

센서 기반의 디바이스 DNA 기술 동향

Trends in Device DNA Technology Trend for Sensor Devices

김주한 (Juhan Kim, juhankim@etri.re.kr)

이상재 (Sangjae Lee, leestrike@etri.re.kr)

오미경 (Mi Kyung Oh, ohmik@etri.re.kr)

강유성 (Yousung Kang, youskang@etri.re.kr)

미래암호공학연구소 책임연구원

미래암호공학연구소 책임연구원

미래암호공학연구소 책임연구원

미래암호공학연구소 책임연구원

ABSTRACT

Just as it is possible to distinguish people by using physical features, such as fingerprints, irises, veins, and faces, and behavioral features, such as voice, gait, keyboard input pattern, and signatures, the an IoT device includes various features that cannot be replicated. For example, there are differences in the physical structure of the chip, differences in computation time of the devices or circuits, differences in residual data when the SDRAM is turned on and off, and minute differences in sensor sensing results. Because of these differences, Sensor data can be collected and analyzed, based on these differences, to identify features that can classify the sensors and define them as sensor-based device DNA technology. As Similar to the biometrics, such as human fingerprints and irises, can be authenticated used for authentication, sensor-based device DNA can be used to authenticate sensors and generate cryptographic keys that can be used for security.

KEYWORDS 디바이스 DNA, PUF, 센서 DNA, PRNU, 이미지 센서 DNA

1. 서론

1. 디바이스 DNA

지문, 홍채, 정맥, 얼굴 등의 신체적 특징과 음성, 걸음걸이, 자판입력, 서명 등과 같은 행동적 특징 등을 이용하여 사람을 구별할 수 있듯이 IoT 디바이스 등에서도 복제 불가능한 여러 가지 특징

을 포함하고 있다.

이러한 특징들은 반도체 공정이 필요한 SDRAM 등과 반도체 집적회로의 구조기술을 기본으로 하는 센서(가속도, 자이로, 이미지 센서 등)에서 주로 발견할 수 있다. 같은 생산 공정에서 생산된 동일 부품이라도 생산 공정의 불완전성으로 인해 각각의 부품들은 부품마다 각기 다른 오차를 포함한다.

* DOI: <https://doi.org/10.22648/ETRI.2020.J.350103>

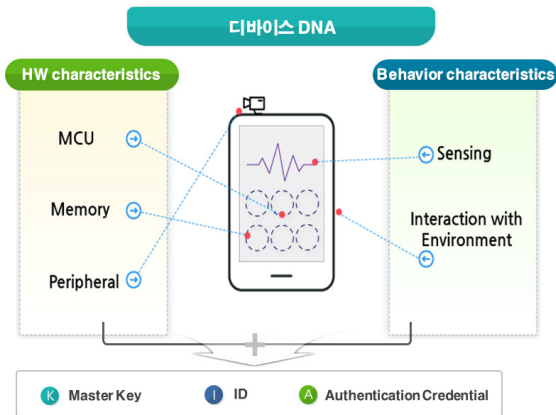
* 이 연구는 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행되었음 [No. 2018-0-00230, (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발(TrusThingz 프로젝트)].



본 저작물은 공공누리 제4유형

출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.

©2020 한국전자통신연구원



출처 강유성 외 3인, 물리적 복제 방지 기능(PUF) 보안 요구사항 및 시험방법 국제표준화 동향"정보보호학회지, 제 28권 제4호, 2018. 8.

그림 1 디바이스 DNA 개요

칩의 물리적 구조 차이 및 소자나 회로의 연산 시간 차이, SDRAM의 전원 on/off 시의 잔류 데이터 차이 및 센서의 센싱 결과의 미세한 차이 등을 예로 들 수 있다.

각 부품들의 미세한 차이는 사람을 구별할 수 있는 DNA 정보처럼 IoT 장치를 구별할 수 있는 정보로 디바이스 DNA로 정의할 수 있다(그림 1 참조).

같은 회사, 동일 모델의 각기 다른 부품들이라도 서로 다른 디바이스 DNA를 가지고 있어 물리적으로 서로 다른 부품의 DNA를 복제할 수 없으므로 물리적 복제 방지 기능(PUF: Physically Unclonable Function)을 갖는다.

물리적 복제 방지 기능(PUF)은 반도체의 미세한 구조 차이 등을 이용하여 물리적으로 복제가 불가능한 암호키나 ID(IDentity)를 생성하는 기술[1]로, PUF를 통해 언제든지 생성할 수 있고 비휘발성 메모리 등에 저장할 필요가 없어 유출 등의 보안 위협에 안전하다. 물리적 복제 방지 기능에 대한 다양한 보안 요구사항들이 있으며, 이에 대한 시험 방법에 대한 국제적인 표준화 작업도 이루어지고 있다[2].

2. 디바이스 DNA 종류

반도체 칩의 물리적 특성을 디바이스 DNA로 이용하는 기술들로는 Arbiter-PUF[3], RO(Ring Oscillator)-PUF[4], LoopPUF[5], VIA PUF[6] 등과 상용 메모리 기반의 SRAM[7]과 DRAM[8]을 이용한 물리적 복제 방지 기술 등이 있다.

표 1은 ETRI에서 최근 연구 중인 디바이스 DNA 기술들에 대한 것으로 레지스터와 커패시터 연결을 통해 발생하는 오차를 이용하는 RC(Resistor-Capacitor) PUF, 통신 칩셋(Wi-Fi, SUN칩)의 여유 SRAM을 이용한 PHY-PUF, 플래시 메모리를 이용한 Flash PUF, 링 오실레이터의 위상 변화의 오차를 이용한 PDRO(Phase Detection Ring Oscillator) PUF 등도 저마다 각기 다른 형태의 디바이스 DNA를 사용한 것이다.


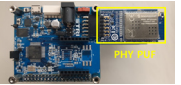



이미지 센서와 가속도 센서 등의 반도체 공정이나 반도체 미세회로 등이 적용된 센서에서도 역시 미세한 오차를 포함하고 있으며, 이를 이용하여 디바이스 DNA를 구성할 수도 있다.

3. 센서 기반의 디바이스 DNA

이미지 센서, 특히 반도체 공정을 사용하는 CMOS 계열에서 센서별 오차를 많이 포함하고 있다. 또한, 초정밀 미세회로가 적용되는 MEMS 기반의 센서들(예, 가속도 센서[9,10], 자이로 센서[10,11], 지자기 센서[10,12] 등)에서도 이러한 오차가 발견되며, 이를 이용한 많이 연구들이 진행되고 있다.

센서 기반의 디바이스 DNA들은 주로 센싱 데이터의 오차를 이용한다. 따라서 데이터에 대한 분석 및 특징 추출 등의 과정이 필요하거나 학습 및 시험 등의 절차가 필요하다. 이렇게 생성되는 디바이스

표 1 ETRI에서 연구/개발 중인 디바이스 DNA 종류

Primitive 명칭	(1) RC PUF	(2) PHY PUF	(3) Flash PUF	(4) Image Sensor PRNU †	(5) External Sensing Data
대상 하드웨어	Resistor-Capacitor (저항-커패시터)	통신 칩셋 SRAM 메모리 (Wi-Fi, SUN)	Flash 메모리	Camera module (이미지 센서)	주변 센서류 (가속도, 자이로스 코프 등)
출력 타입	Dynamic (32bits challenge)	Fixed or Restricted Dynamic	Fixed or Restricted Dynamic	Dynamic	Dynamic
출력 사이즈	128~2,048bits	통신모듈 버퍼 사이즈	Flash 메모리 사이즈	학습 네트워크 모델 (오토인코더의 잠재 공간 노드 수에 비례)	학습 네트워크 모델 (오토인코더의 잠재 공간 노드 수에 비례)
개발 보드 (시험 제품)	STMicro의 STM32F4 MCU를 사용한 보드	Kidde-Ruby 보드 (STM32F4) + P mod WiFi module	Kidde-Ruby 보드 (STM32F4) + S25FL 128S(16MB) Flash Memory	삼성, 로지텍, 샤오미 IP 카메라, 아이폰	스마트폰(안드로이드), 아두이노
특징	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 RC 회로 내장 보드 제작 필요 Voltage(MCU) variance에 강인 챔버 테스트 완료 	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 챔버 테스트 (-20~70°C에서 stability 유지) Voltage variance에 강인 하드웨어 수정 불필요 	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 하드웨어 수정 불필요 온도 및 전압에 대한 신뢰성 평가 진행 예정 	<ul style="list-style-type: none"> 상용제품(판매 중인 IP 카메라)에서 디바이스 DNA 확보 카메라 모듈 고유 노이즈를 학습시켜 활용 	<ul style="list-style-type: none"> 상용제품(판매 중인 안드로이드/아두이노)에서 디바이스 DNA 확보 주변 센서류의 센싱 데이터를 추출하여 활용 

* Fixed 타입(Confined 타입): 출력이 고정되어 있는 타입
 * Dynamic 타입(Extended 타입): Challenge-Response 방식으로 동적으로 출력을 변경할 수 있음
 * Restricted Dynamic 타입: Challenge-Response 방식이나 CRP pair가 제한적이거나 하나인 경우
 † PRNU: Photo Response Non Uniformity

스 DNA는 센서를 확인하는 ID 또는 보안키 등으로 사용할 수 있다.

안드로이드 스마트폰의 경우 웹 브라우저를 통한 웹페이지에서의 모션센서(가속도, 자이로 및 지자기 센서 등)에 대한 접근 권한은 따로 필요 없으며, 아이폰에서는 사용자의 부주의한 승인을 통해 웹 사이트는 쉽게 스마트폰 모션센서 정보를 수집할 수 있다[9,21]. 수집된 정보를 통해 사용자 스마트폰 ID를 생성하고 분류할 수 있으며, 이는 사용자의 프라이버시 침해로 이어질 수도 있다.

이미지 센서는 더 많이 연구들이 진행되고 있는데, 이는 주로 불법 영상물 배포와 특히 아동 영상물의 오용에 따른 소스 카메라를 검증하는 포렌식 기술로 많이 활용되기 때문이다[13-17].

II. 이미지 센서 DNA 기술

1. 이미지 센서 DNA

디지털 카메라는 그림 2의 카메라 프로세싱 흐름을 따라 사진을 구성한다.

CFA를 통과한 빛들은 센서를 통해 양자화되고

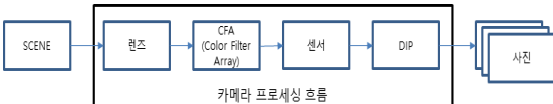


그림 2 디지털 카메라 프로세스 구성

DIP(Digital Image Processing) 과정을 통해 일부 노이즈 제거 및 압축 등을 통해 사진으로 저장된다.

이 과정에서 센서는 생산과정의 불완전성(실리콘 웨이퍼의 균질성 저하로 센서 어레이 픽셀의 빛민감도 차이 유발) 때문에 빛에 균일하게 반응하지 못하는 현상(PRNU: Photo Response Non-Uniformity)이 발생하며, 최근의 디지털 이미지 포렌식 기술들은 소스 카메라 검증에 PRNU를 많이 사용하고 있다.

이미지 센서에서 발생하는 SPN(Sensor Pattern Noise)은 사진 구성 과정에서 생기는 전체 노이즈를 의미하며, FPN(Fixed Pattern Noise)과 PRNU로 구성된다. FPN(Fixed Pattern Noise)은 미세한 전류에 의해 생성되는 노이즈로 카메라 렌즈를 완전히 닫고 촬영된 사진의 평균을 구하여 노이즈를 구할 수 있으며, 이를 이용해 쉽게 제거할 수 있다.

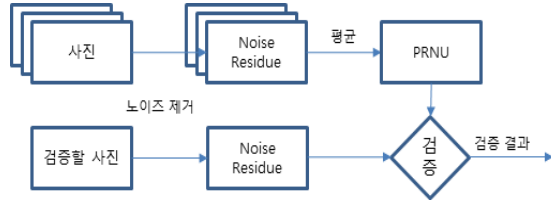


그림 3 PRNU 추출 및 검증 절차

출처 Ashref Lawgaly, "Digital camera identification using sensor pattern noise for forensics applications,"[online] available at: <http://nrl.northumbria.ac.uk/32314/>

2. PRNU 추출 및 검증

그림 3은 이미지들에서 PRNU를 추출하는 방법과 검증하는 절차를 간단한 도식으로 표시한 것이다[18].

이처럼 간단한 절차로도 실험실 레벨(한정된 공간에서의 몇 종류의 카메라 사진들)에서는 상당히 높은 확률로 소스 카메라의 구별이 가능함을 그림 4와 같은 절차의 실험 결과로 확인하였다. 그림 3의 절차에 PRNU 클러스터링[5]을 접목하고 딥러닝 기법을 접목하여 사용하였다. PRNU를 추출하고 단순히 상관도를 비교한 방식도 실험실 레벨에

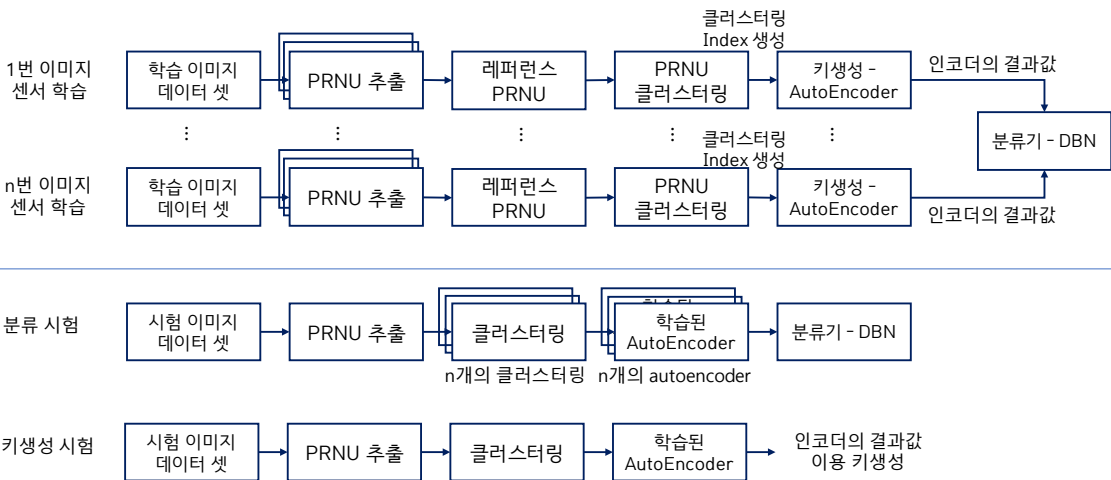


그림 4 PRNU 기반의 디바이스 DNA 추출 및 소스카메라 검증 절차

서는 비슷한 결과를 얻었다.

3. PRNU기반 Counter-Forensic

그림 3에서처럼 PRNU를 추출할 수 있으면 이미지에서 PRNU를 제거 및 위조하여 프라이버시를 높이는 방법도 있다. 즉, 이미지에서 소스 카메라 검증이 어렵게 PRNU를 제거하거나 다른 카메라의 PRNU를 넣어 위조할 수 있는데, 이를 디지털 이미지에 대한 counter-forensic 기술[19,20]로 정의할 수 있다. 최근에는 SNS상에 스마트폰으로 찍은 사진이나 영상 등이 많이 올라온다. 그 사진이나 영상을 수집해 분석하면 한 개인의 스마트폰의 PRNU를 유추할 수 있다. 이를 다른 이미지에 추가하여 소스 카메라 검증에 혼란을 주는 것도 가능

하다.

Counter-forensic 기술을 이용하면 이미지 센서의 고유 패턴을 찾기 어렵게 만들 수 있지만, Ⅲ장에서와 같이 디바이스 DNA를 일종의 ID 및 보안키로 사용하는 방식에서는 그 영향이 제한된다.

Ⅲ. 센서 DNA 활용

1. 가속도 센서 DNA 실험

그림 2의 센서 DNA의 분석, 추출, 사용하는 방법에는 다양한 방식이 존재할 수 있다. 예를 들어, 참고문헌 [9,22]에서는 표 2와 같이 가속도 센서의 데이터를 시간 영역 및 주파수 영역으로 구분하여 각각 10개와 15개의 특징을 추출하였다.

이를 가속도 센서의 지문처럼 사용하여 다른 센

표 2 센서 데이터 특징 분류[9,22]

#	Domain	Feature	Description
1	Time	Mean	The arithmetic mean of the signal strength at different timestamps
2		Standard deviation	Standard deviation for the signal strength
3		Average deviation	Average deviation from mean
4		Skewness	measure of asymmetry about mean
5		Kurtosis	Measure of the flatness or spikiness of a distribution
6		RMS	Square root of the arithmetic mean of the squares of the signal strength at various timestamps
7		Max	Maximum signal strength
8		Min	Minimum signal strength
9		ZCR	The rate at which the signal changes sign from positive to negative or back
10		Non-negative count	Number of non-negative values
11	Frequency	Spectral centroid	Represents the center of mass of a spectral power distribution
12		Spectral spread	Defines the dispersion of the spectrum around its centroid
13		Spectral skewness	Represents the coefficient of skewness of a spectrum
14		Spectral kurtosis	Measure of the flatness or spikiness of a distribution relative to a normal distribution
15		Spectral entropy	Captures the peaks of a spectrum and their locations
16		Spectral flatness	Measures how energy is spread across the spectrum
17		Spectral brightness	Amount of spectral energy corresponding to frequencies higher than a given cut-off threshold
18		Spectral rolloff	Defines the frequency below which 85% of the distribution magnitude is concentrated
19		Spectral roughness	Average of all the dissonance between all possible pairs of peaks in a spectrum
20		Spectral irregularity	Measured the degree of variation of the successive peaks of a spectrum
21		Spectral RMS	Square root of the arithmetic mean of the squares of the signal strength at various frequencies
22		Low-energy rate	The percentage of frames with RMS power less than the average RMS Power for the whole signal
23		Spectral flux	Measure of how quickly the power spectrum of a signal changes
24		Spectral attack time	Average rise time to spectral peaks
25		Spectral attack slope	Average slope to spectral peaks

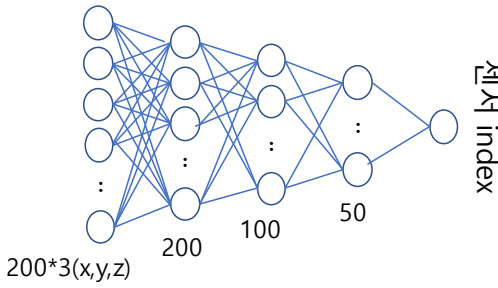


그림 5 센서 데이터 학습 및 분류

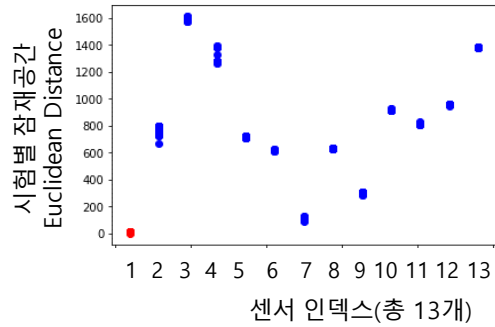


그림 7 개별 센서 학습 모델 시험 결과

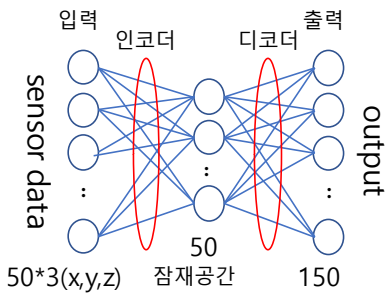


그림 6 개별 센서 데이터 학습

서들과의 데이터 특징과 비교하는 방식을 사용하였지만, 이를 특징 추출하지 않고 그림 5 처럼 간단한 신경망으로 데이터만 학습시켜 센서를 분류할 수도 있으며, 학습에도 다양한 방법을 사용할 수 있다.

센싱 데이터로 분류된다는 의미는 센서 고유의 DNA 존재한다는 의미가 되며, 이를 ID나 키로 활용하기 위해서는 결과가 그림 5의 센서 인덱스가 아닌 센서 특성을 포함하는 다른 종류의 데이터가 필요하다.

센서 특성을 포함한 데이터를 생성하기 위해서는 여러 방법이 있겠지만, 표 2의 특징들을 양자화하거나 그림 6처럼 개별 센서의 센싱데이터를 오토인코더(입력데이터와 출력데이터가 유사하도록 학습시키는 비지도 학습 방법)로 학습시켜 잠재공간(Latent space, 인코더와 디코더 사이의 히든레이어의 결괏값)에 특성이 반영될 수 있게 하여 인코

더의 결괏값을 사용하여도 된다.

그림 6과 같이 학습시킨 모델에서 인코더에 여러 센서의 데이터를 넣어 시험한 결과는 그림 8과 같다.

그림 7은 빨간색으로 표시된 1번 장치의 데이터로 학습시키고 1~13번 센서의 데이터들로 시험한 결과이다. Y축 값은 1번 장치의 첫 번째 잠재공간(50개의 실수 벡터)을 기준으로 유클리디안 거리값을 비교한 것으로 시험 시마다 점을 찍게 한 그래프이다. 1번 장치로 학습시켰기 때문에 1번의 값이 제일 낮게 나오고 센서 DNA가 학습 모델의 인코더에 반영되었음을 알 수 있으며, 이를 인증 및 보안키의 역할로 사용할 수도 있다.

인증 또는 보안키의 역할로 사용하기 위해서는 사용될 환경 및 센서 DNA를 고려한 보안 프로토콜 설계가 별도로 필요하다.

2. 이미지 센서 DNA 실험

그림 8은 그림 4의 이미지센서 분류 학습 모델을 간략화한 것이다. 오토인코더로 개별 이미지센서의 DNA 특성을 반영시키고, 인코더의 출력을 DBN(비지도 학습을 하는 딥러닝 기술) 입력으로 넣어 소스 카메라 인식을 하는 모델이다. 그리고 그

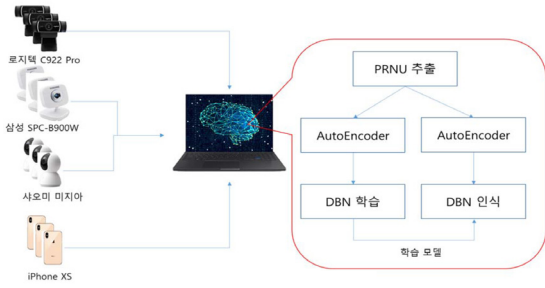


그림 8 이미지 센서 데이터 학습



• 인식률 : 99%

	LogitechA	LogitechB	LogitechC	SamsungA	SamsungB	SamsungC	XiaomiA	XiaomiB	XiaomiC
LogitechA	192	0	0	0	0	0	0	0	0
LogitechB	0	84	0	0	0	0	0	0	0
LogitechC	0	0	36	0	0	0	0	0	0
SamsungA	0	5	0	171	0	0	0	1	1
SamsungB	0	0	0	0	53	0	0	0	0
SamsungC	0	0	0	0	0	25	0	0	0
XiaomiA	0	0	0	0	0	0	163	0	0
XiaomiB	0	0	1	0	0	0	0	34	0
XiaomiC	0	0	0	0	0	0	0	0	51

그림 9 IP 카메라 분류 시험

모델로 실험(IP 카메라-로지텍, 삼성, 샤오미의 IP 카메라 각 3대씩 총 9대)한 결과는 그림 9와 같다.

학습 이미지와는 다른 이미지(사람 및 사람의 움직임이 포함된 사진)가 있어도 99% 정도 분류됨을 알 수 있으며, 이를 통해 이미지 센서 DNA가 존재함을 알 수 있다. 특히 개별 이미지 센서 DNA는 그림 8의 개별 오토인코더의 인코더 부분에 포함되어 있다. 따라서 이 부분을 안전하게 보관할 수 있으면 이미지 센서의 DNA를 반영한 SW 기반의 PUF처럼 운영도 가능하다.

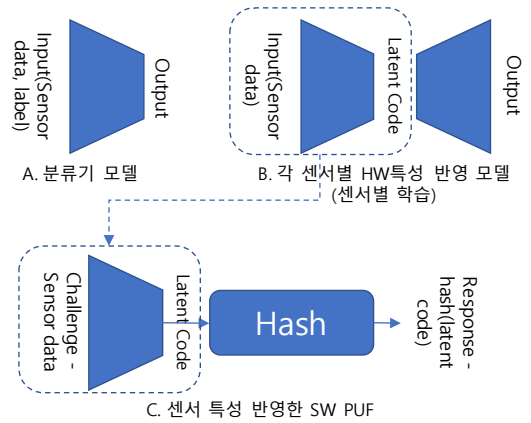


그림 10 센서 특성 기반의 SW PUF 모델

3. 센서 DNA 활용

개별 센서들에 찾아낸 DNA(특징 또는 학습된 모델 등)는 고유의 센서 특성을 포함하고 있어, 이를 그림 10에 보이는 것처럼 PUF와 비슷한 방법으로 운영할 수 있다.

칩 기반의 PUF는 기능들이 칩 안에 들어 있어 상대적으로 안전하지만 그림 10과 같은 센서 기반의 DNA 기술은 PUF처럼 사용하려면 센서 특성이 담긴 특징 또는 모델을 저장할 안전한 곳(Secure 영역)이 필요하다.

4. 센서 DNA 응용

디바이스 DNA 기술들은 센서가 탑재되는 디바이스가 필요한 전 산업 분야에서 센서의 검증 및 이상 여부를 파악하는 기술에 활용할 수 있다.

드론도 디바이스 DNA 기술을 잘 접목할 수 있는 장치이다. 산업용 및 군사용에 필요한 드론들은 인증 및 (피아)식별을 위한 보안모듈이 필수적이다. ETRI에서도 드론에 탑재하여 드론의 인증 및 (피아)식별이 가능한 보안모듈(SW/HW 형태)을 연구 및 개발 중이다. 이 연구에서는 드론의 인증 및 식

별을 보안모듈에 의존한다. 따라서 보안모듈을 이식하였을 경우, 드론의 인증 및 식별 대상이 변화되는 문제가 생길 수 있다.

드론에 포함된 센서들(가속도 센서, 자이로 센서, 지자기 센서, 바로미터 및 이미지 센서 등)의 DNA 기술과 보안모듈을 페어링시키면 드론 장치 그 자체를 보안모듈과 동시에 인증 및 식별해 해결할 수 있다.

IV. 결론

사람의 바이오 정보처럼 디바이스에도 갖가지 형태의 HW 특성이 담긴 정보들이 포함되어 있다. 이를 디바이스 DNA로 정의하고 센서 DNA를 통해 센서를 분류함으로써 이를 검증할 수 있다. 그리고 센서 기반 DNA를 SW 기반의 PUF의 형태로도 활용할 수 있다.

디바이스 DNA는 종류에 따라 디바이스 인증 및 보안키에 핵심으로 사용할 수 있는 특성을 가질 수도 있지만, 센서 기반 DNA 기술은 디바이스 인증 및 보안키에 필요한 이차적인 요소로 사용하는 것이 적합하다. 멀티 팩터 인증의 부가 요소, 디바이스(또는 센서)의 변경 여부를 검증하는 기술로 활용할 수 있다.

용어해설

PUF 반도체 생산공정의 불완전성에 기반한 칩의 물리적 계층의 구성 차이, 소자나 회로의 처리 시간 지연 차이 등으로 생기는 오차가 칩마다 달라 생기는 현상(물리적으로 동일하게 복제가 불가능함)을 이용하여 인증 및 암호키 등에 사용할 수 있는 기술

오토인코더 출력을 최대한 입력과 같아지도록 학습시키는 비지도 학습의 신경망으로 주로 데이터 압축, 노이즈 제거 등에 많이 사용

약어 정리

DBN Deep Belief Network

FPX	Fixed Pattern Noise
MEMS	Microelectromechanical Systems
PNU	Pixel Non-Uniformity
PRNU	Photo Response Non-Uniformity
PUF	Physical Unclonable Function
SPN	Sensor Pattern Noise

참고문헌

- [1] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," In Proc. Annu. Design Autom. Conf., June 2007, pp. 9-14.
- [2] 강유성 외 3인, 물리적 복제 방지 기능(PUF) 보안 요구사항 및 시험방법 국제표준화 동향, 정보보호학회지, 제28권 제4호, 2018. 8.
- [3] D. Lim et al., "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 13, no. 10, 2005, pp. 1200-1205.
- [4] A Maiti et al., "A large scale characterization of RO-PUF," In Proc. IEEE Int. Symp. Hardware-Oriented Security Trust, June 2010, pp. 94-99, June 2010.
- [5] Z. Cherif et al., "An Easy-to-Design PUF based on a single oscillator: the Loop PUF," In Proc. Euromicro Conf. Digital Syst. Design, Sept. 2012.
- [6] T. W. Kim, B. D. Choi, and D. K. Kim, "Zero bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process," Electron. Lett., vol. 50, no. 12, 2014, pp. 876-877.
- [7] D. Holcomb, W. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," IEEE Trans. Comput., vol. 58, no. 9, Sept. 2009, pp. 1198-1210.
- [8] W. Xiong et al., "Run-time Accessible DRAM PUFs in Commodity Devices," In Proc. Conf. Cryptographic Hardw. Embedded Syst., Santa Barbara, USA, Aug. 2016, pp. 432-453.
- [9] A. Das, N. Boriso, and E. Chou, "Every Move You Make: Exploring Practical Issues in Smartphone Motion Sensor Fingerprinting and Countermeasures," Privacy Enhancing Technol. Symp., vol. 2018, no. 1, 2018, pp. 88-108.
- [10] I. Amerini et al., "Smartphone Fingerprinting Combining Features of On-Board Sensors," IEEE Trnas. Inf. Forensics Security, vol. 12, no. 10, Oct. 2017.
- [11] O. Willers et al., "MEMS-based Gyroscopes as Physical Unclonable Functions," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Vienna, Austria, Oct. 2016, pp. 591-602.
- [12] R. Jin et al., "MagPairing: Pairing Smartphones in Close

- Proximity Using Magnetometers,” IEEE Trnas. Inf. Forensics Security, vol. 11, no. 6, June 2016.
- [13] J. Luká’s and J. Fridrich, “Digital Camera Identification From Sensor Pattern Noise,” IEEE Trnas. Inf. Forensics Security, vol. 1, no. 2, June 2006.
- [14] A. Lawgaly and F. Khelifi, “Sensor Pattern Noise Estimation Based on Improved Locally Adaptive DCT Filtering and Weighted Averaging for Source Camera Identification and Verification,” IEEE Trnas. Inf. Forensics Security, vol. 12, no. 2, Feb. 2017.
- [15] Y. Tomioka, Y. Ito, and H. Kitazawa, “Robust Digital Camera Identification Based on Pairwise Magnitude Relations of Clustered Sensor Pattern Noise,” IEEE Trnas. Inf. Forensics Security, vol. 8, no. 12, Dec. 2013.
- [16] 오태우 외, “센서 패턴 잡음을 이용한 디지털 상 획득 장치 판별,” 정보처리학회논문지/소프트웨어 데이터 공학, 제4권 제12호, 2015. 12.
- [17] 이상형 외, “모폴로지필터링기반 센서 패턴 노이즈를 이용한 디지털 동상 획득 장치 별 기술,” 정보처리학회논문지/소프트웨어 데이터 공학, 제6권 제1호, 2017. 1.
- [18] A. Lawgaly, “Digital camera identification using sensor pattern noise for forensics applications,” [online] available at: <http://nrl.northumbria.ac.uk/32314/>
- [19] L. J. G. Villalba et al., “A PRNU-based counter-forensic method to manipulate smartphone image source identification techniques,” Future Generation Comput. Syst., vol. 76, 2017, pp. 418-427.
- [20] Netherlands Forensic Institute. PRNU Decompare. 2013. [online source] available at: <https://sourceforge.net/p/prnudecompare/wiki/Home/>
- [21] S. A. Anand et al., “Spearphone: A Speech Privacy Exploit via Accelerometer-Sensed Reverberations from Smartphone Loudspeakers-How using the smartphone in speakerphone mode erodes your privacy,” IEEE Trnas. Inf. Forensics Security, vol. 12, no. 2, Feb. 2017.
- [22] A. Das, N. Borisov, and M. Caesar, “Exploring Ways To Mitigate Sensor-Based Smartphone Fingerprinting”, ArXiv 2015.