初稿

* Related work
* Fingerprint system attack

Prevailing fingerprint recognition systems are vulnerable to spoof attacks. There are lots of novel approaches of spoof attack having proposed. For example, \citet{DBLP:journals/tifs/Arora0JP16} designed a new method of fabricating an universal 3D fingerprint target for repeatable behavioral (black-box) evaluation of fingerprint reader. It managed to pass three different PIV/Appendix F certified optical fingerprint readers. And \citet{DBLP:journals/corr/EngelsmaAJJ17} presented how to manufacture a new 3D fingerprint target which is effective to capacitive, contact-optical, and contactless-optical fingerprint readers . But they only preserved the 2D calibration pattern of fingerprint. Besides, \citet{DBLP:conf/btas/2018} proposed a GAN-based method to generate image-level MasterPrint \cite{DBLP:journals/tifs/RoyMR17} used to launching dictionary attacks against a fingerprint verification system.

* Fingerprint Anti-spoofing approaches.
* Hardware-based

The hardware-based methods usually use extra or better devices to extract optical features of fingerprint. \citet{DBLP:journals/prl/MarascoS12} combined perspiration feature and morphology feature by using high-resolution sensors to capture the images of fingerprint. New combined features contain more information than each feature. \citet{article2} utilize the fact that the the surface of fake fingerprints is rougher than the surface of live fingerprint. They use the image captured by high-resolution sensors to detect fake fingerprint.

* Software-based

Software-based fingerprint anti-spoofing approaches try to detect fake fingerprint only using the existing hardware design. Now, machine learning algorithms and deep learning algorithms are most popular methods in image processing. They also have a wide range of applications in fingerprint recognition . \citet{DBLP:journals/tifs/NogueiraLM16} firstly try to use convolutional neural network to detect fake fingerprint. \citet{inproceedings} did similar work with Nogueira et al. But they replaced VGG-19 \cite{DBLP:journals/corr/SimonyanZ14a} with GoogleNet \cite{DBLP:conf/cvpr/SzegedyLJSRAEVR15}. Although CNN models perform very well, it spends too much time and memory. \citet{DBLP:conf/biosig/ParkKLKK16} proposed a improved method based on convolutional neural network (CNN) features extracted from fingerprint patches. \cite{DBLP:journals/corr/abs-1803-07830} and \cite{DBLP:journals/tifs/ParkCNK19} proposed separately a new CNN structure with less parameters and lower average detection error rate. But all of them require training samples from both classes. They are possible to fail to detect fake fingerprint of unknown material. So \citet{DBLP:conf/wifs/DingR16} tried to use one class classifier to detect fake fingerprint. They proposed the method used an ensemble of one-class SVMs based on different data sets to detect spoofs generated from previously “unseen” materials. \citet{DBLP:journals/corr/abs-1901-03918} accomplished a one-class classifier through training multiple generative adversarial networks (GANS) to recognize live fingerprint.Though its performance is far better than OC-SVM\cite{DBLP:conf/wifs/DingR16}, its processing speed is much lower than OC-SVM and CNN model.

* Additional sensor based: sweat detector, oxygen saturation detector

Apart from traditional optical hardware-based approaches, additional sensor based approaches are also prevalent to detect live fingerprint. It usually uses extra physical features of the human body to help detect fake fingerprint. Typically, Additional sensor based methods use sweat detector, oxygen saturation detector and skin odor detector. \citet{DBLP:journals/tbcas/ReddyKRM08} proposed a method based on the principle of pulse oximetry, it utilizes the light originating from a probe at two wavelengths to compute the percentage of oxygen in the blood, which can successfully differentiate live finger tips from fake finger tips. \citet{DBLP:conf/icb/BaldisserraFMM06} proposed a method based on odor sensor. It distinguishes between live fingers and fake fingers made of latex, silicone or gelatin by odor signal. But it has no effect on fake finger made of other materials. \citet{DBLP:conf/biosig/SousedikBB13} used the Optical Coherence Tomography (OCT) to obtain a 3D volumetric representation of the scanned fingerprint and took advantage of the structure of high-resolution 3D volumetric scans of fingertips to detect artificial fingers. \citet{article1} innovatively used sub-surface fingerprint with sweat ducts captured by correlation mapping optical coherence tomography (cmOCT) to certified identity. But the captured time of OCT device is long. \citet{DBLP:journals/corr/abs-1908-00102} used the better OCT device and found the profile feature is different between the live finger and fake finger.So they used CNN model to analysis 2D OCT depth profile from cross-sectional B-Scans, which is robust and quick. However, they are hard to integrate additional sensor into existing fingerprint system. And their cost is high than other methods ,especially OCT. In order to reduce costs, \citet{DBLP:journals/access/Goicoechea-Telleria19} proposed effective method to detect fake fingerprint using two low-cost handheld microscopes with special lighting conditions.

[1] Design and Fabrication of 3D fingerprint targets

[2] Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations

[3] DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution

[4] MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems

[6] Fingerprint Liveness Detection Using CNN Features of Random Sample Patches

[7] End-to-End Fingerprints Liveness Detection using Convolutional Networks with Gram module

[8] Presentation Attack Detection Using a Tiny Fully Convolutional Network

[9] Fingerprint Liveness Detection Using Convolutional Neural Networks

[10] An ensemble of one-class SVMs for fingerprint spoof detection across different fabrication materials

[11] Generalizing Fingerprint Spoof Detector: Learning a One-Class Classifier

[12] Robust and interoperable fingerprint spoof detection via convolutional neural networks

[13] Very deep convolutional networks for large-scale image recognition

[14] Going deeper with convolutions

[15] Combining perspiration- and morphology-based static features for fingerprint liveness detection

[16] A New Antispoofing Approach for Biometric Devices

[17] Feasibility of correlation mapping optical coherence tomography (cmOCT) for anti‐spoof sub‐surface fingerprinting

[18] Volumetric fingerprint data analysis using optical coherence tomography

[19] Low-Cost and Efficient Hardware Solution for Presentation Attack Detection in Fingerprint Biometrics Using Special Lighting Microscopes

[20] Fake fingerprint detection by odor analysis

[21] Wavelet based fingerprint liveness detection[22]OCT Fingerprints: Resilience to Presentation Attacks

Software-based : dynamic and static method