<주요 Q&A>

얼굴 인식용 Fuzzy Extractor를 활용한 안전한 사용자 인증

Q1. 쌍둥이 구별을 위해 홍채까지 같이 인식해야 하지 않나요?

말씀하신 대로 보다 확실한 보안을 위해서는 홍채 인식 등 보다 많은 보안이 필요하긴 합니다

Q2. 암호화 과정 없이 비밀 키로 올리는 거면 얼굴 인식도 그 대안이 될 수 있는 건가요?

암호화 과정을 얼굴인식을 통해서 하겠다는 게 핵심입니다!

Q3. 만일, 프라이빗 데이터로 복구가 안될 경우엔 다른 차선 복구방안 대책이 있을까요?

사실 얼굴에 상처를 입거나 부득이하게 인증이 불가능한 경우에는 이메일 인증과 같은 추가적인 기법들이 실제 현장에서는 고려 되야 할 것으로 보입니다.

Q4. 비밀키는 사용자가 지정하나요? 그리고 사용자 컴(모니터)에는 무조건 카메라가 장착이 되어 있어야 하는 전재가 있네요?

비밀키는 사용자가 지정할 수도 있지만 편의성을 위해서 자동적으로 select하는 것으로 보시면 될 것 같습니다.

Q5. 암호화 과정을 얼굴인식을 통해서 한다면 얼굴의 이목구비나 골격이 비슷한 사람들끼리는 보완이 취약하지 않을까요?

맞습니다. 얼굴인식의 한계이긴 합니다. 이 부분은 추후 3D 얼굴 인식 알고리즘 등을 통해서 보완이 되어야 할 것으로 보입니다.

Q6. 다수의 인원이 한꺼번에 몰릴 경우에 얼굴인식을 통한 암복호화 과정이 어느 정도 성능을 보이는지 궁금합니다.

Linear하게 증가한다고 생각하시면 될 것 같습니다.

Q7. 그럼 비밀키 테이블이 존재하나요?

비밀키 테이블은 따로 존재하지 않습니다. public data에 포함되어 있습니다. 다만 공격자는 그 값을 알 수가 없고요

Q8. 아직 휴대폰의 얼굴 인식 기능은 안경이 바뀌거나, 얼굴 각도가 조금만 달라도 인식이 어렵던데 그런 부분은 어떻게 개선이 되나요?

얼굴 인식을 개선하는 것이 저희 알고리즘의 핵심은 아닙니다. 잘 동작하는 얼굴인식 알고리즘이 있을 때, 보안성을 추가 부여할 수 있다는 게 핵심입니다

Q9. 특정 어플리케이션을 위한 연구라고 보면 되겠네요. 더 높은 수준의 보안이 필요한 경우엔 더 다양하거나 몇 스텝 더 거치는 보안이 필요하겠죠?

네 맞습니다. 보다 높은 보안을 요구하는 경우에는 추가적인 보안 요소가 필요할 것으로 보입니다.

Q10. 얼굴 인식하는 데 1ms소요된다고 회신 주셨는데, 몇 명의 얼굴 중에 1:N 인증 시에 소요되는 시간일까요?

Linear하게 증가한다고 생각하시면 될 것 같습니다.

Q11. 이목구비가 닮은 사람을 구별할 때, 앞서 3d를 쓴다고 하셨는데 그렇다면

이때 좌표계 변환을 거쳐서 적용하게 되는지 궁금합니다.

모든 얼굴인식에 적용되는 것은 아니나, 대체적으로 좌표계 변환(직교 좌표계 혹은 구면 좌표계)등을 사용해서 template이 도출된다고 보시면 될 거 같습니다.

Q12. 프라이빗 데이터 복구, 즉 얼굴인식이 안될 경우엔 다른 사용자만의 다른 추가적인 2차, 3차 암호화 모듈이 필요할 것으로 보입니다. 요새, 지문인식도 비슷한 지문이라던가 상대방의 지문을 악용하여 보안체제를 무너뜨리는 사례가 많기 때문에 단순히 얼굴 전체의 인식이 아닌 얼굴의 특징을 이용한 암호화 모듈이 좋을 것 같습니다.

맞습니다. 그래서 저희는 앞 단의 얼굴인식이 개선되고 발전되면 그에 맞춰 적용할 수 있다는 점에서 장점을 갖습니다

Q13. 1ms 의 성능을 확인할 수 있는 단위가 얼마나 되는 지 문의 드립니다.

구현 환경은 일반 사무용 desktop에서 수행되었으며, 1:N의 경우 N=1000명일 경우에는 1초 내외로 보시면 될 거 같습니다.

Q14. 사용자 인증을 하는 데 얼굴 인식용 Fuzzy Extractor를 활용하는 경우 보안 관련하여 해결하고 극복해야 할 사항들에 대해서 질문 드립니다.

얼굴인식 단독이 아닌 추가적인 보안 도구들과 함께 쓸 수 있는 방안에 대한 방법이 필요할 것으로 보입니다.

Q15. 안면인식 할 때 중요한 것은 인종을 구별하고 에이징을 분석할 수 있어야 하는데 이런 점도 고려되었는지요?

에이징 및 인종에 대한 부분은 얼굴인식 알고리즘의 모델을 생성할 때 입력되는 얼굴 사진 dataset으로 해결했다고 보시면 될 거 같습니다.

Q16. 안면인식 사용자 인증을 위해 수집한 사진정보를 모델생성을 위해서 개발업체에게 전달한다면 개인정보보호법에 위반이 되나요?

얼굴인식 알고리즘을 개발할때 사용된 dataset을 CMU등 대학에서 수집한 open data를 사용했으며, 별도의 사진 data를 사용한다면 법적인 문제는 분명 있을 것이라 보입니다. 워낙 민감한 사항이라 조심 또 조심하셔야 할 것 같습니다.

Q17. Fuzzy Extractor 기술은 기존에 생체데이터에 잘 사용되지 않던 기술인가요?

기존에 많이 사용됐습니다. 다만 홍채와 같이 binary data에 국한돼서 적용된 부분이 있습니다.

Q18. 이미지 개인정보 스캔 및 비식별화(OCR)도 가능한지요?

비식별화 서비스의 핵심은 비식별화 하고자 하는 타겟을 얼마나 정확하게 잡느냐의 문제인 것으로 보이는데, 해당 기술을 적용할 수 있을지 여부는 바로 떠오르진 않습니다.

Q19. 구현 환경 및 1ms의 퍼포먼스가 확인되는 얼굴의 수(1:N authentication)에 대하여 문의 드립니다.

구현 환경은 일반 사무용 desktop에서 수행되었으며, 1:N의 경우 N=1000명일 경우에는 1초 내외로 보시면 될 거 같습니다.

Q20. 보안성을 높이는 방법이 보안 단계를 늘리는 방법밖에 없나요? 얼굴인식 단계에서 보안성을 높이는 방법을 한계가 있나요?

얼굴인식은 spoofing attack이라는 취약점을 갖고 있으므로, 확실히 다른 보안 수단과 함께하는 것이 필요할 것으로 보입니다.

Q21. 카메라의 화소수와 거리가 어느 기준 이상 이어야 적용될 수 있을 거라 보이는데 일단 CCTV 나 이런 부분으로 도 가능한지 궁금합니다.

CCTV의 성능에 따라서 많이 달라지기는 한데, 현재로서는 그 부분까지는 달성하지 못한 것으로 보입니다.

Q22. 정교하게 제작한 사람의 머리와 실제 사람의 머리를 구분하는 것이 가능한가요?

네 이 부분은 response challenge를 사용할 수도 있습니다. 눈을 깜빡여 보세요 등등

Q23. 실제 서비스에 사용하기 위한 accuracy 기준치가 어느 정도 되나요?

FAR은 10^-6 정도를 기준으로 했을 때 TAR이 98% 이상 정도로 알고 있습니다.

Q24. Multi-Device Environment (MDE)에서 사용하는 경우 Device별로 생체정보를 등록하고 사용해야 하는 한계를 효율적으로 극복할 수 있는 방법에 대해서 문의 드립니다.

기존에는 MDE환경에서 생체 인증을 사용하려면 기기 별로 등록해야 하는 번거로움이 있었는데, 본 기술을 사용했을 때는 하나의 기기에서만 등록하면 사용 가능합니다.

Q25. 기술의 핵심은 얼굴 인증은 적용의 대표적인 예시일 뿐이고, 실수기반 코사인 유사도 기반 알고리즘에서 보안성을 높이면서 유사도 평가 성능을 유지하는 기술이라고 이해가 됩니다. 맞나요?

정확합니다 얼굴인식뿐 아니라 다양한 데이터에 대해서도 적용될 수 있습니다

Q26. Face aiDee를 활용한 얼굴 본인인증 출입통제 이용사례에 대해 설명 부탁드립니다.

Q27 개인정보 이슈는 없나요?

개인 정보 이슈를 해결하기 위한 알고리즘으로 이해하시면 될 거 같습니다. 저희가 제안한 알고리즘으로 보호를 할 경우, 서버 해킹 및 디바이스 분실에 대해서도 개인정보는 보호 된다는 것으로 이해하시면 될 거 같습니다.

Q28. 안면인식 시 인종과 에이징에 대한 점도 고려대상인데 이런 것은 어떻게 처리를 하셨는지요?

에이징 및 인종에 대한 부분은 얼굴인식 알고리즘의 모델을 생성할 때 입력되는 얼굴 사진 dataset으로 해결했다고 보시면 될 거 같습니다.

Q29. FACE aiDee를 활용하여 무인점포, 공유경제 앱 등에서 본인확인(공유사무실, 킥보드 등)에 대한 사례는 있는지요?

좋은 질문입니다. 공유 경제 앱에서 생체인증을 시도하면 편의성이 확대되지만, 서비스 제공자 (예를 들면 쏘카) 입장에서는 사용자 생체 정보를 관리하기에는 리스크가 커서 아직 단말 기반으로만 적용하는 것으로 보입니다

Q30. Binaryzation 에 비해서 Real 512 인데도 불구하고 떨어지지 않는 인식률을 보여주네요.

네 맞습니다. dimension이 낮긴 하지만 각각의 data가 담을 수 있는 양이 많아서 그런 결과가 나왔습니다

Q31. 마스크를 쓰거나 얼굴을 일부를 가려도 인식률도 문제없이 인증하실 수 있는지 궁금합니다.

마스크를 썼을 경우에, 현재는 얼굴인식이 잘 안되고 있습니다. 이를 해결하기 위해서는 얼굴인식 알고리즘을 training할때, 마스크를 쓴 얼굴을 input data로 사용하면 가능해지지 않을까 합니다

Q32. 매장 내 인원 파악 및 동선 트레킹(바디 인식)도 가능한지요?

인식의 문제를 해결한 알고리즘은 아니라서 적용은 어려울 것으로 보입니다.

Q33. 코사인 유사도 기반 알고리즘이 뭘까요?

구면 위에 찍혀 있는 template간의 유사도를 측정할 때, 내적 계산을 하게 되는데 이를 cosine 유사도 라고 보시면 될 것 같습니다.

Q34. 영상 비식별화 서비스(얼굴, 차량번호판 등)도 가능한지 궁금합니다.

비식별화 서비스의 핵심은 비식별화 하고자 하는 타깃을 얼마나 정확하게 잡느냐의 문제인 것으로 보이는데, 해당 기술을 적용할 수 있을지 여부는 바로 떠오르진 않습니다.

Q35. 퍼지 데이터를 암, 복호화키로 활용 시, 동일한 결과 값을 도출하도록 하기 위한 시스템 보정이나 보완은 어떻게 이루어 지는지요?

동일한 결과값을 도출하도록 하기 위한 별도의 시스템 보정을 필요하지 않고, SW 알고리즘에서 자체적으로 보완을 해주는 게 해당 기술의 핵심입니다.