Fake Detection bei dem Fingerabdruck

Tim Hirschberg
Fachbereich Informatik
Hochschule Bonn-Rhein-Sieg
Sankt Augustin, Deutschland
Email: tim.hirschberg@inf.h-brs.de

***Zusammenfassung*—Mit dem wachsenden Interesse an biometrischen Daten zur Authentisierung, steht auch die Sicherheit dieser Verfahren auf dem Prüfstand. Dabei wird häufig der Fingerabdruck zur Authentifizierung verwendet. Für Angreifer ist es jedoch sehr einfach einen Fingerabdruck seines Opfer zu bekommen. Anschließend kann er daraus einen künstlichen Finger (Fake) erzeugen. Daher ist die Fake Erkennung (Fake Detection) sehr wichtig. Diese soll in dieser Arbeit näher betrachtet werden. Zuerst wird dafür erläutert, welche Arten von Fakes es gibt und wie diese Hergestellt werden. Anschließend werden verschiedene Möglichkeiten der Fake Detection betrachtet. In einem letzten Schritt werden daraufhin Angriffe auf die Fake Detection untersucht und beschrieben. Dabei soll auch bewertet werden, wie gut einzelne Maßnahmen zur Fake Detection wirken und wie gut die Möglichkeiten der Umgehung der Maßnahmen funktionieren.**

I. Einleitung

Die unkomplizierte, schnelle und korrekte Identifikation und Authentisierung von Personen ist sehr wichtig. Dabei besitzen biometrische Merkmale ideale Voraussetzungen. Diese sind den traditionellen Verfahren, wie Passwort oder Token, überlegen. Biometrische Merkmale sind eindeutig einzelnen Personen zuzuordnen und können schwer erraten oder künstlich erzeugt werden. Weiterhin ist ein Verlust oder der Diebstahl dieser Merkmale sehr schwierig.

Biometrische Merkmale sind eindeutige Merkmale eines Menschen. Das Wort Biometrie kommt aus dem Griechischen und setzt sich aus dem Wort *bios*, was Leben bedeutet, und dem Wort *metron*, welches Maß bedeutet, zusammen. Daraus folgt, das die Biometrie, die Wissenschaft des Messens von Leben ist. Dabei werden nur körperliche Merkmale des Menschen betrachtet. In der IT-Welt wird dies häufig weiter eingeschränkt. Hierbei werden nur Merkmale betrachtet welche sich zur Authentifizierung von Personen gegenüber eines Systems eignen. Es gibt zwei Arten von biometrischen Merkmalen: aktive (verhaltenstypische) und passive (physiologische) Merkmale. Unter aktiven Merkmalen werden z.B. die Stimme oder die Unterschrift gezählt. Passive Merkmale sind z.B. der Fingerabdruck oder das Gesicht [1]. Im Rahmen dieser Arbeit wird der Fingerabdruck als biometrisches Merkmal betrachtet.

Eine Gefahr bei der Authentifizierung mit biometrischen Merkmale sind Fakes. Dies sind nach dem Original erzeugte biometrische Merkmale, mit denen sich ein Dritter als Besitzer dieses Merkmals ausgeben kann. Gerade bei den hier betrachtete Fingerabdrücken ist diese Gefahr sehr hoch, da Fingerabdrücke überall hinterlassen werden. Somit hat ein Angreifer sehr gute Voraussetzungen an den Fingerabdruck seines Opfers zu gelangen. Ideal sind dabei glatte Oberflächen, wie Glasflaschen oder Displays von Smartphones. Daraus kann der Angreifer dann einen künstlichen Finger mit dem Abdruck des Opfers erstellen. Beispielsweise aus Latex oder Holzleim. Eine weitere Möglichkeit als die Authentifizierung mit dem Fake ist dabei auch das platzieren von Fingerabdrücken, z.B. an Tatorten.

Wie einfach Fingerabdruckscanner mit Fakes umgangen werden können zeigt der Chaos Computer Club anhand des iPhone 6s. Dabei konnte mit wenig aufwand ein Fake erzeugt und der biometische Scanner umgangen werden. Alles was nötig ist, um an den Fingerabdruck zum erzeugen des Fakes zu kommen, ist ein hochauflösendes Bild des Fingerabdrucks auf der Oberfläche des Smartphone selbst. Anschließend wird mithilfe des Bildes ein Fake aus Holzleim erzeugt. Mit diesem kann sich dann ein dritter am Smartphone authentifizieren [2]. Anhand diese Beispiels wird sehr schön gezeigt, dass eine gute Fake Detection zwingen notwendig ist.

Auch kann gezeigt werden, dass es noch einfacher ist an Fingerabdrücke zu kommen. Ein Angreifer muss nicht mehr in der nähe des Opfers sein, um z.B. den Fingerabdruck von einem Glas, dem Smartphone oder ähnlichem zu nehmen. Es reichen gut aufgelöste Fotos der Finger aus, um an die entsprechenden Fingerabdrücke zu gelangen. Diese Bilder können mit Spiegelreflexkameras geschossen werden oder mit heutigen Smartphones aus der Nähe. Auch mit hochauflösendem Videomaterial kann gearbeitet werden. Eine besondere Gefahr entsteht hierbei, da der Angreifer nicht in die Nähe des Opfers kommen muss. Sondern den Angriff auch remote über das Internet führen kann. Beispielsweise können Fingerabdrücke aus Pressefotos oder über Malware auf dem Smartphone entwendet werden. [3] [4]

Bei der Fake Detection geht es darum, dass erkannt wird, ob es sich um den echten Finger des Benutzers handelt oder nicht. Häufig wird dafür eine Lebenderkennung (liveness detection) verwendet. Dabei werden beispielsweise Temperatur oder Puls verwendet. Auch andere Möglichkeiten der Fake Detection sind möglich. Unter anderem kann der Leitwiederstand des Fingers zur Erkennung von künsltlichen Fingern verwendet werden oder die Lage der Schweißporen im Finger. [5]

Nach einer kurzen Einführung in die Fingererkennung werden anschließend die verschiedenen Arten von Fakes erläutert. Daraufhin werden auf den folgenden Seiten verschie-

dene Verfahren der Fake Detection beschrieben untersucht und evaluiert. Dabei werden zuerst "klassisch"Methoden der Fakeerkennung, sowie Angriffe auf diese vorgestellt. Anschließend werden fünf weitergehende Ansätze der Fake Detection aufgezeigt und diskutiert.

II. Grundlagen der Fingererkennung

Die charakteristischen Merkmale eines Fingerabdrucks nennt man Minutien. Diese werden auch Minuzien geschrieben. Diese Minutien sind die einzelnen elementaren Merkmale des Fingerbildes (Gabelungen, Knoten, Schleifen) [6]. Diese liegen unmittelbar auf den Papillarlinien. Dies sind die Linien auf der Haut des Fingers, welche bei Berührung auf Oberflächen, wie z.B. Gläsern, hinterlassen werden. [7]

Die Extraktion der Minutien erfolgt unabhängig der verwendeten Scanner. Dieser Vorgang ist in Abbildung 1 zu sehen. Hierbei sind die roten Punkte beispielhaft gefunden Minutien. Es sind jedoch keine echten Minutien. Diese sollen nur den Extraktionsvorgang erläutern. Eine echte Minutie im Bild stellt beispielsweise die Gabelung unten rechts im Fingerbild oder die Schleife in der Mitte da. Zuerst wird ein Bild des Fingeradruckes erfasst. In diesem Bild werden anschließend die Minutien ermittelt und je nach Verfahren Position, Ausrichtung und Art des Merkmales betrachtet.

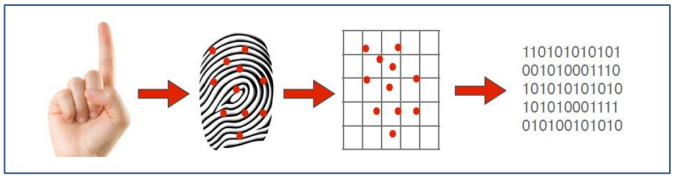


Abbildung 1. Beispielhafter Ablauf zur Fingerabdruckerfassung [8]

Dabei können sechs verschiedene Schritte unterschieden werden: [7]

1) Die Aufnahme des Fingerandruckbildes:

2) Bildqualitätsverbesserung: Hierbei wird eine optische Verbesserung der Papillarlinen erreicht, um eine bessere Erkennung zu gewährleisten.

3) Bildaufarbeitung: Auch hier wird das Fingerbild bearbeitet um eine bessere Erkennung zu erreichen. (Abbildung 2)

4) Musterklassifizierung: Fingerabdrücke können grob in drei Hauptklassen eingeteilt werden. Diese wird im Normalfall nur bei daktyloskopischen Systemen (z.B. AFIS des BKA) eingesetzt. Daher wird hier nicht weiter darauf eingegangen.

5) Merkmalextraktion: In diesem Schritt wird die Lage der der Minutien detektiert und extrahiert. Dabei beeinträchtigt die Bildqualität die Leistungsfähigkeit des Extraktionsalgorithmus.

6) Verifikationsphase: Hierbei werden zwei Merkmalsvektoren verglichen. Dabei wird bestimmt ob zwei Fingerabdrücke übereinstimmen oder nicht.

Das hinzufügen eines Fingers zur Datenbank wird Enrollment genannt. Dazu werden die so erhobenen Daten als Referenzdaten gespeichert. Soll ein Benutzer authentifiziert

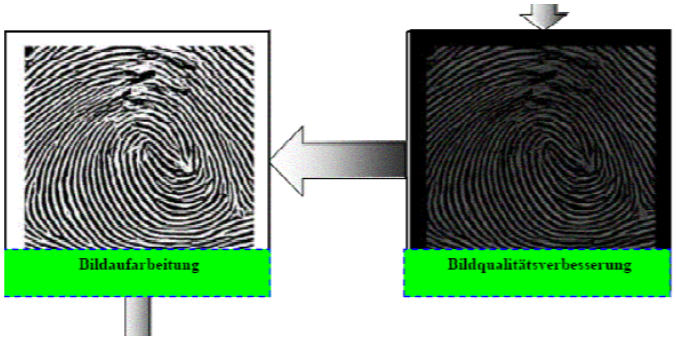


Abbildung 2. Bildverbesserungsmaßnahmen bei der automatischen Erkennung von Fingerabdrücken [7]

werden, wird von der Verifikation gesprochen. Hierbei werden die erhobenen Daten mit den Referenzdaten verglichen. Diese Daten sind niemals 100% identisch, daher wird bei einer ausreichend hohen Übereinstimmung der Nutzer akzeptiert.

Es werden hauptsächlich zwei Fehlerraten betrachtet. Einmal die False Acceptance Rate (FAR) und die False Rejection Rate (FRR). Die FAR betrachtet alle falsch akzeptierten Nutzer. Also Dritte die sich mit Ihrem Finger als legitimer Nutzer authentifizieren können. Diese kann zu einem Sicherheitsproblem führen. Bei der FRR ist der Gegenteil der Fall. Hier werden legitime Nutzer nicht erkannt. Hierbei kann die Nutzerakzeptanz beeinträchtigt werden, da sich legitime Nutzer eventuell mehrfach authentifizieren müssen. Beide Fehlerraten stehen in direktem Zusammenhang. Wird die eine Rate verbessert, verschlechtert sich die andere. [9]

Arten von Fingerabdrucksensoren

Fingerabdrücke können mithilfe verschiedenster Sensoren erfasst werden. Die Informationen zu den Sensoren stammen, wenn nicht anders kenntlich gemacht, aus der Arbeit von Johan Blommé. [10]

7) Optischer Sensor: Bei optischen Sensoren wird ein Photo vom Fingerabdruck gemacht. Dazu beleuchtet eine LED den Finger von unten und die Reflexion des Lichtes fällt durch Prismen und Linsen auf eine Kamera, welche das Bild speichert. Heutzutage werden dazu CMOS Kameras verwendet.

8) Kapazitiver Sensor: Der Kapazitive Sensor arbeitet ähnlich wie der Sensor mit dem elektrischem Feld. Hierbei wird nicht das elektrische Feld sondern die Unterschiedlichen elektrischen Kapazitäten zwischen den Bergen und Tälern des Fingers gemessen. Genauer werden hierbei die Kapazitäten zwischen der Haut der Berge und der Luft in den Tälern unterschieden.

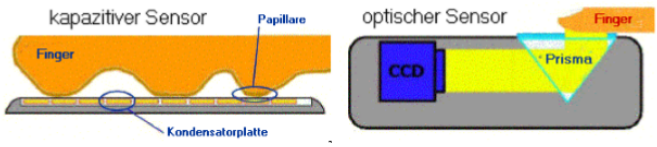


Abbildung 3. Kapazitiver und Optischer Sensor (Schema) [7]

9) Elektisches Feld Sensor: Bei dieser Art von Sensoren werden die Unterschiede in der leitfähigen Schicht unterhalb der Haut gemessen. Diese entstehen durch die unterschiedliche Dicke der Berge und Täler der Papillarlinien. Der Sensor wird in ein Feld von Pixeln aufgeteilt, um so die verschiedenen Bereiche einzeln Messen zu können und ein Bild des Fingerabdruckes zu erzeugen.

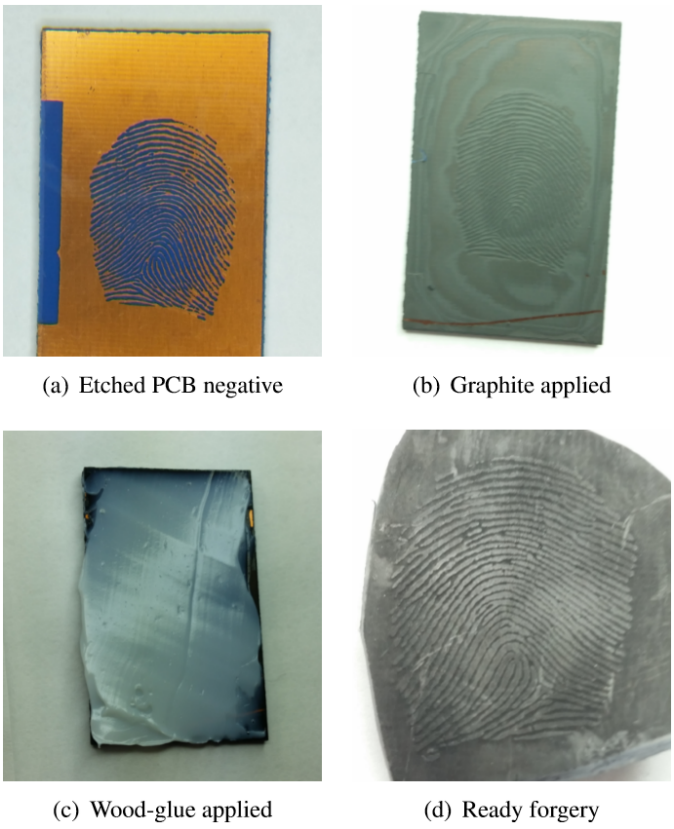
10) Ultraschall Sensor: Bei diesen Sensoren werden Schallwellen mit einer Frequenz über der Grenze des menschlich Hörbaren (20kHz) bis zu mehreren GHz verwendet. Dabei wird die akustische Impedanz gemessen, um so ein Bild des Fingerabdruckes zu erzeugen. Die große Bandbreite der Frequenzen ist nötig, um eine ausreichend Hohe Auflösung zu gewährleisten, sodass die Fingerabdrücke unterscheidbar sind.

11) Temperatur Sensor: Der Temperatur Sensor verwendet ein Feld aus temperaturempfindlichen Elementen, um die Temperaturunterschiede zwischen den Bergen und der Luft in den Tälern der Papillarlinien zu bestimmen und daraus die Form des Fingerabdruck abbildet. Temperatur Sensoren sind häfig kleiner als ein Finger. Daher wird bei diesen Sensoren nicht der Finger auf einmal gescannt. Der Finger wird über diese Art von Sensoren gestrichen, um so den gesamten Finger zu erfassen.

12) Drucksensor: Ein Drucksensor besteht aus einer elastischen Oberfläche, welche die Unterschiede im Druck der Berge und Täler der Papillarlinien auf der Oberfläche erkennt. Daraus wird das Bild des Fingerabdruckes erzeugt.

III. Arten der Fakes

Es gibt verschiedenste Arten von Fakes. Angefangen mit einfachen Bildern über Attrappen aus Holzleim bis zur Latexnachbildung. Der erste Schritt zur Erstellung eines Fakes ist die Beschaffung des Fingerabdruckes des Opfers. Dazu gibt es mehrere Möglichkeiten. Eine Möglichkeit besteht darin das Opfer freiwillig zur Abgabe der Fingerabdrücke zu bewegen. Diese Möglichkeit ist aber eher unwahrscheinlich. Ein weitaus wahrscheinlichere Möglichkeit zur Akquirierung von Fingerabdrücken ist, diese von einer glatten Oberfläche wie einem Glas oder Smartphone abzunehmen. Dazu wird ein hochauflösendes Foto vom Fingerabdruck auf der Oberfläche gemacht. Dieses wird anschließend am PC bearbeitet. Dazu wird das Bild invertiert, gespiegelt, nach schwarzweiß konvertiert, bereinigt und unscharfe Stellen ausgebessert. Anschließend wird das Fingerabdruckbild mit hoher Auflösung auf Folie gedruckt. Mit dieser Maske wird anschließend eine photosensitive Leiterplatte belichtet, um daraus eine Abgussform zu entwickeln. Mithilfe der Gussform kann anschließend mit dem Material der Wahl der Fake erzeugt werden. In der Quelle des Chaos Computer Clubs [2] wird als Material für den Fake Holzleim verwenden. Auf die Leiterplatte kommt zuvor etwas Graphit um den Fake anschließend besser von der Form zu lösen. Das Graphit verbessert zudem den Leitwiederstand des Fakes, womit dieser näher an einen echten Finger kommt. Nach dem Graphit wird der Holzleim aufgetragen. Wenn dieser getrocknet ist, kann er von der Leiterplatte entfernt werden und der Fake ist fertig. [4]



(a) Etched PCB negative (b) Graphite applied

(c) Wood-glue applied (d) Ready forgery

Abbildung 4. Von der Leiterplatte zum Fake [2]

Abbildung 5. Weitere Möglichkeiten um an den Fingerabdruck zu gelangen [2]

Eine weitere Möglichkeit besteht darin, den Fingerabdruck aus hochauflösenden Bildern zu extrahieren. [3] Dabei sind die Schritte die gleichen, wie bei der Fakeerzeugung eines Fingerabdruckes auf einer Oberfläche.

IV. Fake Detection

Im Bereich der Fake Detection gibt es schon einige etablierte Methoden. Diese können mit mehr oder weniger Aufwand Umgangen werden und bieten nur einen rudimentären Schutz. Diese Methoden werden zuerst vorgestellt. Anschließend werden gängige Angriffe auf Sensoren und Möglichkeiten die Fake Detection zu Umgehen näher erläutert. Zum Schluss des Kapitels werden weitere Methoden aufgezeigt und diskutiert.

A. Klassische Methoden der Fake Detection

Bei den klassischen Methoden gibt es vier etablierte Methoden. Diese sind die Messung von Temperatur, Puls, Blutruck und Leitwiderstand der Haut.

1) Temperatur: Die normale Temperatur eines lebenden Finger liegt zwischen 30°C und 36°C. [11] Äußere Einflusse können diese jedoch verändern, z.B. wenn die Außentemperatur niedrig ist, ist auch die Figertemperatur geringer. Sensoren die in Außenbereichen verwendet besitzen daher häufig einen noch größeren Toleranzbereich. Dadurch ist es einfach mithilfe eines Fakes innerhalb des Toleranzbereiches zu liegen. [12]

2) Puls: Auch der Puls kann zur Fake Detection verwendet werden. Auch hier gibt es ein ähnliches Problem wie bei der Temperatur mit einem sehr großen Toleranzbereich. Ein sportlicher Mensch kann einen Ruhepuls von unter 40 Schlägen pro Minute besitzen. Um hier einen Puls zu erfassen muss diese Person den Finger über 4 Sekunden Bewegungslos auf dem Sensor liegen lassen. Sollte die Person sich vorher körperlich betätigt haben oder sehr aufgeregt sein kann der Puls bei über 80 Schlägen die Minute liegen. [12]

3) Blutdruck: Die Messung des Blutdrucks hat die gleichen Probleme wie die Messung des Pulses. Zusätzlich muss der Blutdruck an zwei Punkten gemessen werden, z.B. mithilfe von zwei Fingern. [12] Auch der Toleranzbereich ist sehr groß. Gerade wenn Bluthochdruck oder andere Blutdruckkrankheiten mitbedacht werden. [11]

4) Leitwiderstand: Der elektrische Widerstand eines Fingers liegt bei ca 200k Ohm . Ist der Finger jedoch sehr trocken kann der Widerstand auf mehrere Megaohm wachsen. Bei feuchten, z.B. schwitzigen, Fingern liegt der Widerstand nur noch bei wenigen Kiloohm. [12] Gemessene Wiederstandwerte liegen zwischen 20k Ohm und 3M Ohm. [11]

B. Angriffe auf Fingerabdruck Sensoren

Die einfachsten Art eines Angriffes mit einem Fake auf die einen Sensor, ist die Verwendung einer schwarz-weiß Kopie auf einem Blatt Papier vom Fingerabdruck des Opfers. Einfache Sensoren lassen sich damit schon Umgehen. [11] Ist eine einfache Kopie nicht ausreichend, muss ein Fake erzeugt werden. Hierbei können verschiedenste Materialien verwendet werden. Aufgrund ihrer Eigenschaften und der Nähe am menschlichen Finger wird häufig Gelatine oder

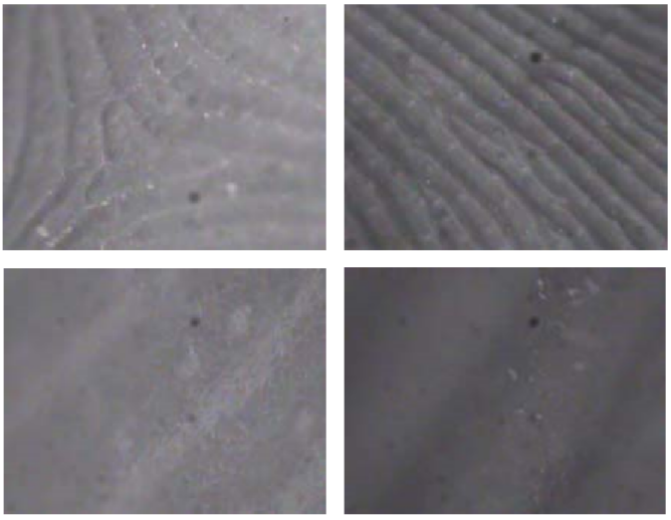


Abbildung 6. Vergleichsbilder einer CCD Kamera bei 4-fach (obere Reihe) und 10-fach Zoom (untere Reihe) [11]

Silikon als Material für Fakes verwendet. [10] [13] [11] [14] Diese Materialien sind ähnlich elastisch und weich, wie die Haut eines echten Fingers. Aber auch stabil genug, um den Fingerabdruck in seiner Form zu erhalten. Silikon wird bei einigen Kapazitiven Sensoren nicht richtig erkannt, da hier der Leitwiederstand um einiges Höher ist als bei einem echten Finger. Hier kann das befeuchten Abhilfe schaffen. Teilweise reicht in einfaches ablecken des Silikonimitates. [13] Eine weitere Möglichkeit die Effizienz des Fakes im Bereich der Leitfähigkeit des Materials zu erhöhen ist die Verwendung von Graphitspray bei der Fakeerzeugung . Dieses wird vor dem Aufbringen des Fakematerials auf die Form gesprüht. Ein weiterer Positiver Nebeneffekt ist das einfachere Ablösen des Imitats von der Gussform. [2] [4]

Auch andere Materialien wie Holzleim, Gummi oder Latex finden Anwendung. [2] [14] [4] Diese werden jedoch häufiger als Fälschungen erkannt. Gegen einige Schutzmaßnahmen kann ein dünnerer Fake helfen. Dies ist insbesondere bei Temperatursensoren wirkungsvoll. Bei diesen ist der Toleranzbereich recht hoch, wodurch die Steigerung der Temperatur am Fake durch wenige Grad oft schon zur Akzeptanz des falschen Fingers führt. Ähnlich kann der Puls und der Blutdruck durch einen hauchdünnen Fake vom Finger des Angreifers gemessen werden. Somit sind diese drei Methoden der Fake Erkennung mit einfachen Mitteln zu Umgehen. Wie weiter oben schon beschrieben ist auch die Schutzmaßnahme den Widerstand zu messen, nicht ausreichend. Hierbei kann das Anfeuchten des Fakes den eigentlich zu hohen Widerstand des Fakematerials auf einen Wert innerhalb des großen Toleranzbereiches senken. [11] Ein Fake aus Gelantine hat einen Leitwiederstand sehr nahe am echten Finger und kann so schon alleine durch Messungenauigkeiten als echter Finger erkannt werden. [15]

C. Weitere Möglichkeiten der Fake Detection

Bisher wurde einige übliche Methoden zur Fake Detection vorgestellt. Alle vorgestellten Methoden, haben den selben

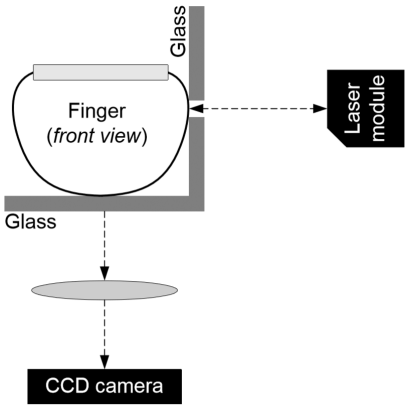


Abbildung 7. Aufbau zum Messen der Bewegung der Papillarlinien Mithilfe eines Lasers [11]

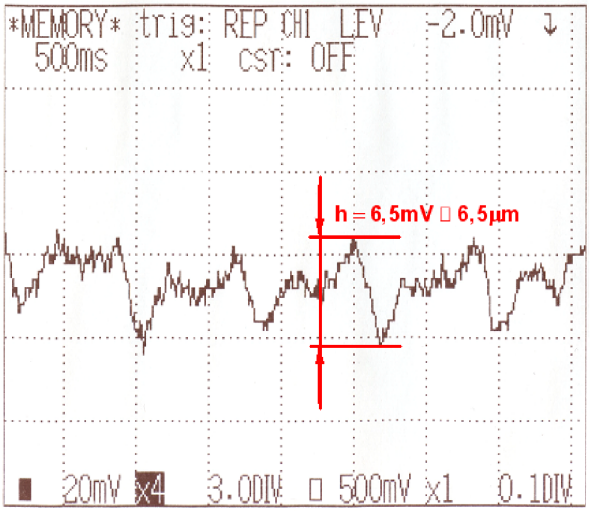


Abbildung 8. Beisielmessung des Lasers. Die x-Achse stellt die Zeit da, die y-Achse den Abstand [11]

Nachteil. Sie sind alle mit einfachen Möglichkeiten zu umgehen und bieten nur einen rudimentären Schutz vor Angriffen. Nun sollen weitergehende Methoden vorgestellt werden, welche einen besseren Schutz bieten sollen. Dabei werden Ansätze betrachtet, welche mit zusätzlicher Hardware arbeiten, sowie Software-basierende Ansätze.

1) Bewegung der Papillarlinien: Das erste Verfahren arbeitet mit zusätzlicher Hardware. Hierbei soll ein Laser oder eine Kamera geringste Bewegungen der Papillarlinien feststelle, welche durch den Blutfluss innerhalb des Fingers hervorgerufen werden. Die Methode mit der Kamera scheitert an der geringen Bildqualität, wie zu sehen in Abbildung 6. Da sich die Bewegungen im µm Bereich befinden, ist der der 4-Fache Zoom nicht ausreichend, um dort Bewegungen festzustellen. Bei dem 10-fachen Zoom können keine Referenzpunkte mehr erkannt werden, um so eine Erkennung zu ermöglichen.

Die Messung mit dem Laser konnte durchgeführt werden. Die Bewegung wird hierbei durch Triangulation ermittelt. Der Laser sitzt bei diesem Verfahren seitlich zum Finger. (Abbildung 7) Hierbei übernimmt der Laser die gesamte Abstandsmessung. In den Versuchen wurde der Laser direkt an einen Plotter angeschlossen. Die CCD Kamera erfasst einzig den Fingerabdruck. In den Experimenten konnte gezeigt werden, dass eine Bewegung eines Punktes auf der Haut von ca. 6,5µm festgestellt werden konnte. (Abbildung 8) Dies lässt auf eine Papillarbewegung schließen. Dies wird zudem von der Tatsache unterstützt das die Bewegung periodisch ist.

Dieses Verfahren eignet sich zur Lebenderkennung, da die Bewegung der Papillarlinen periodsich ist und direkt mit einem vorhandenen Herzschlag zusammen hängt. Bei dem Versuch dieses Verfahren mithilfe eines Fakes zu umgehen, würde die Eigenschaften der Bewegung stark verändern und ist dadurch einfach zu entdecken. [15] [11]

Je nach Position des Lasers kann die Abstandsmessung jedoch auch den Finger des Angreifers messen. So ist dies Beispielsweise der Fall wenn der Laser, wie vorgeschlagen Seitlich des Fingers liegt. Hierzu muss ein Angreifer nur einen Fake, welcher nicht den seitlichen Finger bedeckt erstellen. Dadurch erfasst der Laser eine Bewegung und denkt der erfasste Fingerabdruck ist echt. Dies kann durch eine neue Positionierung des Lasers unterhalb des Fingers parallel zur CCD Kamera gelöst werden. Ob der Laser hierbei eine Erfassung des Fingerabdrucks beeinträchtigt muss dabei untersucht werden. Jedoch können auch beide nacheinander arbeiten. So könnte zuerst der Laser die Echtheit des Fingers bestätigen und anschließend wird mithilfe der Kamera das Fingerbild aufgenommen.

2) Fake Fingerprint Detection by Odor Analysis: Das zweite Verfahren verwendet zur Fakeerkennung den Geruch des Fingers. Dazu wird ein Geruchssensor in den Fingerabdrucksensor integriert. Somit benötigt diese Verfahren auch zusätzliche Hardware. Wie diese Integriert werden soll, ist in dem Paper nicht genau erläutert. Jedoch sind die Sensoren sehr klein (wenige mm²) und kostengünstig und sollen so einfach zu integrieren sein. Das Verfahren erfasst den Geruch in drei Schritten: Kalibrierung, Aufnahme und Wiederherstellung. In der ersten Phase, Kalibrierung, ist das System im Leerlauf. Es liegt also kein Finger auf dem Fingerabdrucksensor. Dabei erstellt das System eine Baseline für die Erfassung und misst den natürlichen Geruch der Umgebung. Die Aufnahmephase ist die zweite Phase und wird aktiviert, wenn sich ein Finger auf dem Fingerabdrucksensor befindet. Dabei erfasst der Geruchssensor den Geruch des Fingers und speichert die erhobenen Daten zur weiteren Verarbeitung. Wird der Finger wieder vom Sensor genommen aktiviert sich die Wiederherstellungsphase. Diese ist dafür, damit der Sensor wieder in den ursprünglichen Zustand zurück kehren kann. Dies dauerte nach den Experimenten von Baldisserra et al zwischen 10 bis 15 Sekunden. Anschließend werden die erhobenen Daten verarbeitet, um zwischen Fake und echtem Finger zu unterscheiden. Die Daten bilden eine Kurve in Abhängigkeit von der Zeit. Dies kann Abbildung 9 entnommen werden. Zur Fakeerkennung wird die Kurve mit einer vorher erfassten Templatekurve verglichen. Sind

diese annähernd gleich wird das Fingerbild als echt eingestuft. Für den Vergleich werden verschiedene Werte ermittelt. Dies

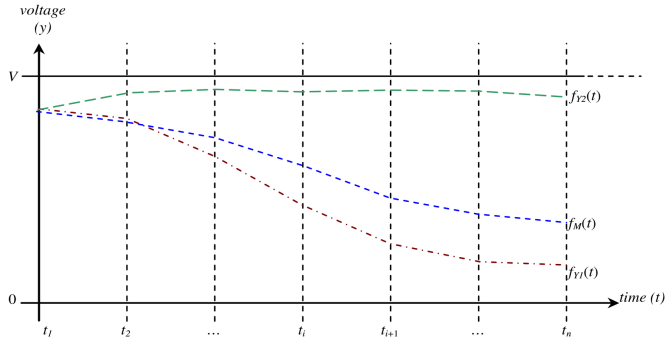


Abbildung 9. Kurvenverlauf verschiedenener Materialien (f_M:Nutzertemplate f_{Y1}:Gelantine f_{Y2}:Silikon) [16]

sind der Funktionstrend, die Fläche zwischen den beiden Funktionen, sowie die Korrelation der Funktionswerte. Diese Werte werden gewichtet und bilden addiert einen Scorewert. Ist dieser höher als eine festgelegter Schwellwert, wird der Finger als echt akzeptiert. In der Abbildung 9 kann erkannt werden, dass Gelatine (rot) sehr nach an das Template (blau), also einen echten Finger kommt. Silikon hingegen ist stark unterschiedlich des Templates (grün). Diesem verhalten, kann mit der Verwendung mehrerer verschiedener Geruchssensoren gegengesteuert werden. Verschiedene Sensoren reagieren unterschiedlich auf Gerüche. So ändern sich die Kurven bei verschiedenen Sensoren. In dem Paper wurde nur ein Sensor in den Experimenten betrachtet. Mehrere Sensoren sollen das Ergebnis verbessern. [16] Der Geruchsunterschied zwischen dem echten Finger und den Fakematerialien kann je nach verwendetem Sensor unterschiedliche Ergebnisse liefern. Im hier betrachteten Fall wurde Silikon sehr gut als falsch erkannt, Gelatine hingegen war sehr nah an einem echten Finger und kann so als echt erkannt werden. Weiterhin wurde kein Vorschlag unterbreitet, wie der zusätzliche Sensor in einen Fingerabdrucksensor integriert werden kann. Eventuell würde dies zu einem größeren Sensor führen und diese wären somit nicht mehr für z.B. Smartphones nutzbar. Vor allem unter der Erkenntnis das mehrere verschiedene Geruchssensoren verwendet werden müssen. Auch die lange Zeit der Erfassung und Wiederherstellung ist gerade im Bezug auf die Nutzerakzeptanz zu beachten. Können mehrere Geruchssensoren eindeutig die verschiedenen Materialien von einem echten Finger unterscheiden ist diese Verfahren zur Fakeerkennung geeignet. Dies muss jedoch noch weiter Untersucht werden.

3) Analysis of Fingerprint Pores for Vitality Detection: Als nächstes wird ein Software-basierendes Verfahren vorgestellt. Hierbei werden die Poren auf der Fingerhaut zur Fakeerkennung herangezogen. Zu sehen ist dies in Abbildung 10. Dabei sollen sich wesentlich weniger Poren auf einem Fake befinden, als auf einem echten Finger. Trotz ihrer größe von weniger als 1mm, sollen die Poren schon bei relativ geringen Auflösungen von ca 500 dpi erkennbar sein. Aufgrund ihrer Größe können die Poren nur schwer mit den verwendeten Materialien für Fakes nach gemacht werden.

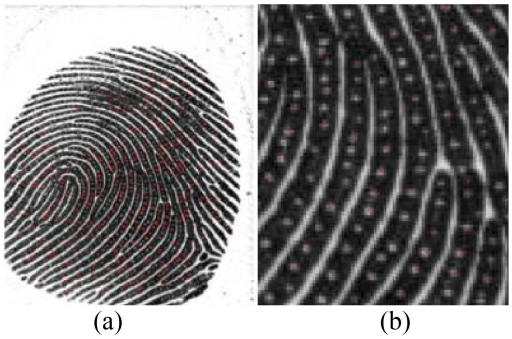


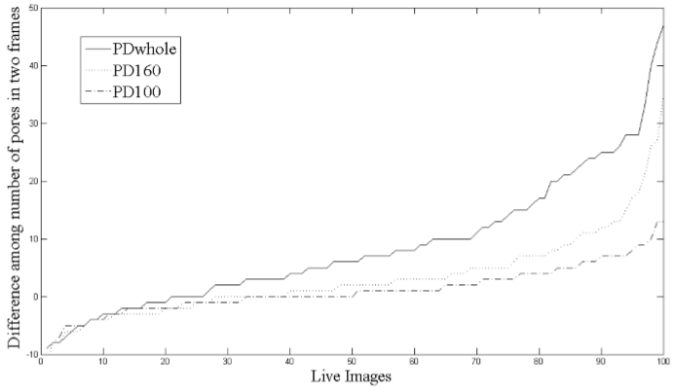
Abbildung 10. Fingeradruck (a) und dessen Vergrößerung mit erkennbaren Poren (b) [17]

In einem ersten Schritt werden zwei Bilder vom Fingerabduck genommen. Einmal zu Beginn und ein zweites Mal 5 Sekunden später. Anschließend werden die Poren mit einem eigens entwickelten Template Matching Algorithmus detektiert. Die Anzahl der Poren wird in drei Bereichen, um die Mitte des Fingerabdrucks gezählt. Diese sind die zwei Bereiche mit 100x100 und 160x160 Pixel, um die die Mitte und des gesamten Bildes. Anschließend werden die Differenzen dieser Werte zwischen dem 0 und 5 Sekunden Bild berechnet und gespeichert. Dies Daten können nun zur Fakeerkennung verwendet werden. Bei Fakes ist die Differenz oft negativ. Dies entsteht, da sehr wenige eher zufällig Poren bei der Fakeerzeugung vom Original übernommen werden oder durch Artefakte im Fakebild selbst. Weiterhin ist die Anzahl der Poren in einem echten Finger weitaus höher als bei einem Fake. Dies kann der Abbildung 11 entnommen werden. Hierbei ist auf die unterschiedlichen Wertet der y-Achse zu achten. [17]

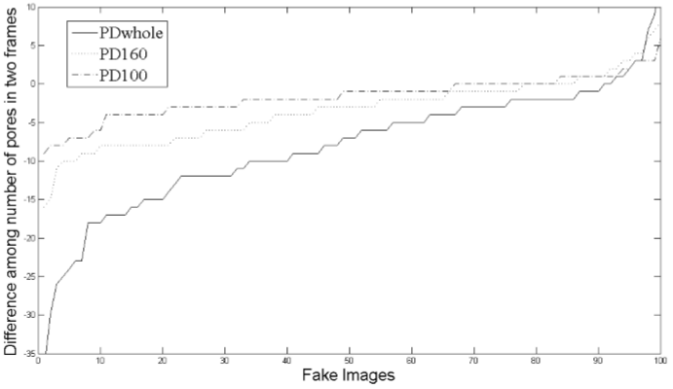
Die Autoren können zeigen, dass bei der Fakeerzeugung Informationen des Fingerabdrucks verloren gehen. In diesem Fall die Anzahl der Poren, da diese zu klein sind um zuverlässig übernommen zu werden. Jedoch wurde als Material lediglich Silikon in den Experimenten verwendet. Ob andere häufig verwendete Materialien ähnliche Ergebnisse liefert sollte untersucht werden, auch wenn dies wahrscheinlich ist. Andererseits können andere Materialien die nötigen Erfolge bieten. Ein großer Pluspunkt ist hier, dass die Erkennung der Poren schon bei relativ geringen Auflösungen Funktioniert und bei höheren Auflösungen vermutlich bessere Ergebnisse liefert.

4) Liveness Detection of Fingerprint based on Band-Selective Fourier Spectrum: Dieses Verfahren ist ein Software-basierendes Verfahren. Dabei wird das Fingerabdruckbild mit der Fourier Transformation analysiert. Dabei sollen erkennbare Unterschiede nach der Transormation zwischen Fake und einem echten Finger existieren.

Der Ablauf des Algorithmus ist in Abbildung 12 zusehen. Er besteht aus 6 Schritten. Dabei steht FFT für die Fast Fourier Transformation.



(a)



(b)

Abbildung 11. Porendifferenz zwischen echtem Finger (a) und Fake (b) [17]

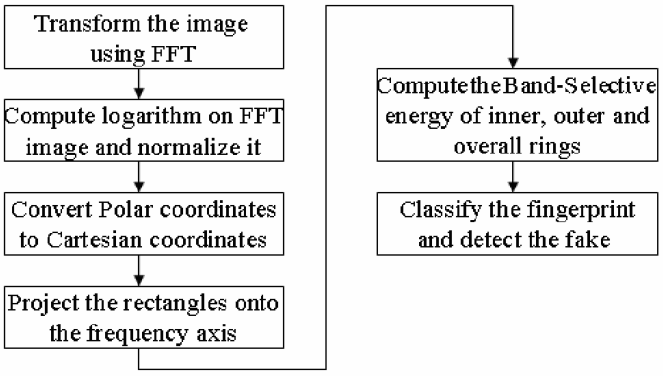


Abbildung 12. Ablauf des Algorithmus [14]

Im ersten Schritt wird das Fingerbild Mithilfe der FFT in seine Ortsfrequenz (spartial frequency) transformiert. Dabei entsteht ein innerer und äußerer Ring (Abbildung 13 links). Dieses Bild wird anschließend normalisiert, um große Abweichungen in den Werten zu vermeiden. Der innere Ring liegt dabei vom Zentrum zwischen Pixel 25 und 59. Der äußere Ring von Pixel 60 bis 100. Anschließend wird die spektral Energie der beiden Ringe und des gesamten Bildes bestimmt. Dazu wird einem Algorithmus von Daugman [18], welcher bei der Iris Erkennung angewendet wird auf den obere Halbkreis angewendet. Dadurch wird das Bild in das kartesische Koordinatensystem transformiert. Dies ist in Abbildung 13 zu sehen. Anschließend werden die einzelnen

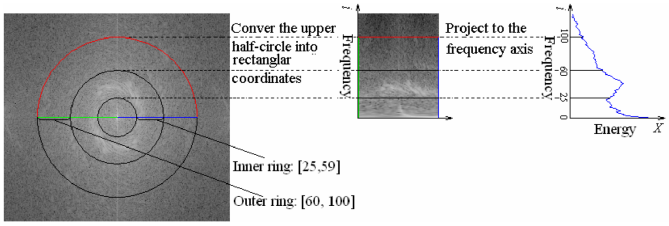


Abbildung 13. Transformationsablauf [14]

Ringenergien in ihren Intervallen zu einem Wert akkumuliert. Diese bilden Cluster, abhängig davon, ob es sich um einen Fake oder einen echten Finger handelt. Dies kann Abbildung 14 entnommen werden. Die Energiewerte sind bei Fakes unter-

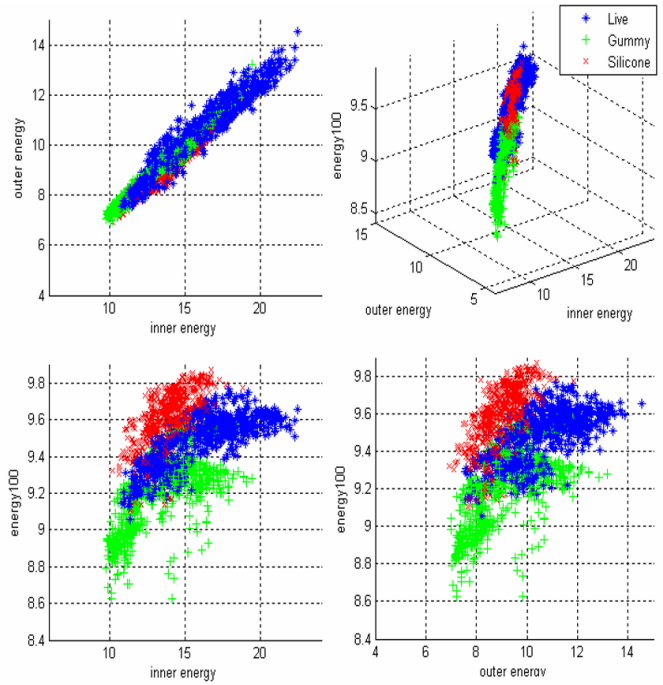


Abbildung 14. Verteilung der Daten in drei Dimensionen [14]

schiedlich zum echten Finger. Dies entsteht durch minimalste Unterschiede in der Oberfläche des Fakes im Vergleich zum Finger. Es kann kein perfektes Abbild eines Finger erzeugt werden. Auch die unterschiedlichen Materialien verändern die Energiewerte. [14] Es kann gezeigt werden, dass verschiedene Materialien unterschiedliche Energiewerte liefern. Somit kann dieses Verfahren zur erfolgreichen Erkennung von Fakes verwendung finden. jedoch wurden keine Angaben zum Berechnungsaufwand gemacht. Dieser könnte für einfache Systeme im Bereich IoT oder Smarthome zu groß ausfallen oder zu unakzeptablen Wartezeiten führen. Weiterhin wurden hier nur zwei Materialien aus denen Fakes erzeugt werden untersucht. Andere Materialien könnten Energiewerte nahe des

echten Fingers bekommen. Auch bei der Fakeerzeugung kann durch eine Verbesserung der Verfahren, eine Annäherung der Energiewerte an das Original erreichen. Dies benötigt weitere Untersuchungen, besonders im Bereich der Materialien.

5) Wavelet based fingerprint liveness detection: Auch das hier letzte vorgestellte Verfahren ist ein softwarebasierendes Verfahren. In diesem Verfahren wird mithilfe der Wavelet Analyse zur Noisereduktion [19] ein Fake erkannt. Dazu wird angenommen, dass ein Fake eine rauere Oberfläche als ein echter Finger hat. Diese Unterschiede entstehen durch das Erstellen des Fakes. Diese Unterschiede können Abbildung 15 entnommen werden. Hierbei wird die Raue der Oberfläche als weißes Rauschen interpretiert. Dieses wird anschließend Analysiert.

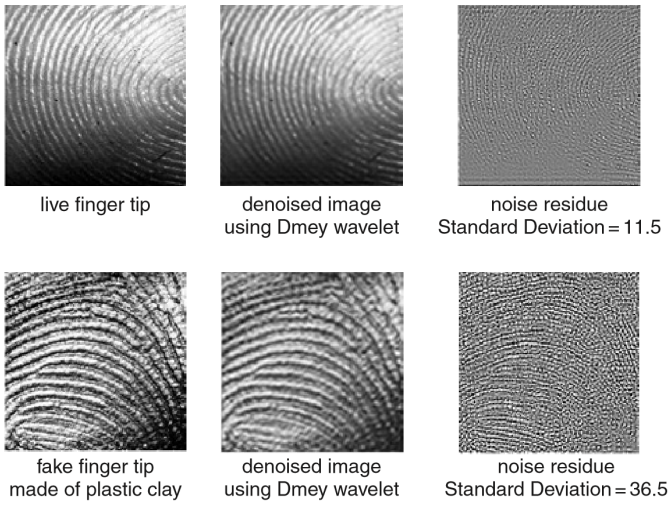


Abbildung 15. Lebenderkennung durch denoising [20]

Im ersten Schritt wird ein hochauflösendes Bild des Fingerabdrucks erzeugt. Dieses hat im Idealfall 1000 dpi oder mehr. Ansonsten ist die Informationsdichte zu gering. Anschließend wird in dem Fingerbild mithilfe der Wavelet Analyse das Rauschen bestimmt und aus dem Bild entfernt. (vgl. Abbildung 15 mitte) Anschließend wird der unterschied zwischen dem entrauschten und dem original Bild ermittelt. Dies ist das weiße Rauschen im Bild. In einem lebenden Finger ist das Rauschen sehr gering und gleichmäßig, während dies in einem Fake nicht der Fall ist. (vgl. Abbildung 15 rechts) Im letzten Schritt wird in dem Rauschbild noch die Standartabweichung ermittelt. Ist diese Höher als ein gewisser Schwellwert handelt es sich um einen Fake. In den Experimenten von Moon et al. konnte ein Schwellwert von 25 ermittelt werden. (Abbildung 16)

In den Experimenten mit Gelatine und Knetmasse kann klar zwischen Fake (obere Kurve) und echtem Finger (untere kurve)unterschieden werden. Jedoch wurden hier nicht Bilder eines Sensors, aus Ermangelung eines Sensor mit ausreichender Auflösung, sondern Bilder einer Kamera als Grundlage verwendet. [20]

Auch dieses Verfahren arbeitet mit dem Qualitätsunterschied zwischen Fake und lebendem Finger. Dieser kann jedoch durch

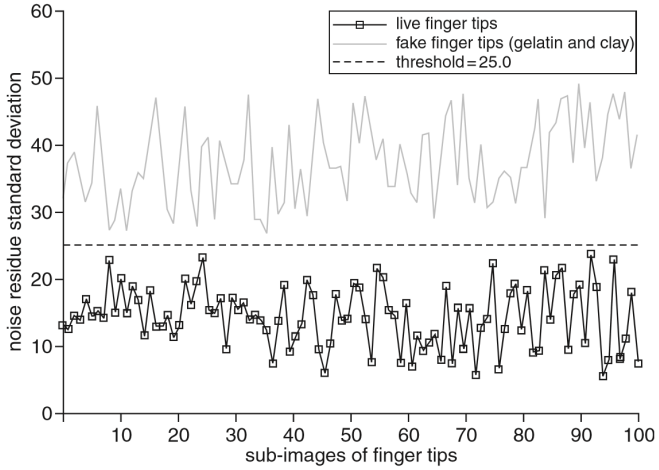


Abbildung 16. Experimentelle Ergebnisse [20]

bessere Verfahren verringert werden. Auch wurden hier nur zwei von vielen möglichen Materialien untersucht. Jedoch konnte anhand dieser zwei Materialien gezeigt werden, dass eine eindeutige Erkennung von Fakes möglich ist. Andere Materialien müssen noch untersucht werden. Auch der zusätzliche Berechnungsaufwand scheint gering zu sein, einzig das hochauflösende Fingerbilder benötigt werden, kann bei manchen Sensoren noch problematische sein. Jedoch sollte dies durch die fortschreitende Entwicklung der Sensoren kein Problem darstellen.

V. Fazit/Ausblick

In dieser Arbeit wurden verschiedenste Ansätze der Fake Detection vorgestellt und diskutiert. Einige Verfahren sind mit einfachsten Mitteln zu umgehen, während andere höhere Sicherheit bieten. Jedoch haben alle Verfahren verschiedene Schwächen. Manche sind noch nicht ausreichend erforscht, andere sind sehr Umständlich zu Implementieren oder haben hohe Anforderungen an die Sensoren und die Technik dahinter. Um ein wirklich sicheres System zu erzeugen müssen dabei mehrere Verfahren kombiniert werden, dies steigert jedoch die Kosten für ein solches System. Weiterhin kann dabei auch die Bedienbarkeit leiden. Gerade für alltägliche Systeme ist dies nicht akzeptabel. Eine teure Lösung würde kein Durchschnittsnutzer bezahlen und wenn die Authentifizierung zulange dauert, wird das System auch nicht vom Nutzer akzeptiert. Im Hochsicherheitsbereich können solche Einschränkungen akzeptabel sein. Aber auch hier können andere Möglichkeiten der Authentifizierung bessere Ergebnisse liefern. Die Authentifizierung mit dem Fingerabdruck kann jedoch eine weitere Hürde für Angreifer darstellen, um so den Aufwand für diesen zu erhöhen.

Für viele der vorgestellten Verfahren wurden verschiedene Einschränkungen in den Versuchen gemacht. Dies beinhaltet vor allem die Auswahl von meist wenigen Materialien zur Fakeerzeugung. Gerade hier gibt es eine viel zahl von Materialien mit verschiedensten Eigenschaften. Hier sollten

die Betrachteten Verfahren auf ihre Gesamtheit mit den Materialien getestet werden, um eine ausreichende härte dieser Verfahren zu gewährleisten. Auch andere Schwächen, wie die Hardwareanforderungen, welche in Zukunft eventuell nicht mehr so gravierend sind, müssen dazu herangezogen werden. Da heute oft noch ältere Scanner im Einsatz sind muss hier über eine eventuell teure Modernisierung nachgedacht werden, um diese Verfahren auch einsetzten zu können.

LITERATUR

[1] V. Nolde and L. Leger, Eds., *Biometrische Verfahren*. Deutscher Wirtschaftsdienst, 2002.

[2] *Chaos Computer Club hackt Apple TouchID*. Chaos Computer Club, 2013, http://www.ccc.de/de/updates/2013/ccc-breaks-apple-touchid [Zugegriffen am: 25.10.2016].

[3] T. Fiebig, J. Krissler, and R. Hänsch, "Security impact of high resolution smartphone cameras," in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/woot14/workshop-program/presentation/fiebig

[4] J. Krissler, *Ich sehe also bin ich... Du*. Chaos Computer Club, 2014, https://www.youtube.com/watch?v=vVivA0eoNGM [Zugegriffen am: 25.10.2016].

[5] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, ser. Springer Professional Computing. Springer London, 2009. [Online]. Available: https://books.google.de/books?id=1Wpx25D8qOwC

[6] M. Behrens and R. Roth, Eds., *Biometrische Identifikation*. Vieweg, 2001.

[7] BSI, *Fingerabdruckerkennung*. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Fingerabdruckerkennung_pdf.pdf?__blob=publicationFile [Zugegriffen am: 07.01.2017].

[8] R. E. O. Paderes, "A comparative review of biometric security systems," in *2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)*. IEEE, 2015, pp. 8–11.

[9] Bundesamt für Sicherheit in der Informationstechnik, *Einführung in die technische Grundlagen der biometrischen Authentisierung*, 2005, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/ Technische_Grundlagen_pdf.pdf?__blob=publicationFile [Zugegriffen am: 07.01.2017].

[10] J. Blommé, "Evaluation of biometric security systems against artificial fingers," 2003.

[11] M. Drahansk, W. Funk *et al.*, "Liveness detection based on fine movements of the fingertip surface," in *2006 IEEE Information Assurance Workshop*. IEEE, 2006, pp. 42–47.

[12] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," in *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications on Smart Card Research and Advanced Applications*. Norwell, MA, USA: Kluwer Academic Publishers, 2001, pp. 289–303. [Online]. Available: http://dl.acm.org/citation.cfm?id=366214.366298

[13] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Electronic Imaging 2002*. International Society for Optics and Photonics, 2002, pp. 275–289.

[14] C. Jin, H. Kim, and S. Elliott, "Liveness detection of fingerprint based on band-selective fourier spectrum," in *International Conference on Information Security and Cryptology*. Springer, 2007, pp. 168–179.

[15] D. TanishaAggarwal and C. K. Verma, "Fake fingerprint detection methods."

[16] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *International Conference on Biometrics*. Springer, 2006, pp. 265–272.

[17] G. L. Marcialis, F. Roli, and A. Tidu, "Analysis of fingerprint pores for vitality detection," in *Pattern Recognition (ICPR), 2010 20th International Conference on*. IEEE, 2010, pp. 1289–1292.

[18] J. Daugman, "How iris recognition works," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 21–30, 2004.

[19] W.-S. Lu, "Wavelet approaches to still image denoising," in *Signals, Systems & Computers, 1997. Conference Record of the Thirty-First Asilomar Conference on*, vol. 2. IEEE, 1997, pp. 1705–1709.

[20] Y. S. Moon, J. Chen, K. Chan, K. So, and K. Woo, "Wavelet based fingerprint liveness detection," *Electronics Letters*, vol. 41, no. 20, p. 1, 2005.