Fingerabdrücke Hacken

im Seminar

Automatisierte Fingerabdruckidentifizierung praktisch hinterfragen

Andre Schmelzer & Christian Steinfeldt

Institut für Informatik

2. November 2012

Überblick

1 – FakeFinger

Abbildung:
https://erdgeist.org/archive/46halbe/schaeuble-attrappe.png

Herstellung:

Realer Finger
↓
Schablone
↓
FakeFinger

- Eine detaillierte Schablone ist essentiell!
- In der Praxis hat sich die Nachbearbeitung eines fotografierten Abrucks als sehr zeitaufwändig und mühselig erwiesen.

1 – Schablonen

Das Negativ kann man jetzt

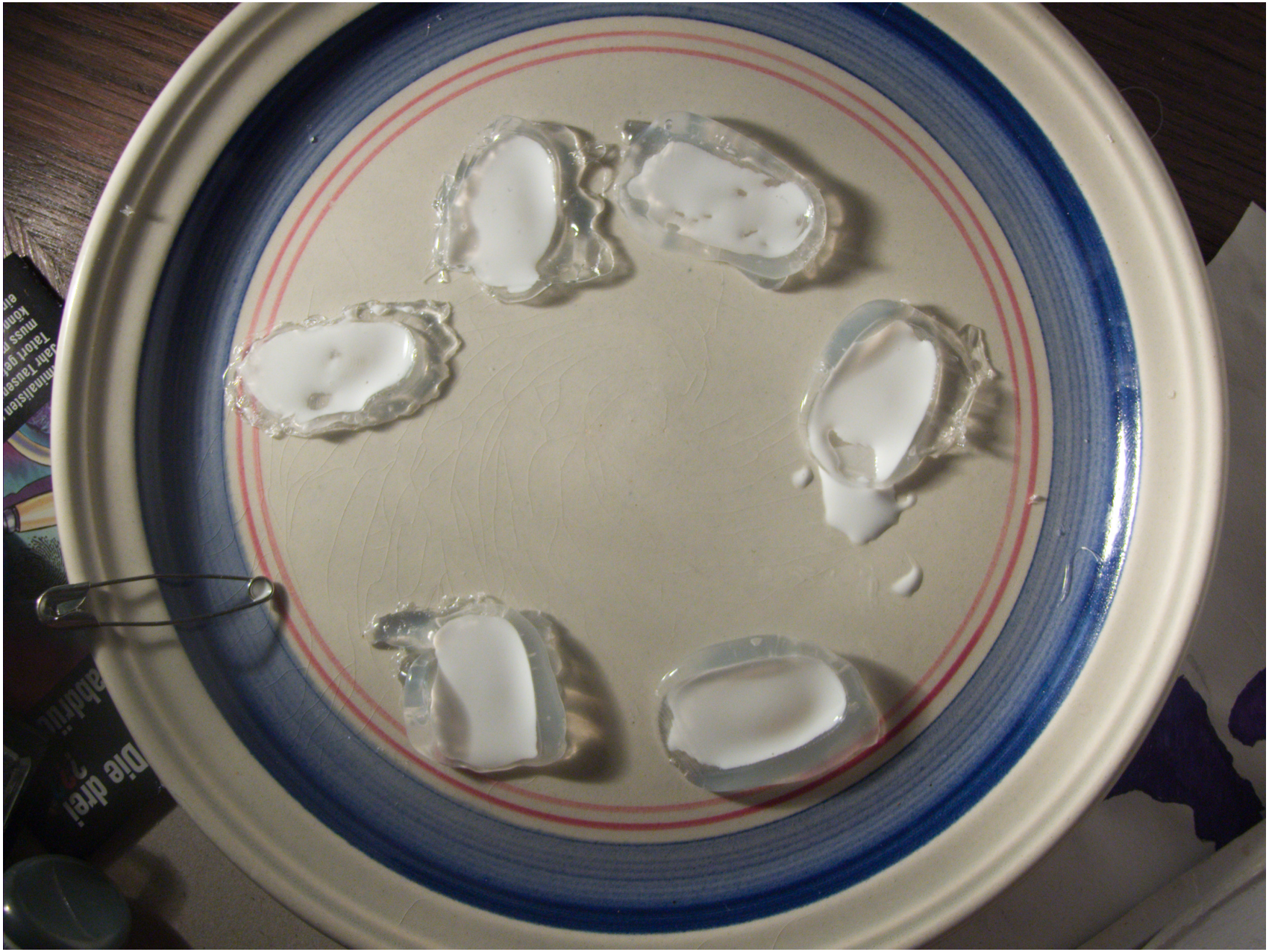
- direkt auf Folie drucken; die Wölbungen der Farbe reichen als Papillartäler aus.
- in ein Platine einätzen. Diese sind die robustesten aller probierten Methoden.

Alternativ kann man auch Knete, Heißkleber oder eine ähnliche Substanz benutzen und direkt verformen. Je nach Material ist die Schablone hier aber nach kürzerer Zeit abgebraucht.

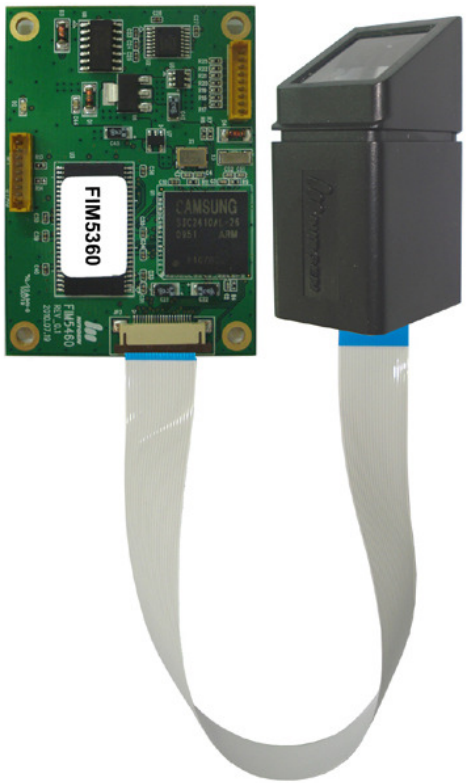
Hat man eine Form, die das Papillargewölbe gut wiedergibt kann man sich an den falschen Finger machen.

Holzleim Je dünner aufgetrgen, desto flexibler. Plastik.

Geliermittel Organisch. Trocknet schnell aus.



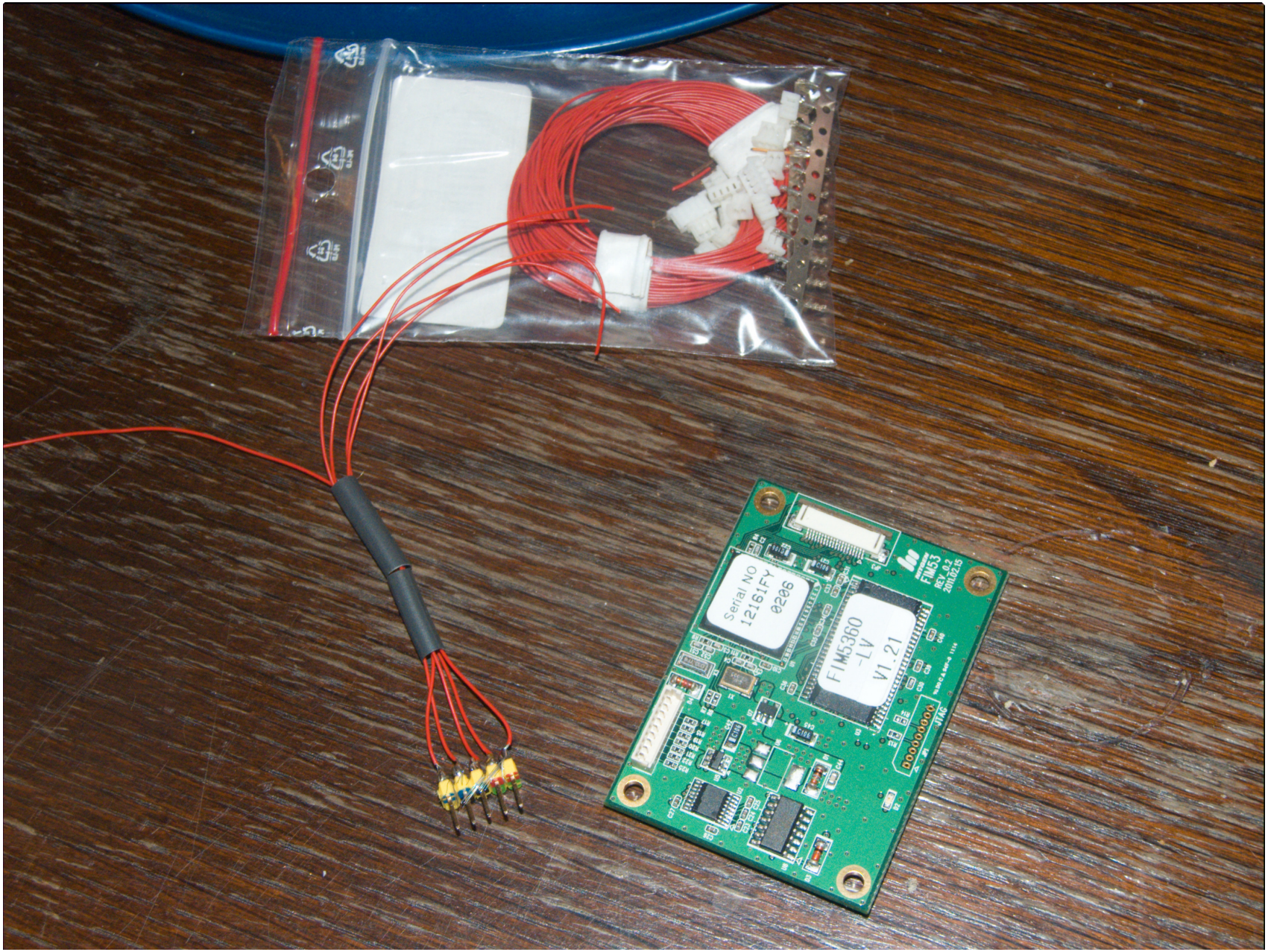
2 – Sensoren – Nitgen FIM5360-LV



Sensortyp:	Optisch
Sensorbereich:	15,0 mm x 18,5 mm
Auflösung:	500 DPI
Bildgröße:	260 x 300

Probleme:

- Kabel zum Arduino nicht erhältlich
- ungenügende Informationen vom Hersteller
- keine Möglichkeit zur Kommunikation


Serial NO
12161FY
0206
FIM5360
-LV
V1.21
FIM53
REV A2
2011/02/15

2 – Sensoren – digitalPersona U.are.U4000

Sensortyp:	Optical
Sensorbereich:	14.6mm x 18.1mm
Auflösung:	512 DPI
Bilddaten:	8-Bit Graustufen

Features: (Herstellerangaben)

- Excellent image quality
- Encrypted image data
- Counterfeit image rejection
- Works well with dry, moist or rough fingerprints

2 – Sensoren – digitalPersona U.are.U4000

Features (really)

- Excellent image quality – Hängt sehr vom Scan ab. Bei unseren Tests traten auch viele Fehler und Nichterkennungen auf.
- Encrypted image data – Nein. Die digitalPersona Software hat die Bilder verschlüsselt gespeichert. Über USB wird unverschlüsselt übertragen.
- Counterfeit image rejection – Ist durch das kleine *Checksummen*-Bild auch beim richtigen Finger unter Umständen ein Problem.
- Ist ein Spielzeug; kein Securityfeature

3 – Test

Mit den Fingern haben wir folgende Testszenarien:

	echt	Leim	Geliermittel
echt			
Leim			
Geliermittel			

Legende: Enrolled, Identify

3 – Test

Abbildung: links: echter Finger, mitte: Agartinefinger, rechts: Holzleimfinger

3 – Test

- Es ist nur in Einzelfällen möglich, den Scanner zu täuschen.
- Zwischen den Attrapen ist die Erkennungsrate höher.
- Ein immer gefälschter Fingerabdruck funktioniert!

4 – Replay-Attacken

Die fehlende Verschlüsselung erlaubt allerdings Replay-Attacken.

- Installiere einen USB-Sniffer auf dem Ziel. Suche in dem Datenstrom nach der Sequenz mit einem passenden Bild. Simuliere mit einem andern Rechner über einen Adapter eine Authentifiziereung mit dem gefundenen Bild.
- Mit einer passenden Schablone kann man sofort die Authetifizierung simulieren.

5 – Referenzen

- Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino, http://cryptome.org/gummy.htm, 2002
- H4CK1NG B10M37RiC5::fingerprints, Antti Kaseva, Antti Stén, http://stdot.com/pub/ffs/index.html, 2003
- libfprint, Open-Source Fingerprint Library, http://www.freedesktop.org/wiki/Software/fprint/libfprint
- Mikko Kiviharju, Hacking fingerprint scanners, http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Kiviharju/bh-eu-06-kiviarju.pdf, 2006