동형암호 기반 프라이버시 보존 CNN 알고리즘 개발 꿀팁 대방출

최현민
NAVER Cloud

NAVER DEVIEW 2023

CONTENTS

1.동형암호 기반 머신러닝 소개

1.1 머신러닝 기술과 프라이버시

NAVER
DEVIEW
2023

시리즈 AI&산업

[스페셜리포트]① 화장실에도 들어온 얼굴 인식 기술, 어디까지 갈까?

AI타임스
2021.08.27. 09:

접촉 없이 신원 증명 기
은행, 공항 등 신원인증
딥러닝으로 빠르고 정

This WACV 2020 paper is the Open Access version, provided by the Computer Vision Foundation.
Except for this watermark, it is identical to the accepted version;
the final published version of the proceedings is available on IEEE Xplore.

Can a CNN Automatically Learn the Significance of Minutiae Points for Fingerprint Matching?

Anurag Chowdhury*, Simon Kirchgasser+, Andreas Uhl+, Arun Ross*
*Michigan State University, USA
+University of Salzburg, Austria
{chowdh51, rossarun}@cse.msu.edu, {skirch, uhl}@cs.sbg.ac.at

글로벌경제신문

[창간8주년]인공지능(AI)과 의료 기술의 결합에 진화하는 '디지털 헬스케어'

의료 AI기술 도입 사례 "△영상 △음성 △정밀 의료 분야" 현황 분석

이재승 의학전문기자 / 바이오 의·공학 박사

입력 2022.08.25 11:18 | 댓글 0

1.1 머신러닝 기술과 프라이버시

NAVER
DEVIEW
2023

머신러닝 기술, 편리한 만큼 안전할까?


데일리안

‘AI 이루다’ 개인정보 못 걸러냈다… 가명정보 사업 안전할까?

입력 2021.01.13. 오후 1:08

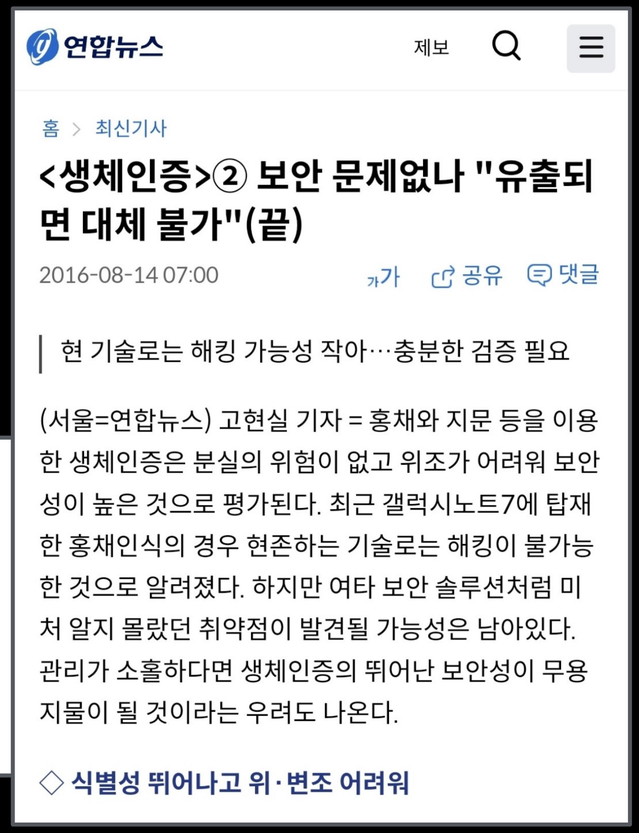
이호연 기자 >


아시아경제 구독

일상 엿듣는 AI…'사생활 침해' VS '불가피한 학습과정'

입력 2019.09.04. 오전 8:12 · 수정 2019.09.04. 오전 8:13 기사원문

이민우 기자


연합뉴스 제보

홈 > 최신기사

<생체인증>② 보안 문제없나 "유출되면 대체 불가"(끝)

2016-08-14 07:00 가가 공유 댓글

현 기술로는 해킹 가능성 작아…충분한 검증 필요

(서울=연합뉴스) 고현실 기자 = 홍채와 지문 등을 이용한 생체인증은 분실의 위험이 없고 위조가 어려워 보안성이 높은 것으로 평가된다. 최근 갤럭시노트7에 탑재한 홍채인식의 경우 현존하는 기술로는 해킹이 불가능한 것으로 알려졌다. 하지만 여타 보안 솔루션처럼 미처 알지 몰랐던 취약점이 발견될 가능성은 남아있다. 관리가 소홀하다면 생체인증의 뛰어난 보안성이 무용지물이 될 것이라는 우려도 나온다.

◇ 식별성 뛰어나고 위·변조 어려워

1.2 동형암호란 무엇인가?

NAVER
DEVIEW
2023

동형암호란

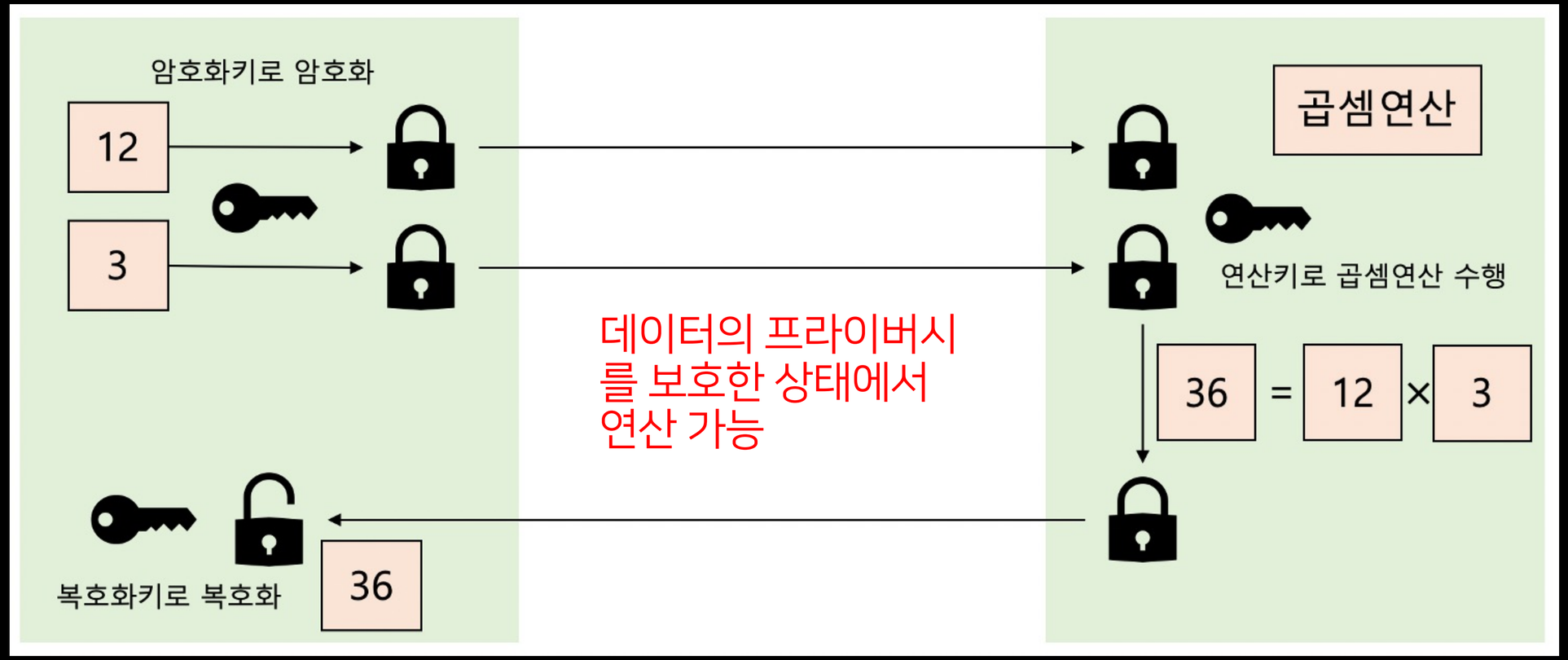
- 암호화된 데이터를 복호화 없이 컴퓨터가 수행하는 모든 연산이 가능한 암호기술
- 2016년 부터 급속도로 실용화 연구가 진행되어 Google, MS Azure, Amazon AWS 에서도 연구 중인 기술
- 동형암호의 키는 암호화키, 복호화키, 연산키로 구성

	암호화키	연산키(계산키)	복호화키
종류	공개키	공개키	비밀키
기능	데이터 암호화시 사용	암호문간 연산 시 사용	암호문의 복호화시 사용

1.2 동형암호란 무엇인가?

NAVER
DEVIEW
2023

암호화된 상태에서 연산이 가능한 암호 알고리즘



1.2 동형암호란 무엇인가?

NAVER DEVIEW 2023

CKKS 알고리즘

- 2016년 Cheon 외 3인은 반올림 연산이 효율적으로 진행 가능한 동형암호 알고리즘 설계 (이하 CKKS)
- 현재 CKKS 기반 동형암호 알고리즘의 연구가 활발히 지속되고 있음

세대	시작 년도	특징	연산	ISO 표준
1세대	2009년	최초 완전동형암호	Bit 연산	-
2세대	2011년	최초의 상용화 가능한 동형암호	정수 연산	BGV, BFV
3세대	2013년	Bitwise 데이터 연산에 효과적인 동형암호	Bit 연산	TFHE
4세대	2016년	최초의 실수 연산을 지원하는 동형암호	실수 연산	CKKS

1.2 동형암호란 무엇인가?

NAVER DEVIEW 2023

하지만 동형암호의 연산 속도는 평문 데이터 연산 속도보다 수십~수백 배 이상 느림

연산	수행 시간(단위 : 초)
Add	0.311
Sub	0.270
Mult	0.258
Variance	0.972
Kurtosis	19.5
Corrlation	50.8s
Max	11m 22s

연산	수행 시간(단위 : 초)
Add	0.0799
Sub	0.0624
Mult	0.0388

테스트 라이브러리 : HEaaN
테스트 스킴 : CKKS
좌 : Full depth (부트스트랩 기능을 통한 곱셈 횟수의 제한 없음)
우 : Depth 3 : 최대 3번 곱셈 가능

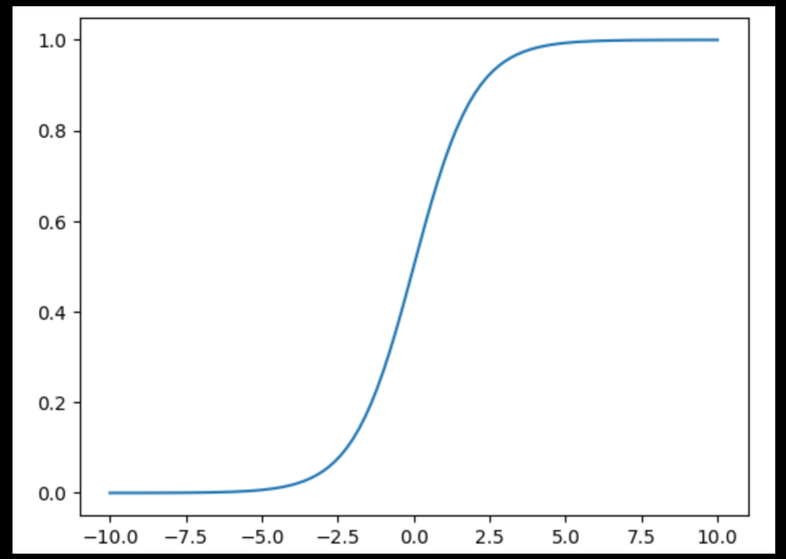
[테스트 환경] Naver Cloud server, RAM : 32GB CORE : 3.0GHz vCPU 8개

1.3 동형암호 기반 머신러닝 사례

NAVER
DEVIEW
2023

1. 로지스틱 회귀(Logistic Regression)

- 독립변수의 선형결합을 통해 사건의 발생 가능성을 예측하는 알고리즘
- 로지스틱 함수를 선형회귀에 적용
- 분류 문제에 주로 사용됨

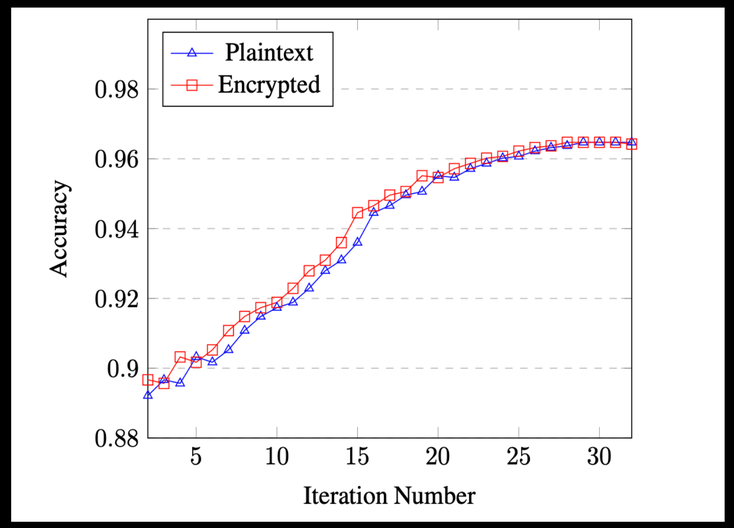


로지스틱 함수 그래프

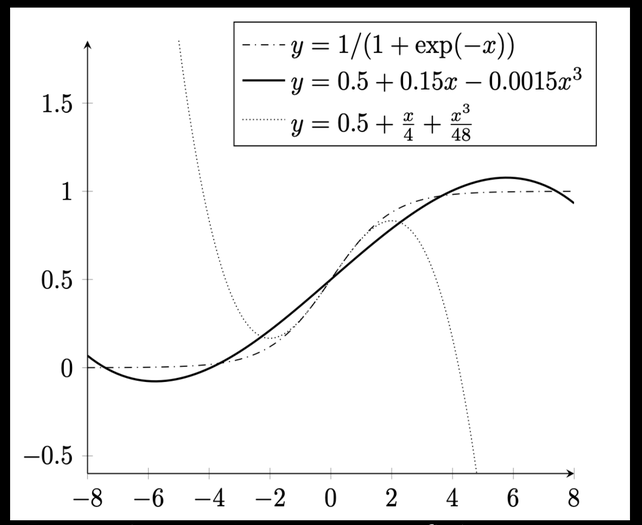
1.3 동형암호 기반 머신러닝 사례

NAVER
DEVIEW
2023

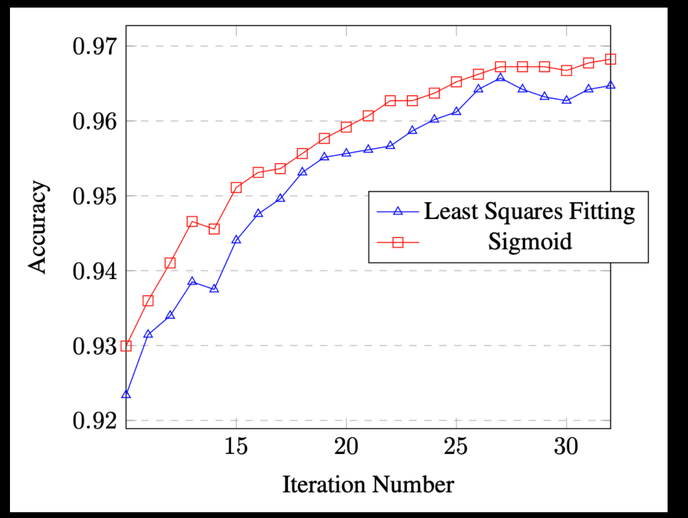
1. 로지스틱 회귀(Logistic Regression)



Accuracy by Iteration Number



Comparison to Least squares fitting on sigmoid curve and Talyer Expansion curve



The Comparison of accuracy between the Least Squares Fitting and Sigmoid

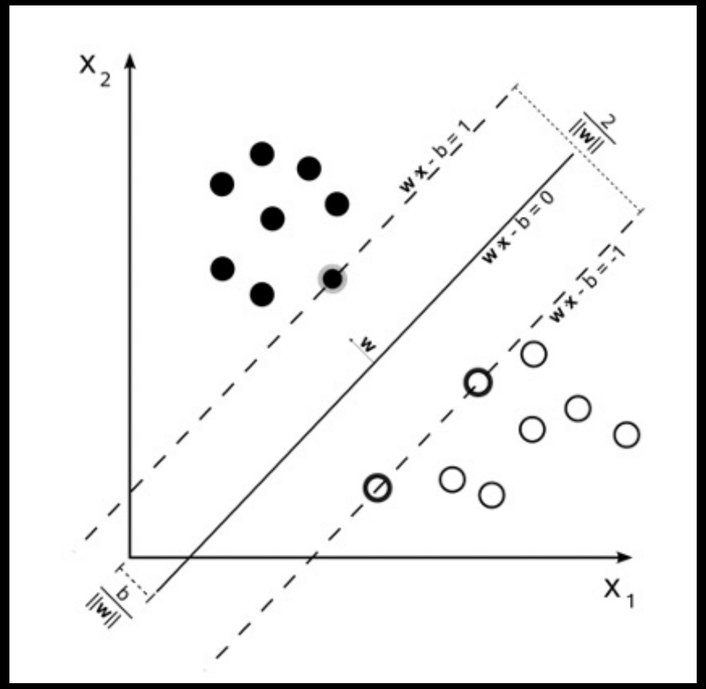
- Tayler Series 대신 Least Squares Fitting을 사용하여 Sigmoid를 비교적 낮은 차수인 3차 다항식으로 구현

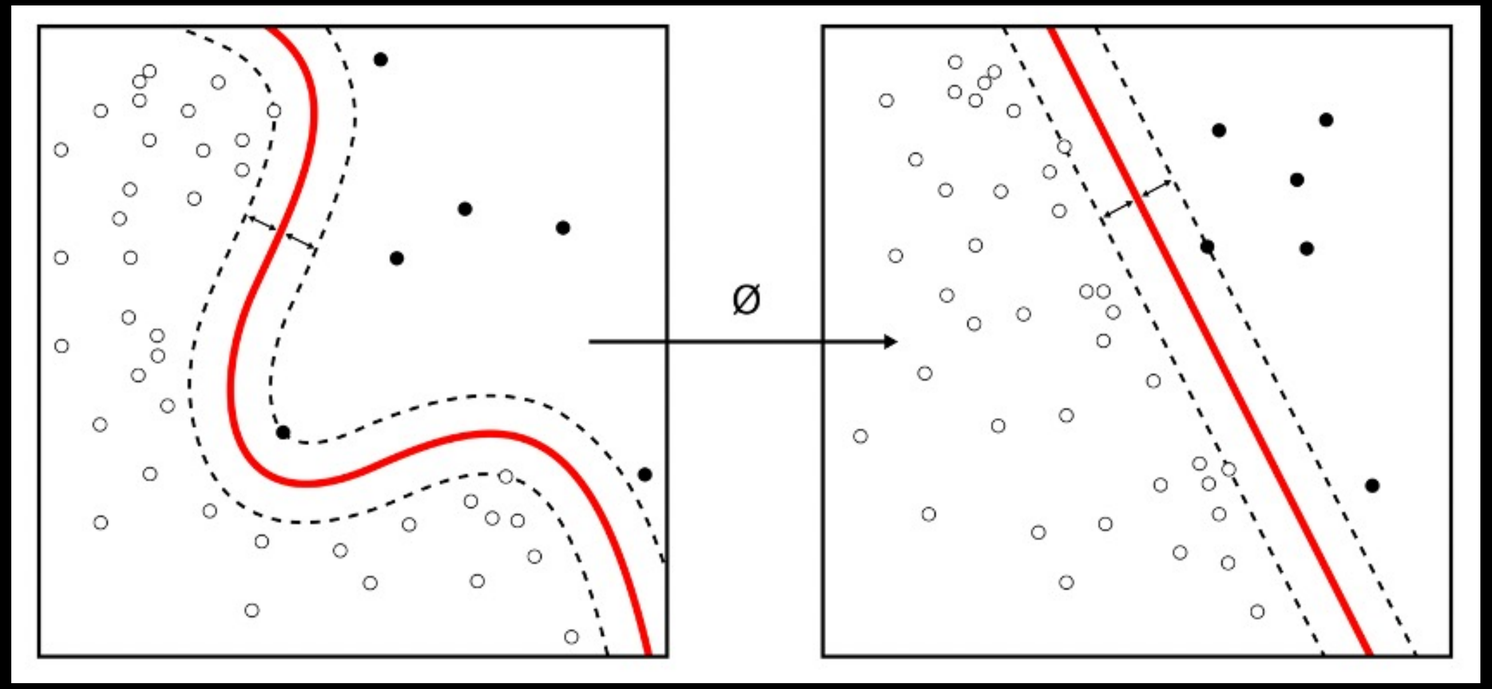
[출처] https://ojs.aaai.org//index.php/AAAI/article/view/5000

1.3 동형암호 기반 머신러닝 사례

NAVER
DEVIEW
2023

2. 서포트 벡터 머신(Support Vector Machine, SVM)



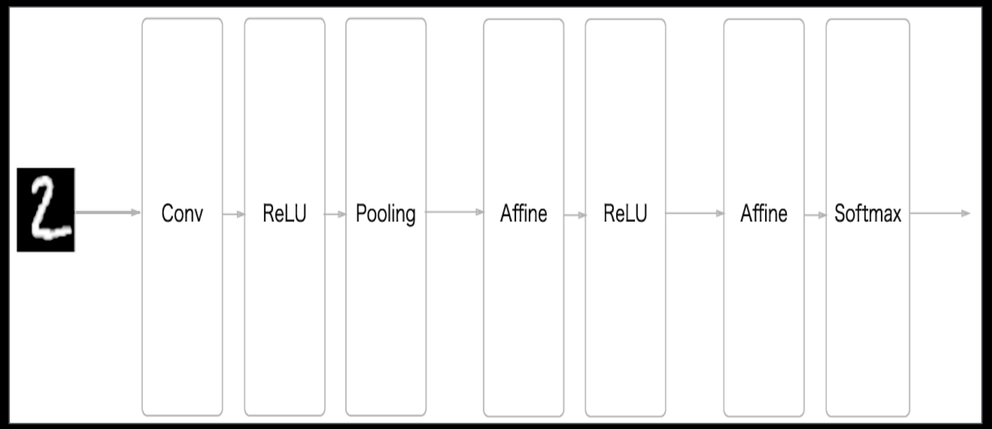


[출처] https://ko.wikipedia.org/wiki/%EC%84%9C%ED%8F%AC%ED%8A%B8_%EB%B2%A1%ED%84%B0_%EB%A8%B8%EC%8B%A0

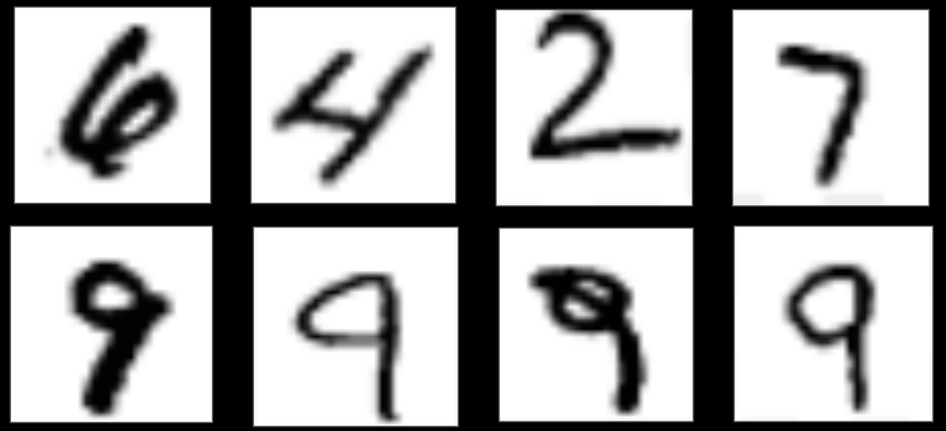
1.3 동형암호 기반 머신러닝 사례

NAVER
DEVIEW
2023

3. CNN(Convolutional Neural Network)



CNN 알고리즘의 구조



MNIST 손글씨 데이터셋

- CNN은 이미지나 영상 데이터를 처리할 때 주로 사용되는 딥러닝 모델
- 기존 딥러닝 모델과 다르게 Convolution 계층이 있어 이미지의 공간적/지역적 정보 유지

[출처] https://github.com/youbeebee/deeplearning_from_scratch

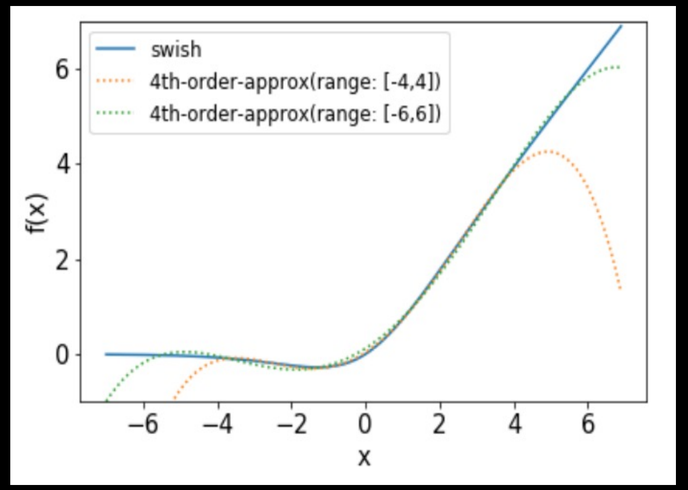
[출처] https://ko.wikipedia.org/wiki/MNIST_%EB%8D%B0%EC%9D%B4%ED%84%B0%EB%B2%A0%EC%9D%B4%EC%8A%A4

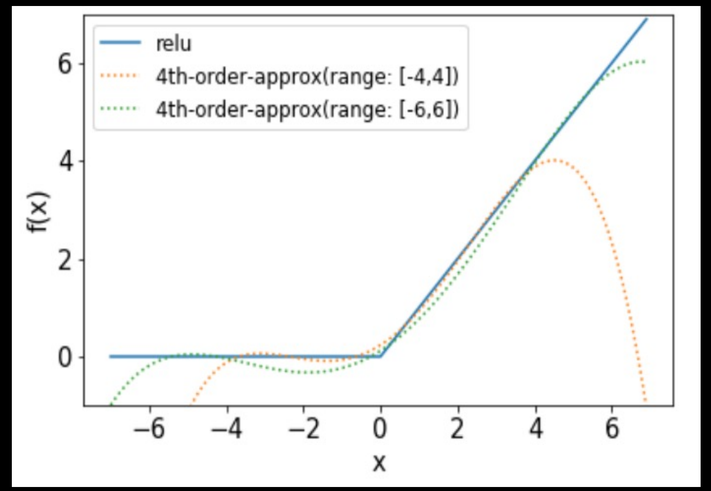
1.3 동형암호 기반 머신러닝 사례

NAVER DEVIEW 2023

3. CNN(Convolutional Neural Network)

Activation function	deg ree	x-axis range to be fitted	polynomial approximated
Swish	4	$[-4, 4]$	$0.03347 + 0.5x + 0.19566x^2 - 0.005075x^4$
		$[-6, 6]$	$0.1198 + 0.5x + 0.1473x^2 - 0.002012x^4$
	2	$[-4, 4]$	$0.12592 + 0.5x + 0.145276x^2$
		$[-6, 6]$	$0.0851505 + 0.5x + 0.344125x^2$
ReLU	4	$[-4, 4]$	$0.234606 + 0.5x + 0.204875x^2 - 0.0063896x^4$
		$[-6, 6]$	$0.119782 + 0.5x + 0.147298x^2 - 0.002015x^4$
	2	$[-4, 4]$	$0.375373 + 0.5x + 0.117071x^2$
		$[-6, 6]$	$0.563059 + 0.5x + 0.078047x^2$





- 기존의 비선형 활성화 함수를 4차 이하의 근사다항식으로 대체

=> 약간의 정확도는 하락하나 연산 속도 면에서 월등히 빨라짐

[출처] https://arxiv.org/abs/2009.03727

2. 동형암호 기반 CNN 알고리즘 구현 꿀팁 대방출

2.1 CNN 알고리즘 소개

NAVER
DEVIEW
2023

CNN(Convolutional Neural Network)

1. Convolutional Filter
2. Pooling
3. Batch Normalization
4. Activation

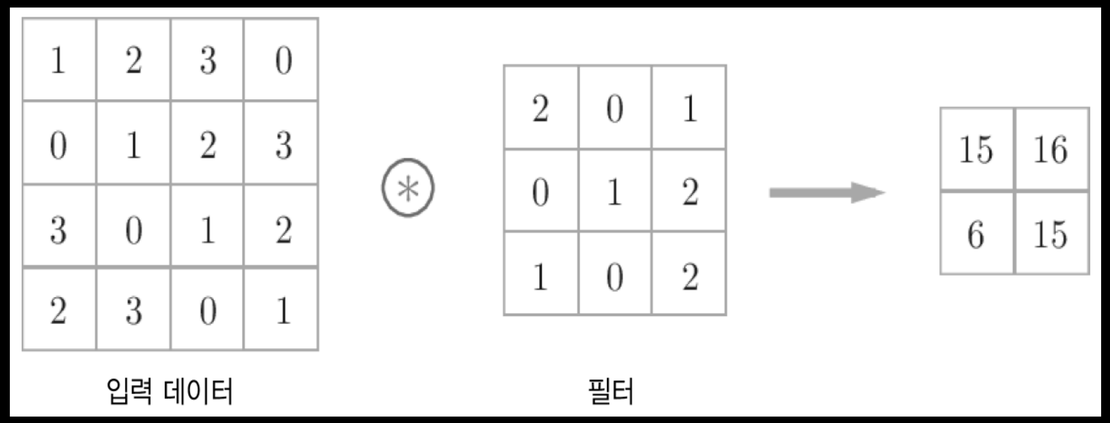
2.1 CNN 알고리즘 소개

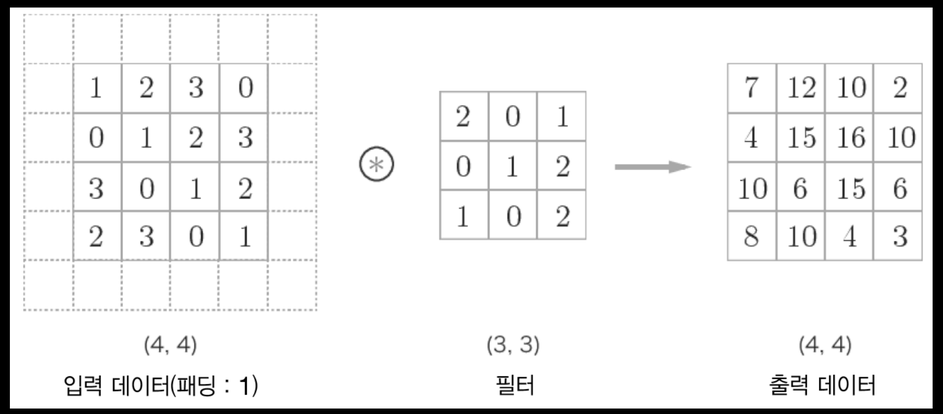
NAVER
DEVIEW
2023

1. Convolutional Layer

Convolutional Layer에서는 필터를 이동하여 합성곱 연산을 수행

- stride : 필터의 이동 칸 수를
- padding : 합성곱 연산 시 이미지가 작아지기 때문에 둘레에 0을 더하는 과정





[출처] https://github.com/youbeebee/deeplearning_from_scratch/blob/master/images/fig%207-3.png

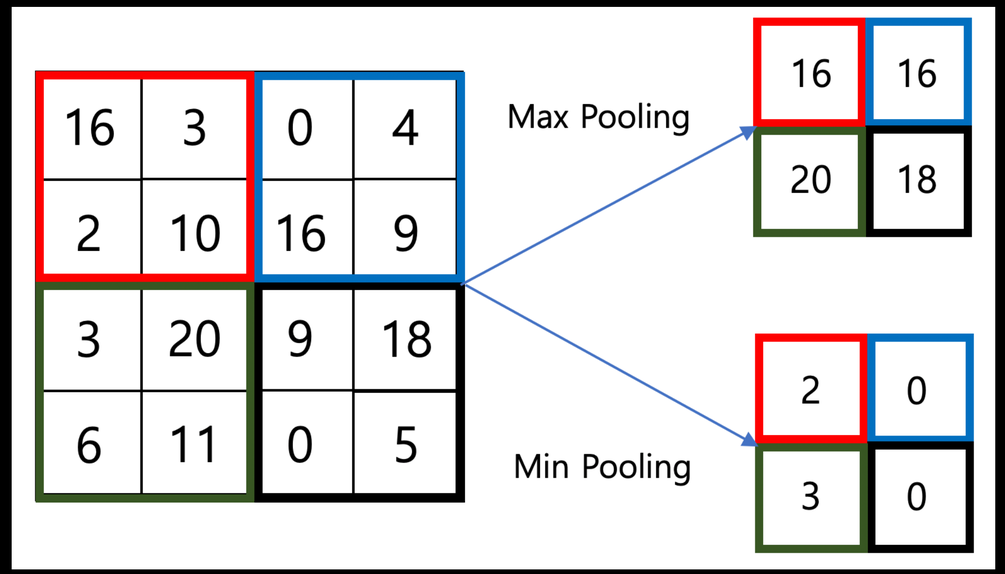
[출처] https://github.com/youbeebee/deeplearning_from_scratch/blob/master/images/fig%207-6.png

2.1 CNN 알고리즘 소개

NAVER
DEVIEW
2023

2. Pooling Layer

- 이미지의 크기를 줄이는 방법
- 크게 Max pooling, Min pooling, Average Pooling 이 있음



2.1 CNN 알고리즘 소개

NAVER
DEVIEW
2023

3. Batch Normalization

- 각 배치 단위 별로 평균과 분산을 활용해 데이터의 분포를 정규화 하는 과정
- 배치 단위 간 데이터의 분포 차이로 인한 학습 성능 하락을 막을 수 있음

2.1 CNN 알고리즘 소개

NAVER
DEVIEW
2023

4. 활성화 함수(Activation)

- 딥러닝에서 각 레이어마다 적용하는 비선형 함수
- 활성화함수를 통해 딥러닝의 층을 깊게 할 수 있음

(ex, f1, f2, f3가 선형 함수이면 g(x) = f3(f2(f1(x))) 역시 선형 함수가 되어 딥러닝의 층을 깊게 만들수 없음)

- 대표적인 활성화 함수에는 ReLU, Sigmoid 등이 있음

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER
DEVIEW
2023

알고리즘 개발 단계에서 여러 시행착오를 겪음

(1) Convolutional 계층을 어떻게 구현할 수 있을까?

(2) 동형암호 연산 횟수를 줄이는 방법은?

(3) SIMD based Architecture

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

Requirement

곱셈의 횟수를 제한 없이 연산이 가능한 Bootstrapping은 속도가 매우 느리기 때문에 실시간 서비스에 적합한 연산이 아님

=> 기술적으로 아무리 최적화를 하더라도 현재 동형암호 기술의 한계로 인해 연산 속도는 평문의 연산속도보다 현저히 느림

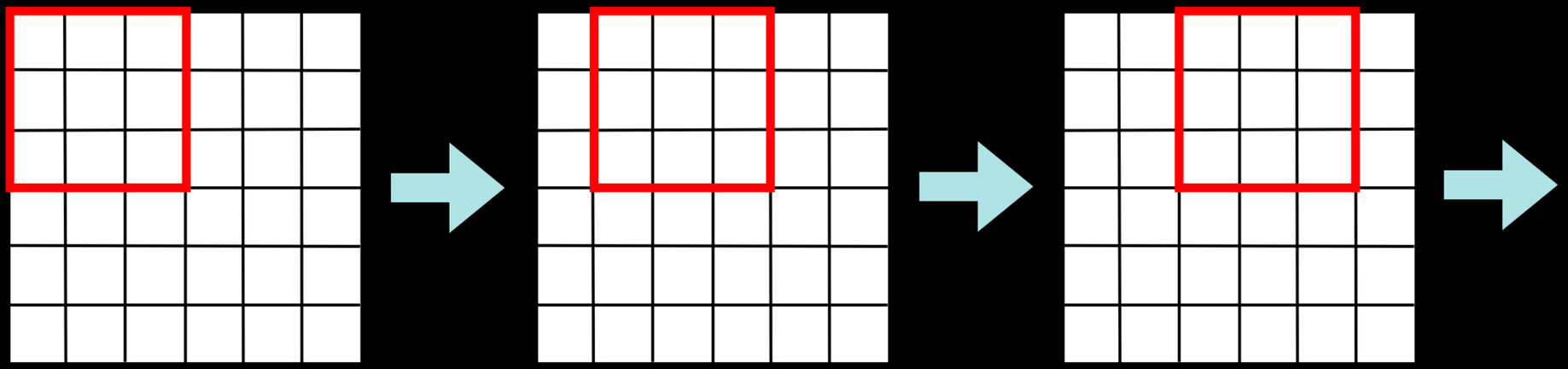
=> Bootstrapping 없이 최대한 빠르게 CNN 연산이 가능하도록 알고리즘 개발 필요

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(1) Convolutional 계층을 어떻게 구현할 수 있을까?

- Filter의 이동 횟수는 Filter의 사이즈와 Stride 크기에 비례해서 증가
- Filter가 이동할 때 마다 동형암호 연산(Mult, Add, Rotation)이 수행되므로 합리적인 연산 방법이 필요

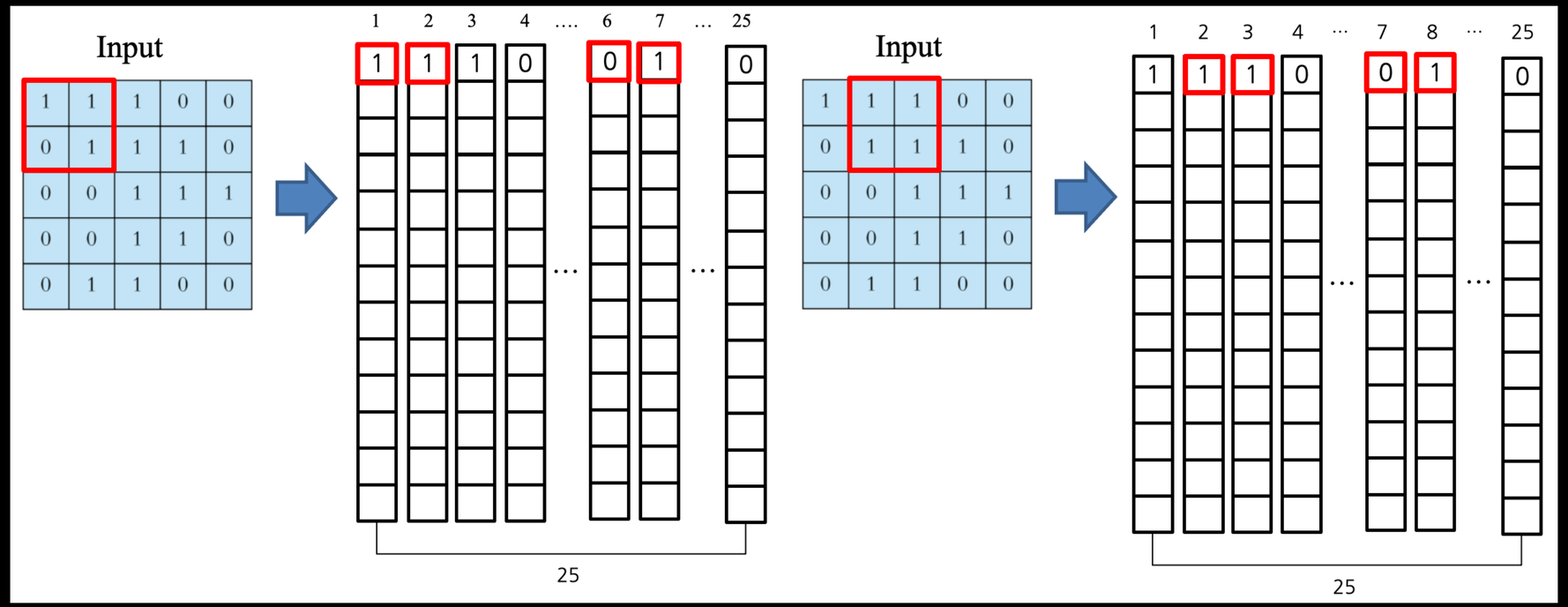


2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(1) Convolutional 계층을 어떻게 구현할 수 있을까?

- 일반적인 구현 방식

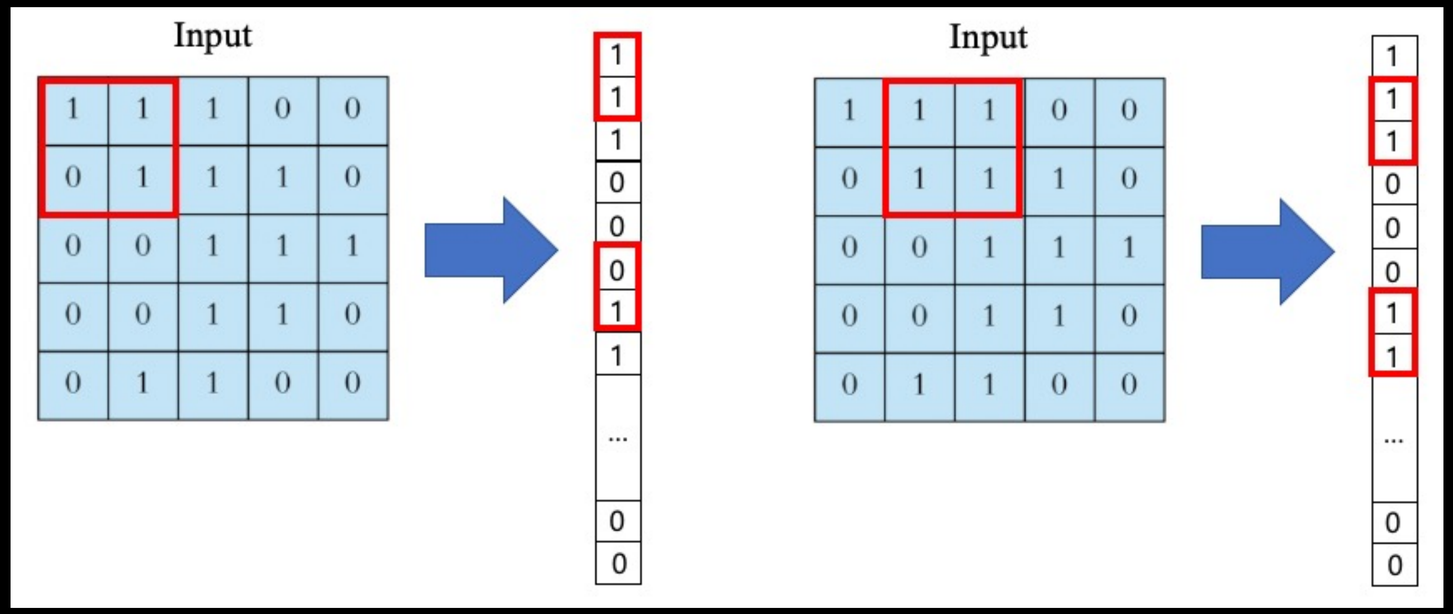


2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(1) Convolutional 계층을 어떻게 구현할 수 있을까?

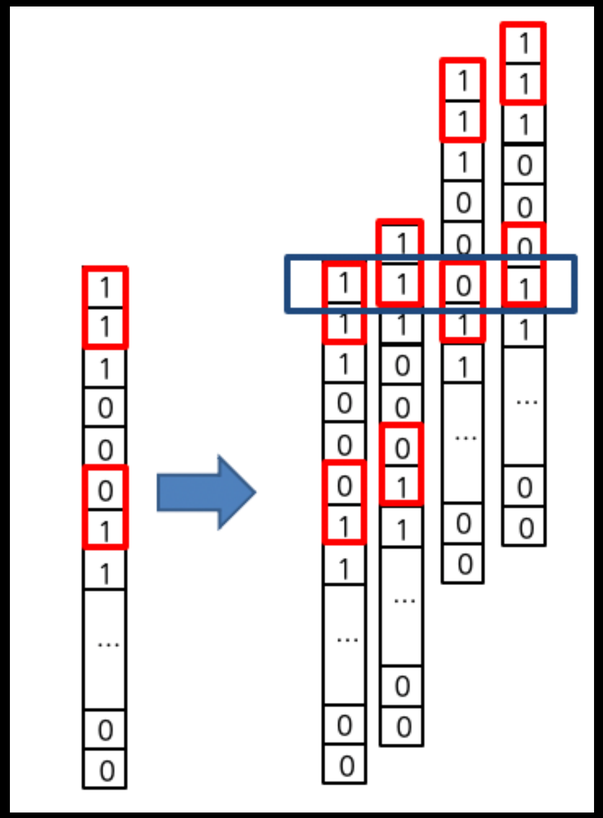
- 하나의 암호문에 2d인 이미지를 1d로 변경하여 연산



2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(1) Convolutional 계층을 어떻게 구현할 수 있을까?



파란 부분을 더하면 빨간 부분의 합이 나옴

→ 필터곱의 합 계산 가능

→ 필터의 원소 갯수 만큼의 rotation과 addition만 수행하면 됨

2.2 동형암호 기반 CNN 구현 꿀팁 대방출

NAVER
DEVIEW
2023

꿀팁 #1

Packing을 잘 활용하여 합성곱 연산을 구현하자!

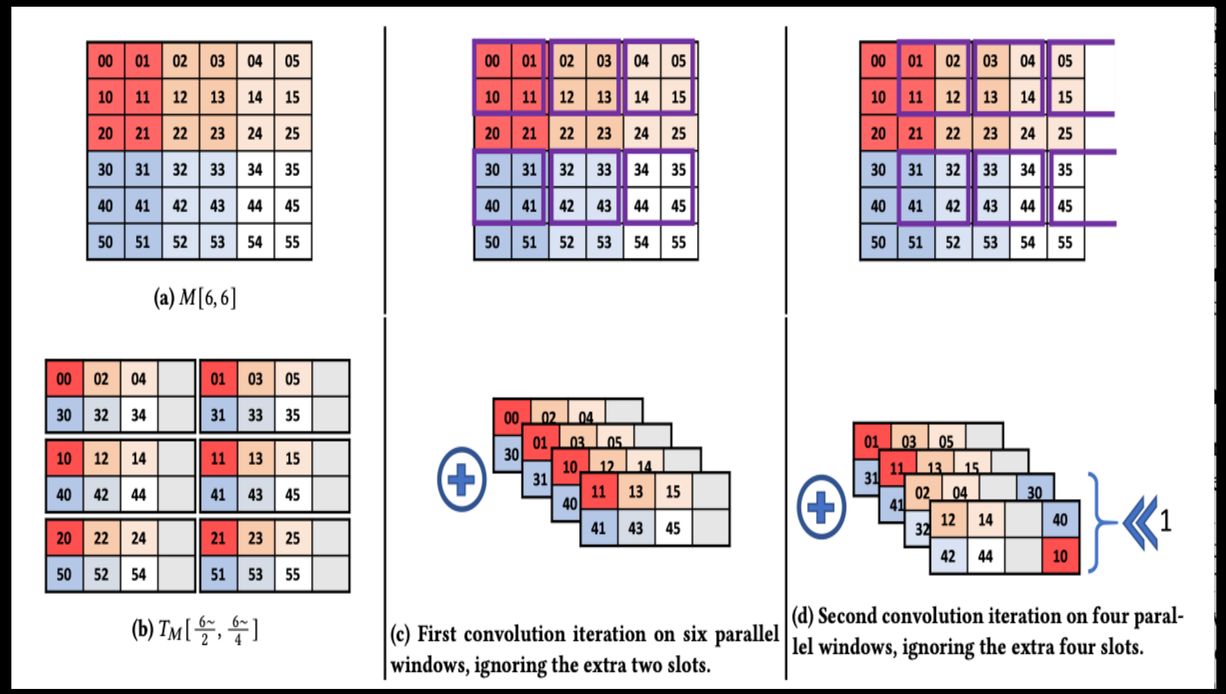
- Packing을 잘 활용하면 보다 효율적으로 합성곱 연산 계산이 가능
- 동형암호 연산에서 rotation 연산과 덧셈을 잘 활용하면 곱셈의 횟수를 줄일 수 있음
- 하지만, rotation연산이 무조건 곱셈보다 효율적인 것은 아니므로, 적절한 tradeoff가 필요함

2.2 동형암호 기반 CNN 구현 꿀팁 대방출

NAVER DEVIEW 2023

꿀팁 #1

Packing을 잘 활용하여 합성곱 연산을 구현하자!



[출처] https://arxiv.org/pdf/2011.01805.pdf

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(2) 동형암호 연산 횟수를 줄이는 방법은?

- 합성곱 연산의 문제를 해결했으나 ReLU, SeLU 등 비선형 활성화 함수는 동형암호의 덧셈과 곱셈, rotation 연산으로 간단하게 나타내기 어려움.
- 찾아본 결과 활성화 함수는 낮은 차수의 다항식으로 근사화하는 연구들이 보임

TABLE II. POLYNOMIAL APPROXIMATION RESULT

Activation function	degree	x-axis range to be fitted	polynomial approximated
Swish	4	$[-4, 4]$	$0.03347 + 0.5x + 0.19566x^2 - 0.005075x^4$
		$[-6, 6]$	$0.1198 + 0.5x + 0.1473x^2 - 0.002012x^4$
	2	$[-4, 4]$	$0.12592 + 0.5x + 0.145276x^2$
		$[-6, 6]$	$0.0851505 + 0.5x + 0.344125x^2$
ReLU	4	$[-4, 4]$	$0.234606 + 0.5x + 0.204875x^2 - 0.0063896x^4$
		$[-6, 6]$	$0.119782 + 0.5x + 0.147298x^2 - 0.002015x^4$
	2	$[-4, 4]$	$0.375373 + 0.5x + 0.117071x^2$
		$[-6, 6]$	$0.563059 + 0.5x + 0.078047x^2$

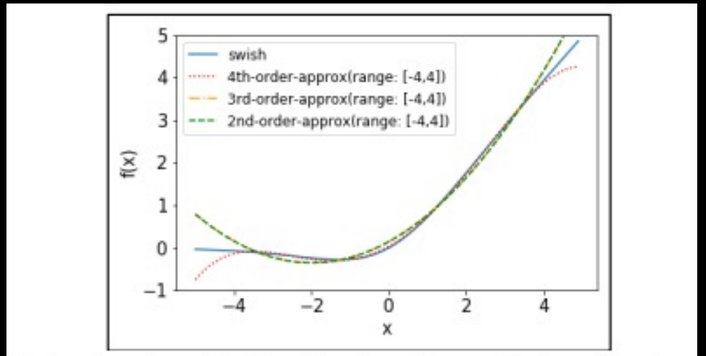


Fig. 2. Comparison of Swish and its polynomial approximation with various orders

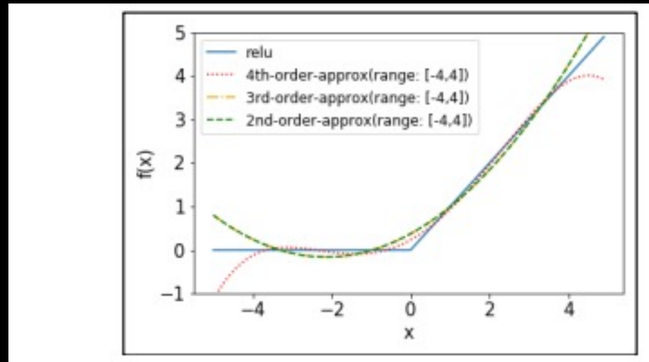


Fig. 3. Comparison of ReLU and its polynomial approximation with various orders

[출처] https://arxiv.org/pdf/2009.03727.pdf

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

(2) 동형암호 연산 횟수를 줄이는 방법은?

- 그러나....! 이러한 비선형 함수는 0과 거리가 먼 지점부터는 형태가 많이 달라짐

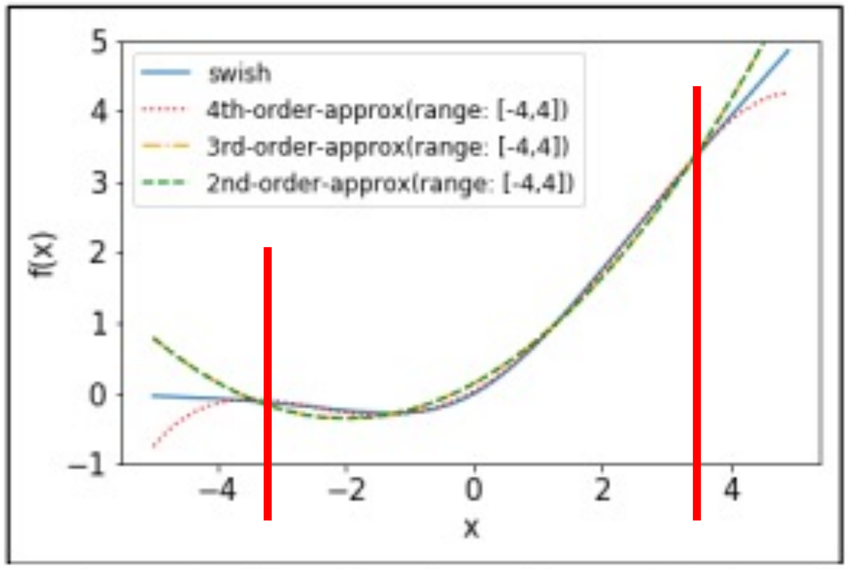


Fig. 2. Comparison of Swish and its polynomial approximation with various orders

- 딥러닝 층이 많아지게 되면 결과 값들의 절댓값 크기가 커지기 때문에 실제 모델의 추론 값과 차이가 생김

[출처] https://arxiv.org/pdf/2009.03727.pdf

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER DEVIEW 2023

꿀팁 #2

곱셈을 최소화하자!

- 각 딥러닝 Layer 마다 BatchNormalization을 사용
- 모델 학습 시 활성화 함수를 비선형 다항함수로 근사화 하여 사용
- 이 경우 학습 시 BatchNormalization이 각 계층마다 적용되어 있다고 가정

Activation function	Approx. degree	Approx. range	BN	Accuracy [%]	
				MINST	*CIFAR-10*
Swish	-	-	-	98.86	77.88
			✔	99.25	82.00
ReLU	-	-	-	98.82	83.53
			✔	99.05	83.69
Square	-	-	-	99.18	76.37
			✔	99.18	77.46
Approx. Swish	4	$x \in [-4, 4]$	-	98.83	74.85
			✔	99.16	80.09
		$x \in [-6, 6]$	-	98.79	75.30
			✔	99.21	80.47
	2	$x \in [-4, 4]$	-	98.80	72.89
			✔	99.28	79.11
		$x \in [-6, 6]$	-	98.46	70.58
			✔	99.05	76.75
Approx. ReLU	4	$x \in [-4, 4]$	-	98.90	74.43
			✔	99.11	79.38
		$x \in [-6, 6]$	-	98.94	73.70
			✔	99.25	81.02
	2	$x \in [-4, 4]$	-	98.51	71.80
			✔	99.17	79.07
		$x \in [-6, 6]$	-	98.41	72.54
			✔	99.15	74.72

[출처] https://arxiv.org/pdf/2009.03727.pdf

2.2 동형암호 기반 알고리즘 개발의 시행착오

NAVER
DEVIEW
2023

(3) SIMD based Architecture

- 한 번에 여러 데이터를 추론할 수 있도록 하자. (SIMD approach)
- 하나의 암호문에 저장될 수 있는 데이터의 갯수를 알아야 함
- 즉, 연산 전 필요한 곱셈의 횟수(Depth) 에 대해 알고 있어야 함

2.2 동형암호 기반 CNN 구현 꿀팁 대방출

NAVER
DEVIEW
2023

꿀팁 #3

Batch를 활용하자!

- MNIST의 경우 784 = 28 X 28 개의 속성으로 구성됨.
- 만일, CNN에 필요한 곱셈 연산이 11개 이면 Depth 11로 설정 가능

  => 이 경우 16,384 크기의 실수 벡터 암호화 가능

  => 최대 20 (= 16,384 / 784) 개의 MNIST 이미지 암호화 가능

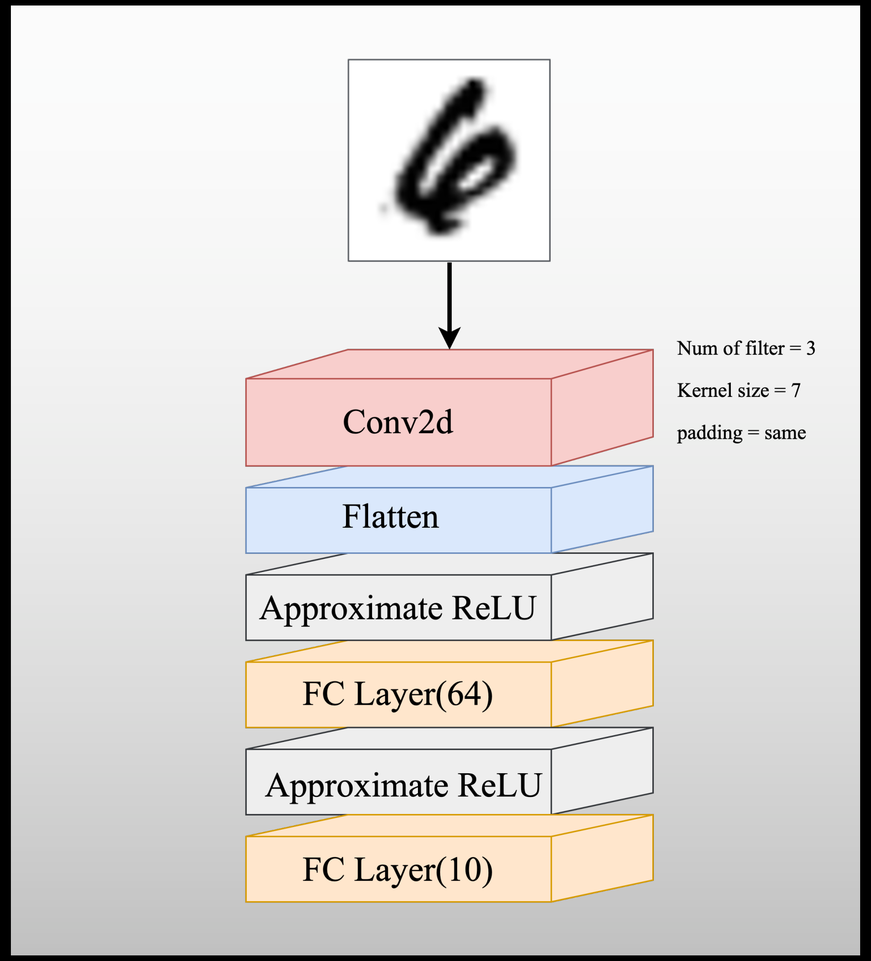
2.3 MNIST 데이터셋에서의 성능측정

NAVER
DEVIEW
2023

실험 환경

- 데이터셋 : MNIST
- CNN 구조 : 오른쪽 그림 참조
- Depth : Depth 11
- Approximate ReLU :

  2차 다항식으로 근사화된 ReLU
- 추론 데이터 수 : 20개 (Batch)



2.4 CPU VS GPU

NAVER
DEVIEW
2023

20개의 MNIST 추론 시 암호화 속도 비교

스펙	CPU Instance	GPU Instance
메모리 (GB)	64GB	320GB
CPU	vCPU (Powered by Intel® Xeon® Gold Processor) 32개	vCPU (Powered by Intel® Xeon® Gold Processor) 32개
GPU	-	V100 4장
수행시간	평균 30초 이내	평균 16초 이내

3.동형암호 기반
CNN 알고리즘 적용 가능 사례

3.1 NAVER Cloud의 동형암호 PaaS 적용 사례

NAVER DEVIEW 2023

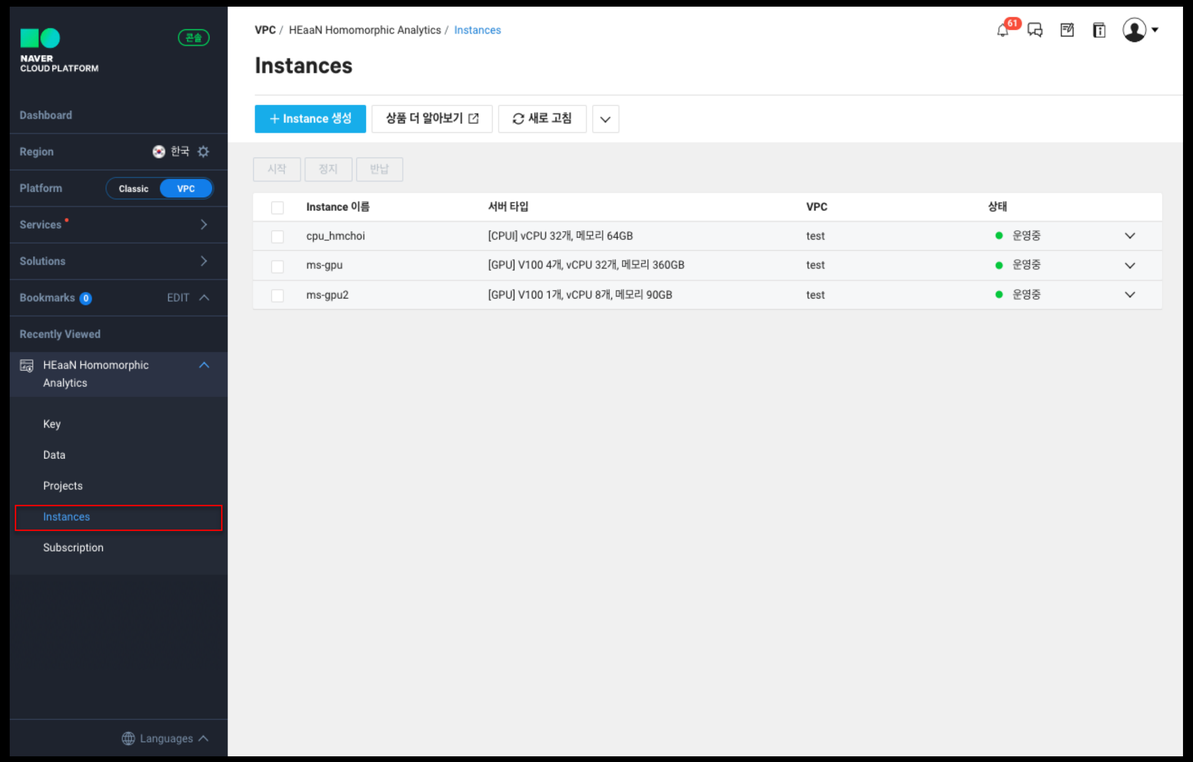
NAVER Cloud의 동형암호 PaaS 상품

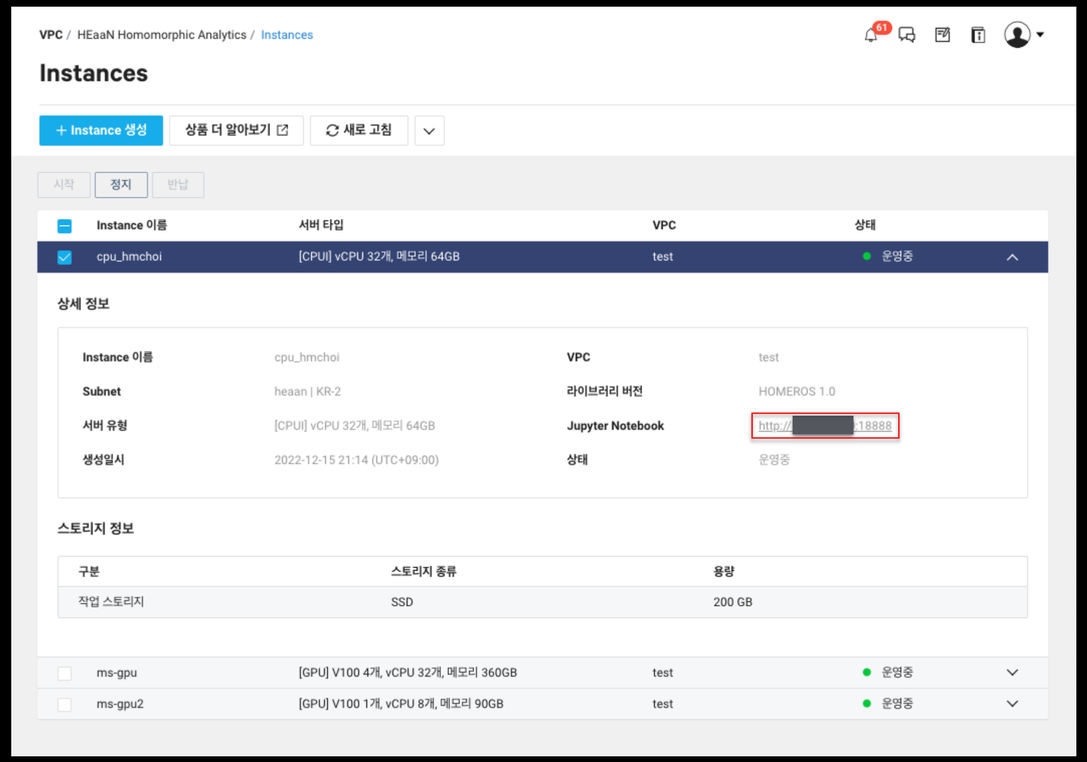
- HEaaN Homomorphic Analytics 상품에서 동형암호 기반 SaaS 및 PaaS 제공
- PaaS 상품은 파이썬 기반 HOMEROS SDK에서 동형암호 기반 통계 분석 및 머신러닝 기능 제공
- PaaS 상품은 CPU 및 GPU 각각 3 종류씩 제공
- Jupyter notebook 을 통해 접속 가능하며 예제 샘플 제공
- URL : https://www.ncloud.com/product/analytics/heaanHomomorphic

3.1 NAVER Cloud의 동형암호 PaaS 적용 사례

NAVER DEVIEW 2023

포털 메인 & 세부 항목 조회

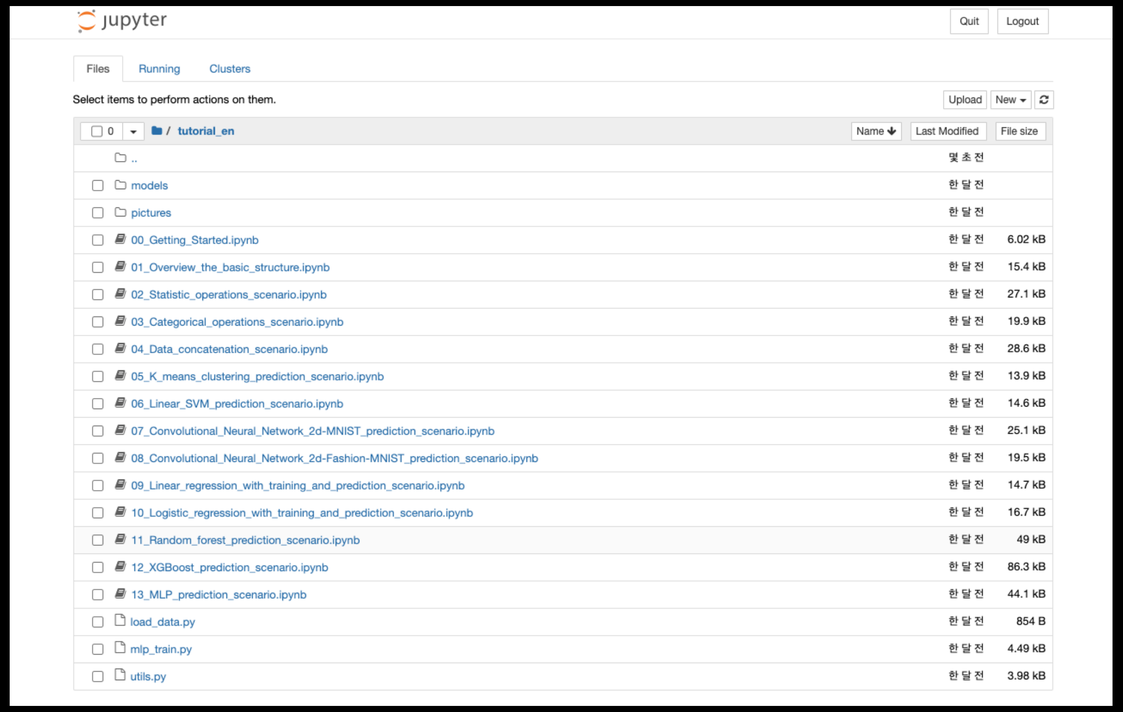


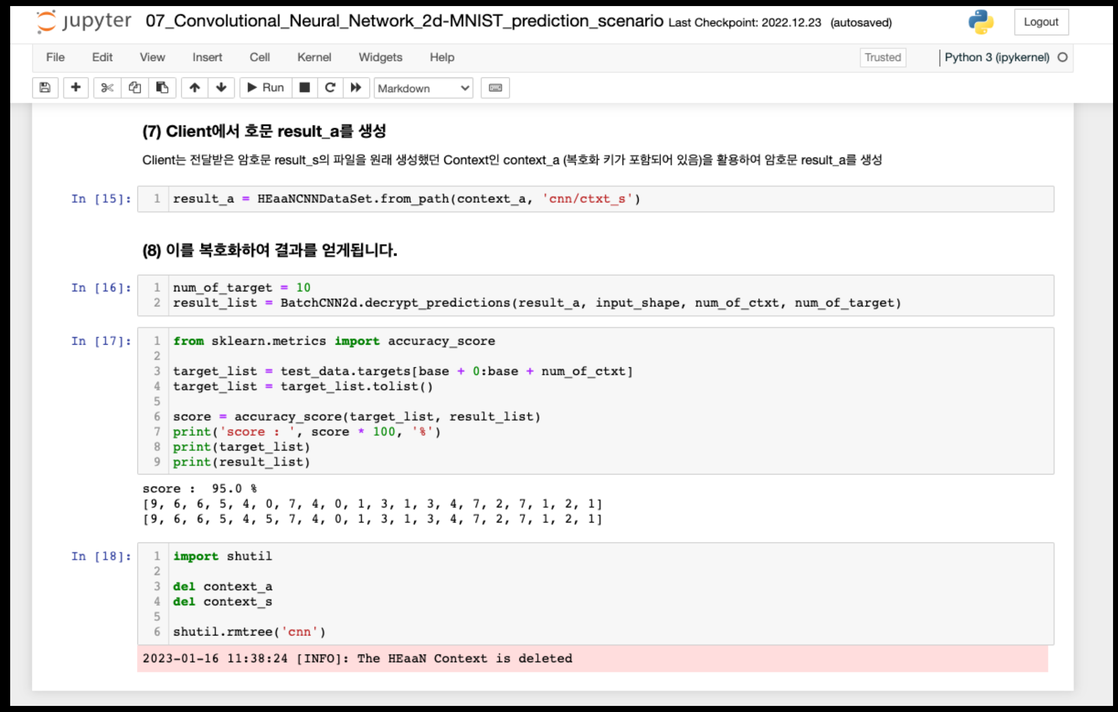


3.1 NAVER Cloud의 동형암호 PaaS 상품 소개

NAVER DEVIEW 2023

Jupyter Notebook 예시





3.2 응용분야 소개

NAVER
DEVIEW
2023

응용분야 1 : CNN 기반 생체인증

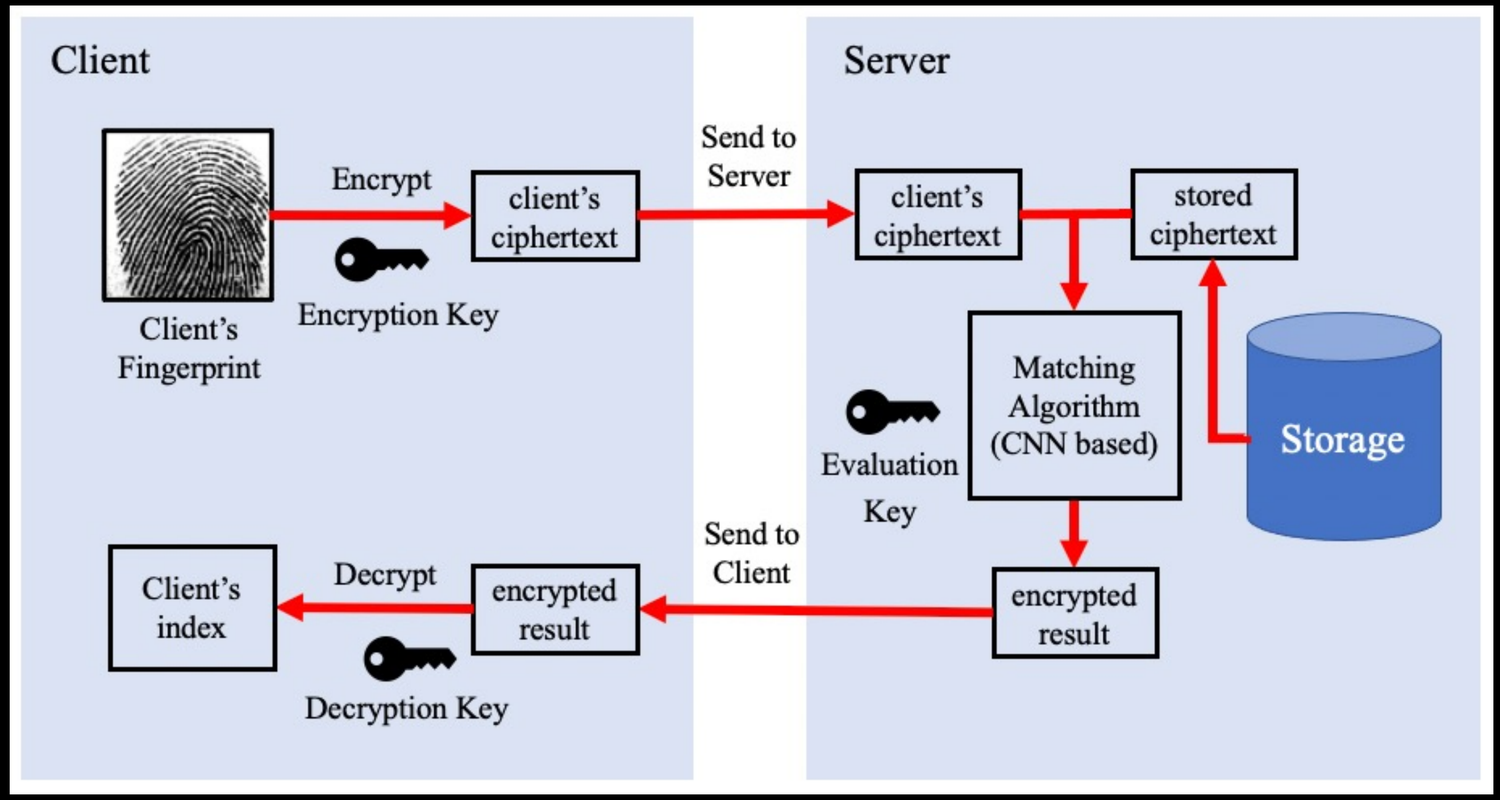
- 지문, 정맥, 홍채 등은 생체인증을 위해 많이 사용되는 생체정보
- 하지만 생체정보는 측정 시 노이즈가 함께 측정되기 때문에 기존 패스워드에서 주로 사용되던 일방향 해시 함수 적용이 어려움

생체정보를 동형암호로 암호화하여 저장한 후 CNN 알고리즘을 통해 특징점을 추출하여 비교하는 방식으로 인증

3.2 응용분야 소개

NAVER
DEVIEW
2023

응용분야 1 : CNN 기반 생체인증



3.2 응용분야 소개

NAVER
DEVIEW
2023

응용분야 2 : 이미지정보 기반 의료처방

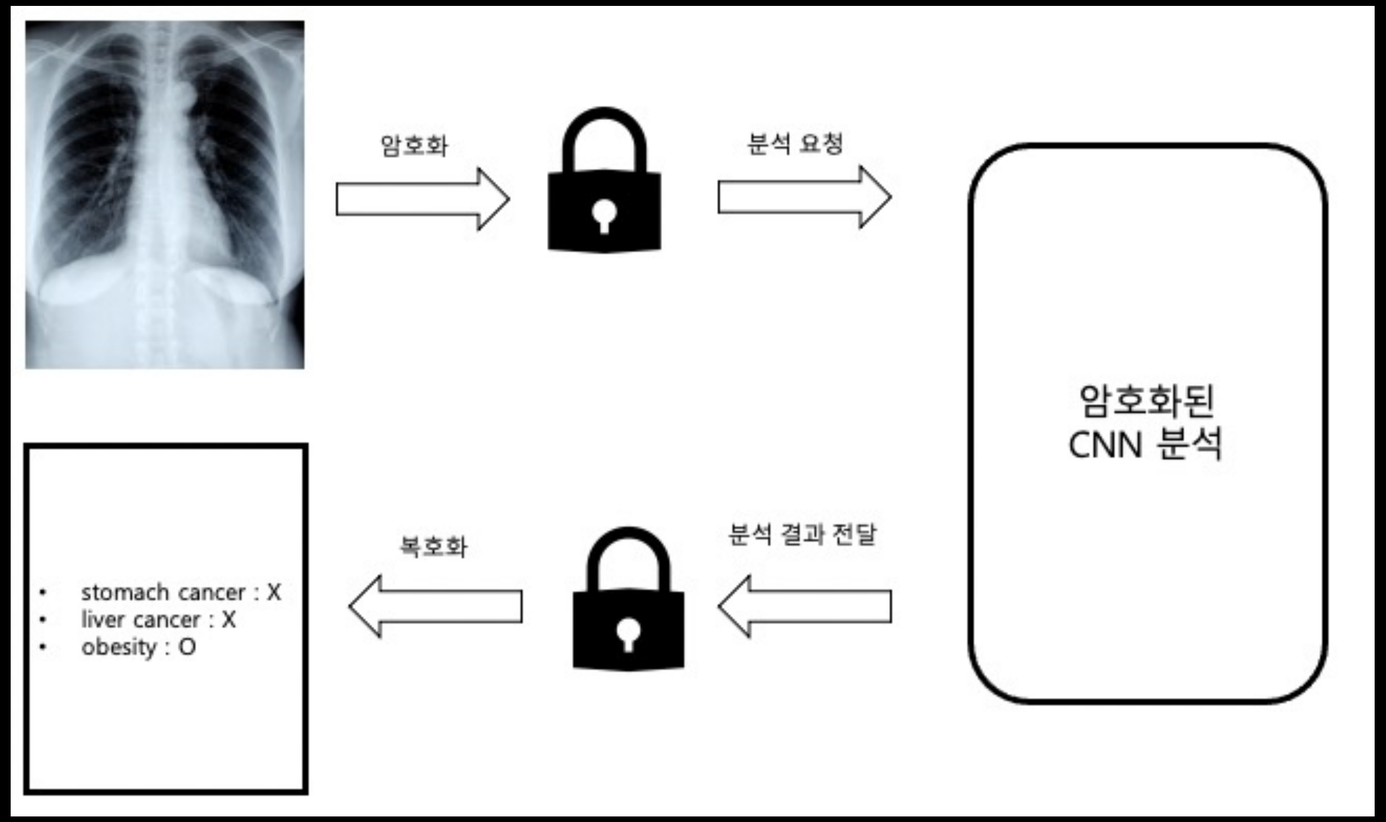
- X-ray, CT 사진 등을 기반으로 머신러닝 알고리즘이 특정 질병의 유무 판단 가능
- 환자의 이미지를 환자의 공개키로 동형암호를 통해 암호화한 후 의료처방 알고리즘을 통해 암호화된 질병 예측 후 환자는 그 결과를 자신의 복호화키로 복호화
- 환자의 프라이버시를 지키며 질병 판단 예측 가능

동형암호를 적용한 의료처방 기술의 활성화를 통해 프라이버시 침해의 한계를 극복하고 보다 다양한 의료 서비스 제공 기대

3.2 응용분야 소개

NAVER
DEVIEW
2023

응용분야 2 : 이미지정보 기반 의료처방



[출처] https://kr.freepik.com/free-photo/female-chest-x-ray_923296.htm#query=x%20ray&position=1&from_view=keyword

3.3 추후 연구 방향 제시

NAVER
DEVIEW
2023

1. CNN 알고리즘 성능 향상

- 내부 구현 알고리즘 최적화를 통한 알고리즘 성능 향상
- 다양한 크기의 필터와 여러 layer들의 조합에서도 최적의 성능 제공

2. 동형암호 기반 CNN 활용사례 발굴

- 생체인식 : 지문인식, 정맥인식, 홍채인식 등
- 의료처방 : X-ray, CT 사진 등을 기반으로 한 의료 처방
- 스팸탐지 : 이미지 기반 스팸 이메일, 문자 탐지

Q & A

Thank You