드론을 위한 암호화된 얼굴 이미지 인증 프레임워크 제안

노현아[1*], 이주희[2†]
[1,2]성신여자대학교 (학생, 교수)
[1]20211056@sungshin.ac.kr, [2]jooheelee@sungshin.ac.kr

Privacy-Preserving Facial Image Authentication Framework for Drones

Hyun-A Noh[1], Joohee Lee[2]
[1,2]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

최근 드론으로 극한 환경에서 범죄 수배자 및 실종자를 탐색하는 시도가 활발하다. 이때 생체 인증 기술인 얼굴 인증 기술을 사용하면 탐색 효율이 높아지지만, 암호화되지 않은 인증 프로토콜 적용 시 생체 정보 유출의 위험이 있다. 본 논문에서는 드론이 수집한 얼굴 이미지 템플릿을 암호화하여 안전하게 인증할 수 있는 효율적인 생체 인증 프레임워크인 DF-PPHDM(Privacy-Preserving Hamming Distance biometric Matching for Drone-collected Facial images)을 제안한다. 수집된 얼굴 이미지는 암호문 형태로 서버에 전달되며 서버는 기존 등록된 암호화된 템플릿과의 Hamming distance 분석을 통해 검증한다. 제안한 DF-PPHDM을 RaspberryPI 4B 환경에서 직접 실험하여 분석한 결과, 한정된 리소스를 소유한 드론에서 효율적인 구현이 가능하며, 인증 단계에서 7.83~155.03 μs(microseconds)가 소요된다는 것을 입증하였다. 더불어 서버는 드론이 전송한 암호문으로부터 생체 정보를 복구할 수 없으므로 프라이버시 침해 문제를 예방할 수 있다. 향후 DF-PPHDM에 AI(Artificial Intelligence)를 결합하여 자동화 기능을 추가하고 코드 최적화를 통해 성능을 향상시킬 예정이다.

1. 서론

최근 드론이 범죄 수배자 수색 및 실종자의 위치 추적 같은 공공·안전 분야에 활용되고 있다 [1]. 이때 생체 인증 기술 중 하나인 얼굴 인증 기술을 사용하여 효율적으로 수색할 수 있으나, 암호화되지 않은 인증 프로토콜 사용 시 생체 정보 유출의 위험이 존재한다.

본 논문에서는 드론이 수집한 얼굴 이미지를 FFB-IPE(single key Function-hiding Inner Product Encryption for Binary string) [2]을 활용하여 암호화하고 암호화된 생체 템플릿을 서버로 전송함으로써, 서버가 암호화된 상태로 인증에 대한 연산을 수행하는 생체 인증 프레임워크인 DF-PPHDM(Privacy Preserving Hamming Distance biometric Matching for Drone-collected Facial images)를 제안한다.

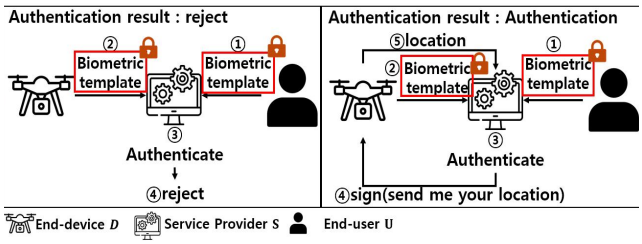
본 논문의 기여는 다음과 같다.

- 드론이 수집한 생체 템플릿을 FFB-IPE로 암호화 후 서버에 전달하고, 서버는 Hamming Distance(HD)를 활용한 생체 인증을 수행할 수 있는 효율적인 프레임워크인 DF-PPHDM을 제안하였다. 이때, 서버는 암호문으로부터 HD 외의 생체 정보에 대한 어떠한 정보도 얻을 수 없어 프라이버시를 보호할 수 있다.
- RaspberryPI 4B에서 128-bit 안전성을 갖는 DF-PPHDM을 구현하여, 측정한 평균 연산 속도는 한정된 자원을 가진 드론에서도 효율적인 구현이 가능하다는 것을 입증한다.

2. 제안

본 논문에서는 FFB-IPE [2]을 활용하여 드론을 위한 암호화된 생체 인증 프레임워크인 DF-PPHDM를 제안한다. FFB-IPE [2]는 네 가지 알고리즘인 (Setup, KeyGen, Enc, Dec)로 이루어지며 복호화 시 두 암호화된 비트열 간의 HD를 출력하는 함수 암호의 일종으로, Learning with Errors(LWE) [3] 기반의 수학적으로 증명 가능한 안전성을 가지고 있다.

* 주저자
† 교신저자



[그림 1] Flow of DF-PPHDM

먼저, 얼굴 이미지의 인코딩을 위해서는 [4]의 JPEG 2000 compression(ISO/IEC 15444-1)을 활용한다. 얼굴 이미지는 인코딩을 거쳐 4,632~145,832-bit의 범위를 갖는 생체 템플릿 $(x,y \in \{-1,1\}^k)$으로 변환된다. DF-PPHDM는 Service Provider S가 생체 템플릿 $x,y \in \{-1,1\}^k$에 대해 암호화된 상태에서 유사도 검증을 실행하는 것을 목표로 한다.

해당 프레임워크는 End-user U, End-device D, Service Provider S가 참여하는 Registration 단계, Collection 단계, Authentication 단계로 이루어져 있으며 각각의 과정은 다음과 같다.

① Registration (등록) 단계

1. End-user U는 security parameter λ에 따라 FFB-IPE [2]의 parameter를 설정한다.
2. U는 $\text{Setup}(1^\lambda) \rightarrow (msk, pp)$를 생성하고 End-device D에 (msk, pp)를 저장한다.
3. U는 생체 템플릿 x에 대한 비밀키인 KeyGen $(pp, msk, x) \rightarrow sk$를 생성하고 threshold $T > 0$와 (sk, pp)를 Service Provider S에게 전달한다.
4. S는 (sk, pp), T를 저장한다.

② Collection (수집) 단계

1. D는 카메라 센서를 통해 얼굴 이미지 FI를 수집하여 저장한다.
2. D는 FI을 추출하고, JPEG 2000 compression(ISO/IEC 15444-1) 과정을 통해 인코딩하여 생체 템플릿 y를 얻는다.
3. D는 암호문 $\text{Enc}(pp, msk, y) \rightarrow c$를 계산한다.
4. D는 S에게 c를 보낸다.

③ Authentication (인증) 단계

1. S는 (sk, pp)과 c를 통해 $\text{Dec}(pp, msk, y)$을 이용하여 내적값 z를 구한다. 그리고 생체 인증 템플릿 x,y 사이의 hamming distance $d = (k-z)/2$를 얻는다.
2. S는 d가 threshold T보다 작다면 accept를 출력하고 D에게 현재 위치를 알려달라는 신호를 보낸다. 만약 d가 T보다 작지 않다면 reject을 출력하고 신호를 보내지 않는다.

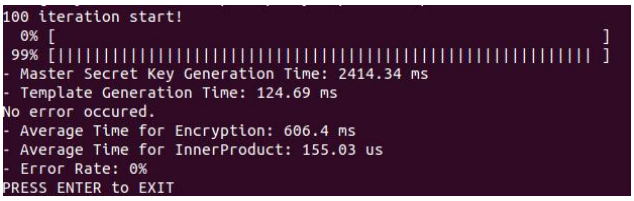
정리 1. U, D가 프로토콜을 정직하게(semi-honest) 수행하고 S와 공모하지 않으며, FFB-IPE가 안전하다고 가정 시, S는 생체정보 x,y에 대해 $\text{HD}(x,y)$ 외의 어떠한 정보도 얻을 수 없다.

3. 실험

본 논문에서 제안한 DF-PPHDM의 각 과정을 Raspberry PI 4B에서 C++로 구현하였다([표 1]).

템플릿 (bit)	Registration (ms)	Collection (ms)	Authentication (μs)
4632	82.00	11.84	7.83
145832	2539.03	606.40	155.03

[표 1] Raspberry PI에서 각 과정 100번 반복 시 평균 연산 시간



[그림 2] Raspberry PI에서의 145,832-bit 생체 템플릿 평균 연산 시간 측정 결과 화면

[표 1]에서 확인할 수 있듯이, DF-PPHDM를 사용할 경우 4,632~145,832-bit 생체 템플릿 인증을 위해 7.83~155.03μs의 연산 시간이 소요된다.

4. 결론 및 향후 계획

드론에서 얼굴 이미지를 암호화하여 전송하고 암호화된 생체 정보에 대해 효율적인 인증 연산을 수행하여 혹독한 환경에서 사람을 수색하는 인적·시간적·경제적 비용을 절약할 수 있다. 이는 프라이버시를 보호함과 동시에 공공의 안전 향상에 이바지할 수 있다. 향후, AI와 결합하여 자동화 기능을 추가하고 코드 최적화를 통해 성능을 향상할 예정이다.

참고문헌

[1] Debra R. Cohen McCullough, "Unmanned Aircraft Systems (UAS) Guidebook in Development", COPS, 2014.

[2] Cheon, Jung Hee, et al. "Lattice-based secure biometric authentication for hamming distance". ACISP 2021, Springer, 2021. p. 653-672.

[3] Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography." JACM, 56, 6, p. 1-40, 2009

[4] Quinn, George W., et al. "IREX IX part one: Performance of Iris recognition algorithms". Gaithersburg, NIST, 2018.