IoT 디바이스 기반 프라이버시 보존 안면 인식 시스템의 구현

이수민, 오재기, 정민욱, 최진아, 윤병우
LG 전자

sum.lee@lge.com, jaeky.oh@lge.com, minwook.jeong@lge.com,

jina11.choi@lge.com, byoungwoo.yoon@lge.com

An Implementation of Privacy-Preserving Face Recognition System on IoT Devices

Sumin Lee, Jaeky Oh, Min-Wook Jeong, Jina Choi, Byoungwoo Yoon
LG Electronics

요 약

본 연구는 리소스가 제한된 IoT 디바이스 환경에서 동형암호를 활용하여 프라이버시를 보존하면서 안면 인식 서비스를 제공하는 시스템을 제안한다. 경량화된 동형암호 파라미터를 적용하여 클라이언트에서 생체정보를 암호화하고 서버에서 암호화된 상태로 유사도 분석을 수행함으로써 기존 온디바이스 방식의 확장성 한계를 극복하고 다중 디바이스 간 생체정보 활용이 가능함을 실증하였다.

Ⅰ. 서 론

생체인식 기술의 활용이 증가함에 따라 생체정보의 프라이버시 보호가 중요한 과제로 대두되고 있다. 전통적인 생체인식 시스템은 서버에서 평문 상태로 생체정보를 처리하거나 서버 없이 온디바이스 방식으로 처리한다. 전자는 서버 공격에 취약하고 후자는 디바이스 간 데이터 공유가 어렵다는 한계가 있다. 동형암호는 암호화된 상태에서 연산을 수행할 수 있어 두 가지 문제를 모두 해결할 수 있으나, 높은 연산 복잡도로 인해 리소스가 제한된 디바이스에 적용하기 어렵다.

본 연구는 리소스가 제한된 디바이스에서 동형암호 기반 안면 인식 시스템을 실용적으로 구현할 수 있음을 실증하였다. 기존 연구[1]에서 동형암호를 활용한 안면 인식 시스템을 제안한 바 있으나, 이는 충분한 연산 자원을 가진 디바이스를 전제로 설계하였다. 본 연구에서는 경량화한 동형암호 파라미터를 적용하여 리소스가 제한된 IoT 디바이스에서 동형암호 기반 안면 인식 시스템을 최적화하였다. 이를 통해 생체정보의 기밀성을 보장하면서도 여러 디바이스에서 수집한 생체정보를 통합 활용할 수 있는 확장성을 확보하였다.

Ⅱ. 동형암호

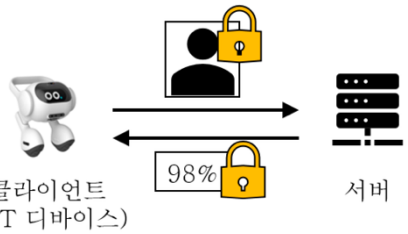
동형암호는 암호화된 데이터에 대해 복호화 없이 직접 연산을 수행할 수 있는 암호 기술이다. 평문 m_1, m_2 에 대한 암호문을 각각 $c_1 = \mathrm{Enc}(m_1)$, $c_2 = \mathrm{Enc}(m_2)$라고 할 때 동형암호는 아래와 같은 성질을 만족한다.

$$\mathrm{Dec}(c_1 \oplus c_2) = m_1 + m_2$$
$$\mathrm{Dec}(c_1 \otimes c_2) = m_1 \times m_2$$

현대의 실용적인 동형암호는 환(ring) 기반 격자암호를 기반으로 하며, 여기서 암호문 모듈러스(ciphertext modulus)는 하나의 암호문에서 수행할 수 있는 최대 곱셈 횟수에 해당하는 연산 깊이(multiplicative depth)에 비례한다. 복잡한 계산을 처리하려면 연산 깊이가 커질수록 모듈러스 값이 증가하게 되는데, 이로 인해 일정한 보안 수준을 유지하기 위하여 환의 차원(ring dimension)도 함께 증가한다. 환의 차원과 암호문 모듈러스가 동형암호 키와 암호문의 크기를 결정하므로 리소스가 제한된 디바이스에서는 키 생성이나 암복호화 과정이 실행 불가능하거나 심각한 성능 저하를 초래할 수 있다. 이에 본 연구에서는 안면 인식에 필요한 최소한의 연산 깊이로 경량화된 동형암호 파라미터를 설계한다.

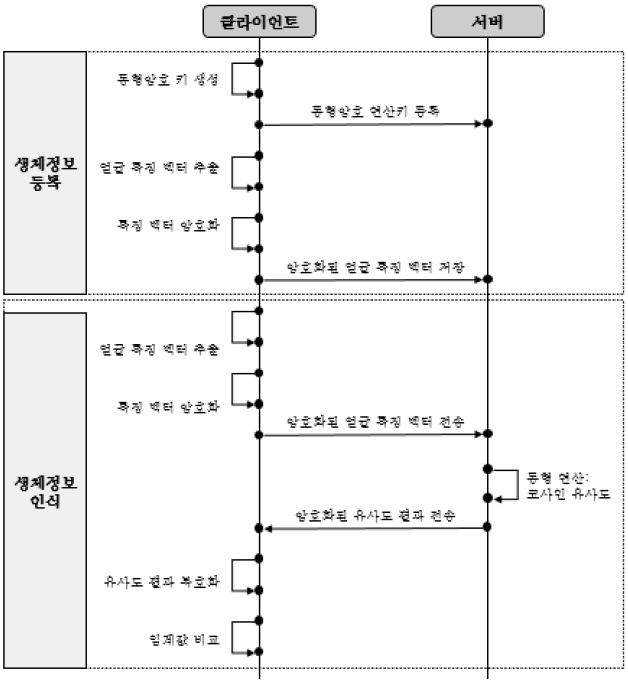
Ⅲ. 시스템 설계 및 구현

3-1. 시스템 아키텍처



[그림 1] 프라이버시 보존 안면 인식 시스템 구조

본 연구에서 제안하는 프라이버시 보존 안면 인식 시스템은 [그림 1]과 같이 구성한다. 클라이언트는 리소스가 제한된 IoT 디바이스이며, 카메라를 통해 얼굴 이미지를 획득하고 동형암호 키 생성 및 암복호화를 수행한다. 서버는 암호화된 얼굴 특징 벡터를 저장하고, 암호화된 상태에서 코사인 유사도 연산을 수행하여 안면 인식 결과를 클라이언트에게 전달한다. 이러한 구조를 통해 서버는 평문 생체정보에 접근할 수 없으며, 클라이언트만이 복호화 키를 보유하여 최종 인식 결과를 확인할 수 있다.



[그림 2] 생체정보 등록 및 인식 프로세스

[그림 2]는 생체정보 등록 및 인식 프로세스이다. 등록 단계에서는 클라이언트가 카메라를 통해 사용자의 얼굴 이미지를 획득하고, 사전 학습된 모델을 사용하여 특징 벡터로 변환한다. 얼굴 특징 벡터는 공개키를 사용하여 암호화되며, 암호화된 특징 벡터는 서버로 전송되어 데이터베이스에 저장한다. 이때 서버는 암호화된 데이터만을 저장하므로 평문 생체정보를 알 수 없다. 여러 사용자의 생체정보를 등록할 경우, 각 사용자별로 암호화된 특징 벡터가 서버에 저장되며, 이는 이후 인식 단계에서 비교 대상으로 사용된다.

생체정보 인식 단계에서는 클라이언트가 카메라로 얼굴 이미지를 획득하고 특징 벡터로 변환한 후 암호화하여 서버로 전송한다. 서버는 수신한 암호화된 특징 벡터와 데이터베이스에 저장된 암호화된 특징 벡터들 간의 코사인 유사도를 계산한다. 두 벡터 a, b 에 대한 코사인 유사도는 $\mathrm{CosSim}(a,b)=a\cdot b/\|a\|\|b\|$로 정의되며, 이는 암호화된 상태에서 동형 덧셈과 동형 곱셈을 통해 계산된다. 서버는 동형연산키를 사용하여 암호화된 상태로 내적과 벡터 크기를 계산하고, 최종적으로 암호화된 코사인 유사도 값을 얻는다. 계산된 암호화된 유사도 값들은 클라이언트로 전송되며, 클라이언트는 비밀키를 사용하여 이를 복호화한다. 복호화된 유사도 값이 사전에 설정된 임계값(threshold)을 초과하면 등록된 사용자로 인식한다.

3-2. 구현 및 실험

본 시스템은 LG 전자 스마트홈 AI 에이전트(Qualcomm QRB5165) 클라이언트와 Intel Core i9-14 CPU, 512GB RAM 의 서버로 구성하였다. 동형암호 처리는 OpenFHE[2] 라이브러리로 구현하였고, IoT 디바이스에서 128 비트 보안 강도를 유지하기 위하여 경량화된 동형암호 파라미터를 설계하여 적용하였다. 본 연구에서는 실수 벡터 연산을 지원하는 CKKS[3] 스킴을 사용하여 얼굴 이미지의 특징 벡터를 암호화하고 코사인 유사도 연산을 수행한다. 안면 인식에 필요한 코사인 유사도 연산은 한 번의 동형곱셈 연산으로 수행할 수 있기 때문에 연산 깊이는 1 로 설정하였다. 환의 차수 32768 과 암호문 모듈러스 90 비트로 동형암호 파라미터를 설정하여 IoT 디바이스에서 키 생성과 암복호화 연산을 효율적으로 수행할 수 있게 하였다.

제안 시스템의 성능을 평가하기 위하여 키 생성, 암호화, 유사도 연산, 복호화 시간을 측정하였다. 경량화된 파라미터를 사용한 결과, 클라이언트에서의 키 생성 시간은 1.92 초, 단일 얼굴 특징 벡터의 암호화 시간은 0.05 초로 측정되었다. 서버에서 두 암호화된 벡터 간의 코사인 유사도 계산 시간은 0.67 초이며, 클라이언트에서의 복호화 시간은 0.10 초로 측정되었다. 메모리 사용량 측면에서 동형암호 키는 0.79MB 의 복호화키와 2.62 MB 의 암호화키, 그리고 78.66 MB 의 동형연산키로 구성되었고, 단일 암호문 크기는 1.57 MB 로 측정되었다. 이를 통해 제한된 리소스를 가진 IoT 디바이스에서도 동형암호 기반 시스템이 실용적으로 동작할 수 있음을 확인하였다.

IV. 결론

본 연구에서는 리소스가 제한된 IoT 디바이스 환경에서 동형암호를 활용한 프라이버시 보존 안면 인식 시스템을 설계하고 구현하였다. 경량화된 동형암호 파라미터를 적용하여 클라이언트에서 키 생성 및 암복호화를 효율적으로 수행하고, 서버에서 암호화된 상태로 유사도 분석 연산을 수행함으로써 생체 정보의 기밀성을 보장하면서도 실용적인 성능을 달성하였다. 본 시스템은 기존 온디바이스 방식의 확장성 한계를 극복하고 다중 디바이스 간 생체정보 활용이 가능함을 실증하였다.

참 고 문 헌

[1] S. Kim et al., " IDFace: Face Template Protection for Efficient and Secure Identification," in Proc. of IEEE/CVF ICCV, 2025, pp. 13995-14005.

[2] A. Al Badawi et al., "OpenFHE: Open-source fully homomorphic encryption library," in Proc. 10th Workshop Encrypted Comput. Appl. Homomorphic Cryptogr., 2022, pp. 53-63.

[3] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., 2017, pp. 409-437.