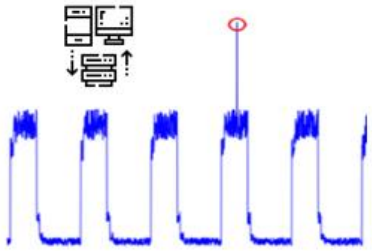
Fraud

Malware

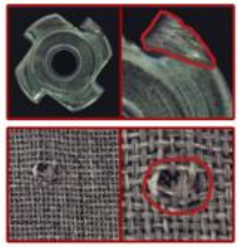
Medical



Social Network



IoT Big-Data



Industrial

Video Surveillance

https://hoya012.github.io/blog/anomaly-detection-overview-1/

Reference Paper.

1. Raghavendra Chalapathy, et al, “Deep Learning for Anomaly Detection: A Survey”, 2019.

2. Lukas Ruff, et al, “Deep One-Class Classification”, In ICML, 2018.

QnA?

Thank You!