보이지 않는 물리적 패치를 사용한 QR 코드 공격

김경헌[1], 박한훈[1,2]*

[1] 국립부경대학교 전자정보통신공학부, [2] 국립부경대학교 인공지능융합학과

alswls6758@naver.com, *hanhoon.park@pknu.ac.kr

QR Code Attack Using Invisible Physical Patches

Gyeongheon Kim[1], Hanhoon Park[1,2]*

[1] Div. of Electronics and Communications Engineering, Pukyong National Univ.
[2] Dept. of Artificial Intelligence Convergence, Graduate School, Pukyong National Univ.

요 약

본 논문은 눈에 보이지 않는 물리적 패치를 QR 코드에 부착하여 원하는 타겟 QR 코드로 인식하도록 하는 적대적 공격(adversarial attack) 방법을 제안한다. 실험을 통해 재귀반사(retro-reflective) 테이프를 부착하여 QR 코드를 변경함으로써 광원과 다른 방향에서는 공격 여부를 알 수 없지만 광원과 같은 방향에서는 타겟 QR 코드로 인식될 수 있음을 확인하였다.

Ⅰ. 서 론

QR(Quick Response) 코드는 디지털 세계로의 물리적인 포인터로서, 디지털 정보 제공, 웹 사이트 이동, 인증 등 다양한 응용 분야에 적용, 활용되고 있다. QR 코드는 카메라로 촬영한 이미지 정보를 기반으로 검출, 인식되는데 고도의 오류 정정 기능을 갖고 있기 때문에 이미지 정보가 크게 훼손되거나 변경되지 않는 한 높은 정확도로 검출, 인식된다. 그러나, 오류 정정 기능을 역이용하여 눈에 띄지 않게 QR 코드를 변경할 경우, 사람은 QR 코드의 변경 여부를 알 수 없으나 인식 시스템은 잘못된 정보를 제공하도록 공격할 수 있다. 본 논문에서는 이와 관련하여 눈에 보이지 않는 물리적 패치를 사용한 QR 코드 공격 방법을 제안한다.

일반적인 카메라 센서나 촬영 각도에서는 검게 보이지만 특정 파장의 센서나 촬영 각도에서는 밝게 보이는 물리적 패치를 사용한다. 즉, 물리적 패치를 QR 코드의 흑색 셀(cell)에 부착하면, 일반적인 카메라 센서나 촬영 각도에서는 QR 코드에 패치 부착 여부를 알 수 없지만 특정 파장의 센서나 촬영 각도에서는 패치가 부착된 흑색 셀이 백색 셀로 인지되어 기존 QR 코드에 담긴 정보가 아닌 다른 정보를 전달하게 된다. 같은 원리에 기반하여 기존에 적외선 레이저를 활용한 방법[1]이 제안되었으나, 고가의 레이저 장비와 정밀한 레이저 투사를 요구하기 때문에 실생활에서 구현이 어렵다는 한계가 있다. 본 논문에서는 구현상의 편의를 위해 재귀반사(retro-reflective) 테이프를 사용한다. 재귀반사 테이프는 빛을 광원 방향으로 강하게 반사시키기 때문에, 광원과 다른 방향에서는 QR 코드의 공격 여부를 알 수 없지만 광원과 같은 방향의 카메라 센서는 해당 셀을 포화된 백색으로 인식하게 하기 때문에, QR 코드는 다르게 인식된다.

Ⅱ. 실험 및 결과

실험을 위해 segno 라이브러리[2]를 사용하여 Version 2-M 규격의 QR 코드를 생성하여 사용하였다. 해당 규격은 총 44개의 코드워드 중 16개가 오류 정정 코드로 할당되어 있으며, 최대 8개의 코드워드 손상을 복구할 수 있다. 따라서, 공격 대상의 QR 코드의 흑색 셀을 백색 셀로 바꾸면서 타겟 QR 코드와는 8개 이하의 코드워드 차이를 가지도록 해야 한다. 그림 1은 “attack”을 의미하는 원본(Cover) QR 코드와 “afpack”을 의미하는 타겟(Target) QR 코드를 보여주며, 파란색과 빨간색으로 표시된 영역이 서로 다른 값을 가지는 셀이다. 빨간색 셀은 원본에서는 흑색이고 타겟에서 백색이므로 공격 패치를 부착하면 되지만, 파란색 셀은 원본에서는 백색이고 타겟에서 흑색인 셀로 공격할 수 없다. 따라서, 파란색 셀을 포함하는 코드워드 수가 8을 초과하면 타겟 QR 코드로 인식할 수 없다. “attack”과 “afpack”의 경우 8이므로, 그림 2에서 보는 것처럼 빨간색 셀에 부착된 패치가 백색으로 인식된다면 “attack” QR 코드는 “afpack” QR 코드로 인식된다. 즉, 광원과 다른 방향에서는 보이지 않는 물리적 패치를 부착하여 원본 QR 코드가 타겟 QR 코드로 인식되었다.

그림 1. 원본 QR 코드, 타겟 QR 코드, QR 코드의 구조 및 차이 시각화.

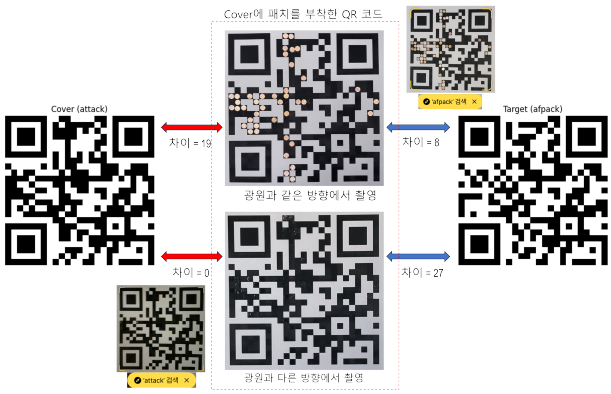

그림 2. 보이지 않는 물리적 패치를 사용한 QR 코드 공격 결과.

참 고 문 헌

[1] D. Itakura, et al., “A targeting attack by dynamic fake QR code using invisible laser irradiation,” Proc. of ICISSP, pp. 455-462, 2025.

[2] https://segno.readthedocs.io/en/latest/