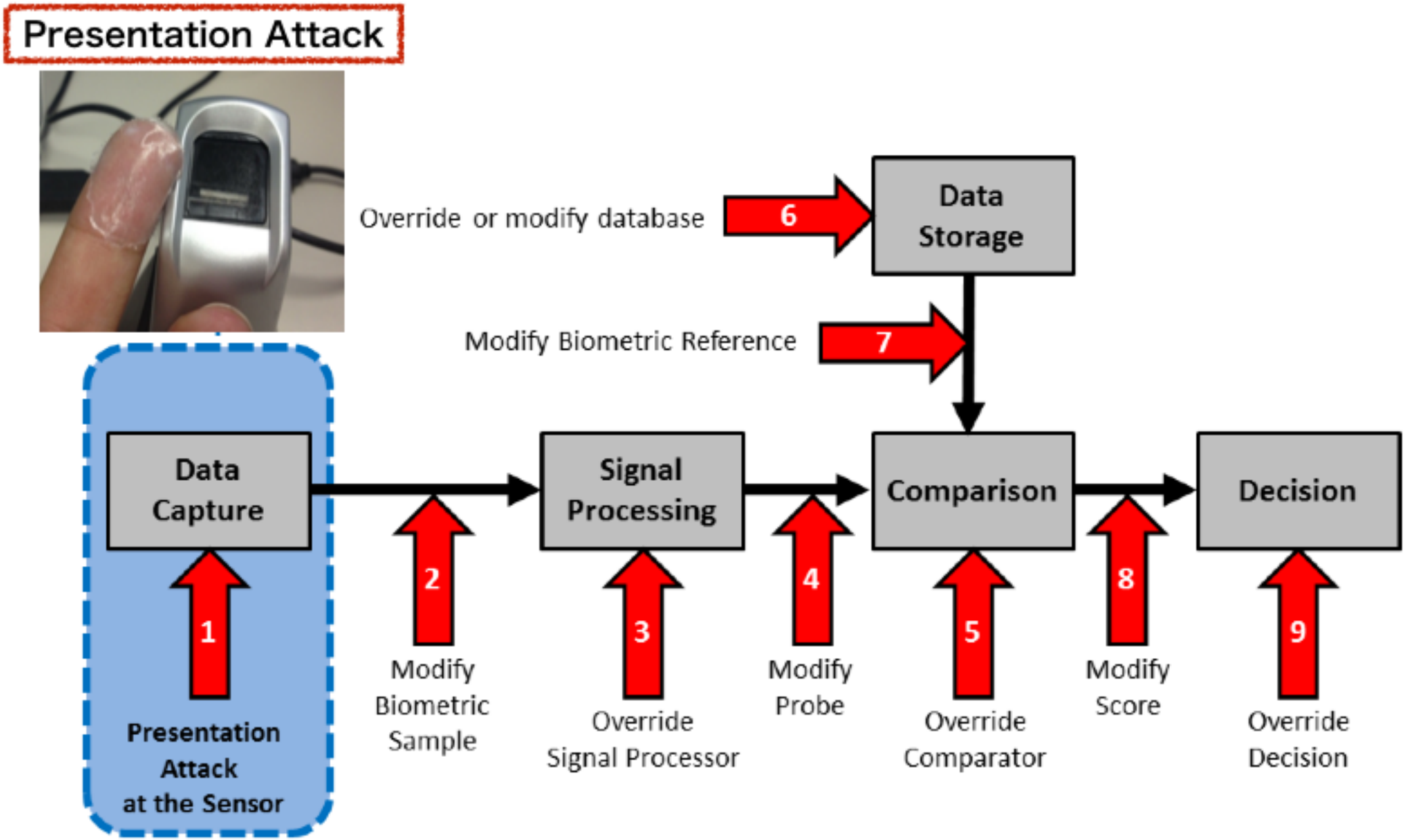
第2回セキュアシステムシンポジウム

バイオメトリクス認証のセキュリティ

産業技術総合研究所
○大塚 玲, 大木哲史

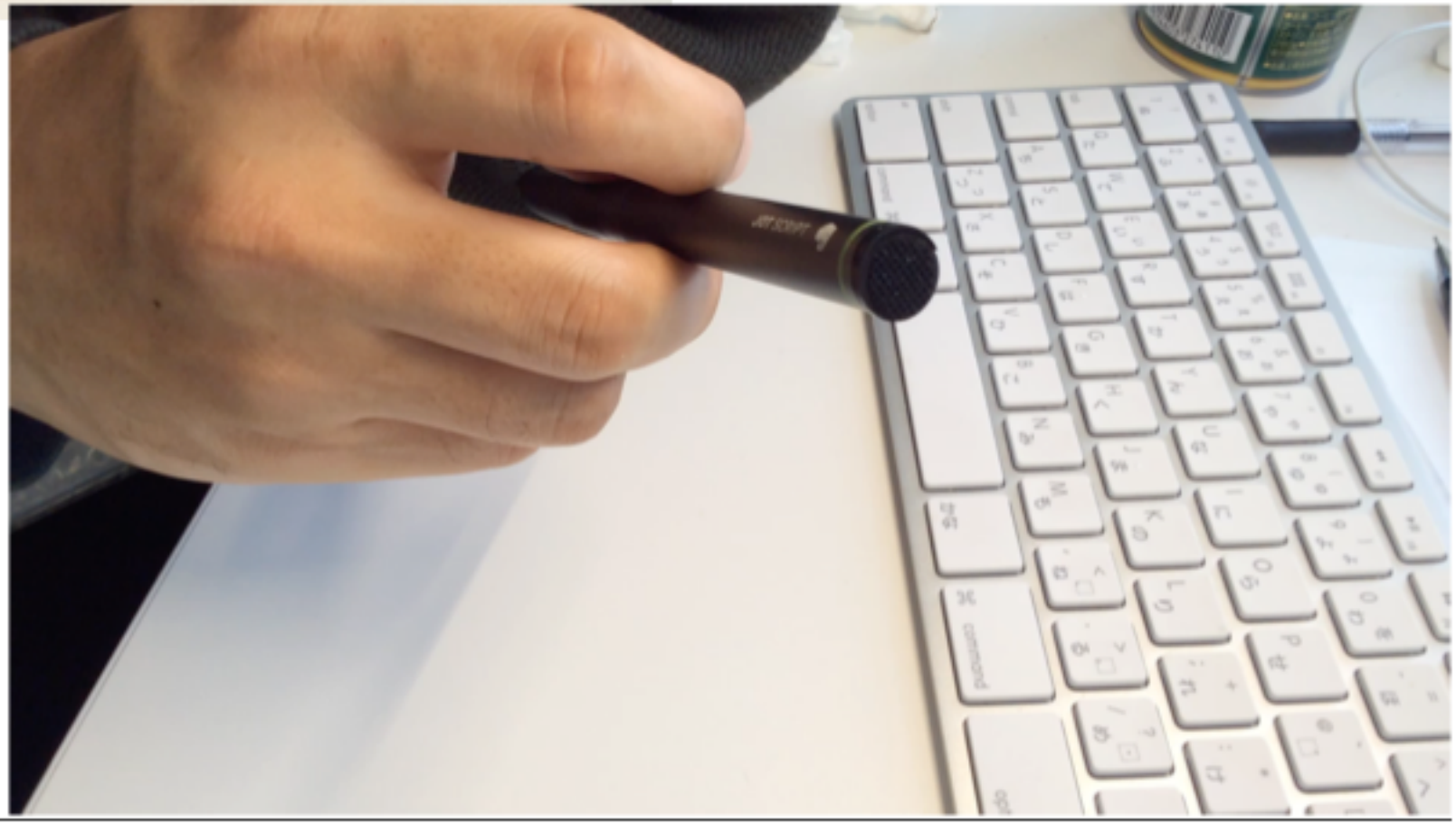
生体認証システムの攻撃ポイント



指紋認証システムに対するPresentation Attack例

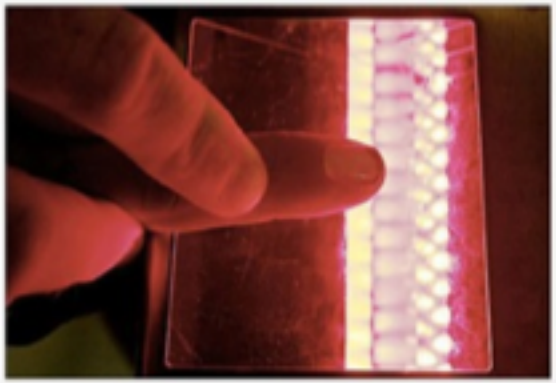
導電シリコン

レーザー加工装置



なりすまし攻撃の事例(1)

Million Dollar Border Security Machines Fooled with Ten Cent Tape



So much for biometrics and immigr
security: A South Korean woman
managed to fool a million-dollar
fingerprint reading machine in Jap
border controls using a simple piec
tape stuck to her fingers.

It happened at Tokyo airport. The
woman has repeatedly entered Jap
using the same trick without anybo
noticing. Japanese officials say that they suspect many others have been doing the
things, demonstrating that the biometric systems they installed in 30 airports in 20
the tune of $45 million-are completely useless. The woman was deported in July 2
for illegally staying in Japan as a bar hostess in Nagano, but she entered again wit

http://gizmodo.com/5122259/million-dollar-border-security-machines-fooled-with-ten-cent-tape

2009年1月、テープで指紋を変えることで日本への入国審査を通過したとして外国人女性2名が逮捕された。

なりすまし攻撃の事例(2)

Doctor caught red-fingered, buddy-punching absent co-workers in Brazilian hospital

By Adam Vrankulj

Like 0 Tweet 4

March 13, 2013 - A Brazilian doctor has been charged with fraud, after being caught using silicone fingers to clock absent co-workers in, spoofing the biometric workforce management solution installed at a hospital outside of Sao Paulo.

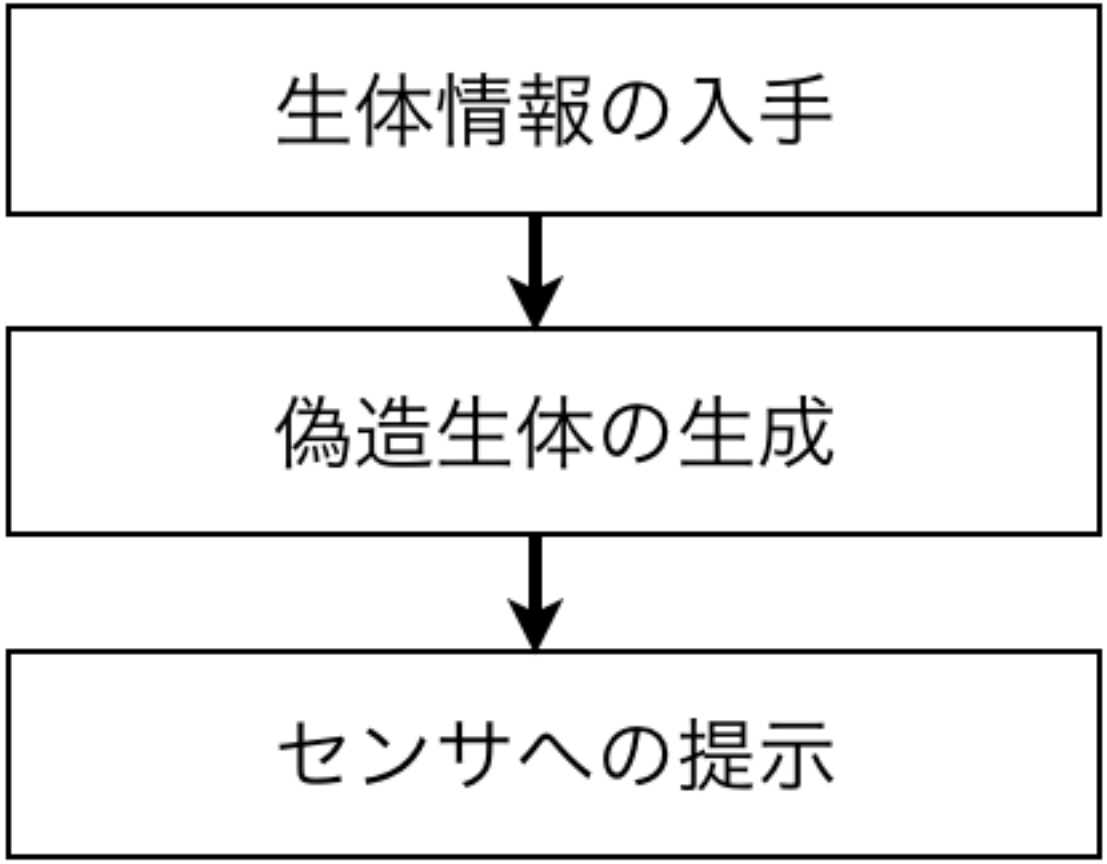
Making headlines around the world this morning, the doctor, 29-year-old Thaune Nunes Ferreira has been arrested, and according to a report in Folha De S.Paulo, Ferreira told police she had been using the silicon fingers as she had been coerced by her employer to do so, as she faced losing her job.

Following suspicion that some sort of fraud had been occurring, cameras were installed near the biometric time clock and eventually caught the doctor red-handed.

http://www.biometricupdate.com/201303/doctor-caught-red-fingered-buddy-punching-absent-co-workers-in-brazilian-hospital

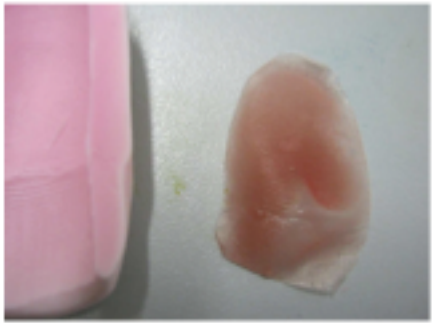
2013年3月、ブラジル・サンパウロ近郊の病院に勤務する医師が、シリコンで偽造した指を使うことで指紋認証をすり抜け、同僚の勤怠記録を偽装していることがわかった。

Presentation Attack の手順



生体情報の入手

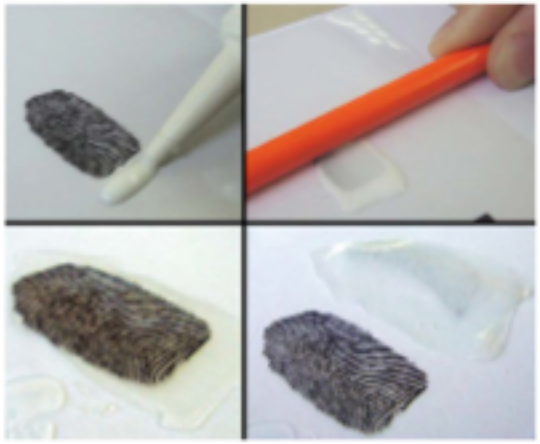
協力的なりすまし(Cooperative)



攻撃者は攻撃対象者の生体サンプルを直接入手し、そこから偽造物を作成することができる。

Ref) http://prag.diee.unica.it/fldc-tset/LivDet_2013_slides.pdf

残留（Latent）



遺留物(**Latent**)から偽造物の元となる生体特徴を入手することができる。

例）指紋，DNA

※虹彩や静脈は遺留しにくい．
但し，虹彩は高解像度デジタル写真等に記録されやすい．

Springer Science+ Business Media LLC, “Encyclopedia of Biometrics: Fake Fingerprint,” 2009

入手した生体情報を利用した偽造生体の作成

生体の模倣（造形）	Cast(two step mold/cast process)	1.型取り(Molding)- 生体特徴の三次元表現	人間からキャプチャされた顔型、医療用素材で作られた指の型、プリント基盤に印刷された指紋など
		2.成型(Casting) - 型からの再生成	演劇用マスク、粘土やゼラチン、シリコンなどの素材で作った偽造指など
	Direct Rendering	二次元プリント	虹彩や顔、指紋、静脈パターンなどを透過性のある紙にプリントしたもの
		三次元プリント	模様が印刷されたコンタクトレンズ、静脈の模様が印刷された人工の手ものなど
		エッチング	金属に指紋をエッチング加工したもの
		ペインティング - 人工器官に描かれた模様や色	人工の目に虹彩の模様を描かれたものや，人工の手に静脈の模様を描いたもの
	Mask	生体特徴の偽造物による変更や秘匿	指に接着剤をつけたもの、化粧、取り外し可能な移植組織、不透明レンズ、スキーのマスクなど
生体の模倣（動画／音声）	Computing device	ラップトップやタブレットに表示された画像やビデオ	顔・虹彩の画像や動画
	Time series player	時間軸で記録された情報	音声の録音，デジタルタブレットを用いた署名の登録，脳波の登録など
生体情報の人工合成		合成生体特徴の作成	指紋，顔，音声の合成，ウルフ合成サンプルや三次元顔の彫像など

生体の模倣（造形） (1) Cast

Cast の例

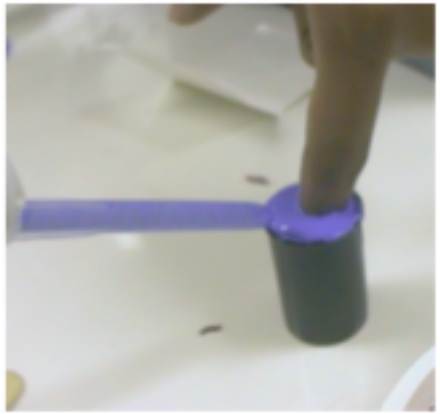
型取り(Molding)と成形(Casting)の2つのプロセスから構成される

1. 型取り

入手した生体特徴を元に型を作成する

2. 成型

型にシリコンやゼラチンを流し込んで偽造指を作成




生体の模倣（造形） (2) Direct Rendering

Direct Rendering

二次元プリント

三次元プリント

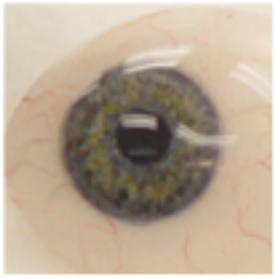
Nesli, et al, IEEE International Conference of the Biometrics Special Interest Group(BIOSIG), 2013.

エッチング

左図：プリント基板に対して指紋画像をエッチング処理したもの

http://www.atmarkit.co.jp/fsecurity/column/ueno/48.html

ペインティング



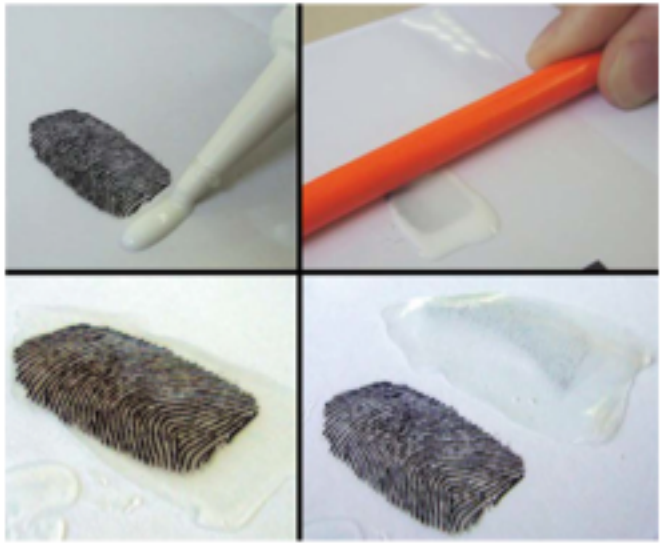
左図：義眼に対し半透過レイヤを30枚重ねて虹彩模様を作成したもの

Lefohn, et al, IEEE Computer Graphics & Applications article, 2003.

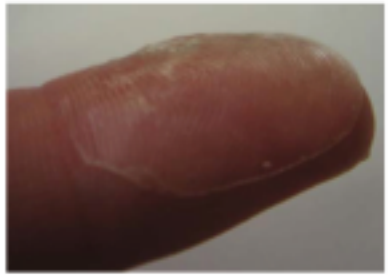
生体の模倣（造形） (3) Mask

Mask

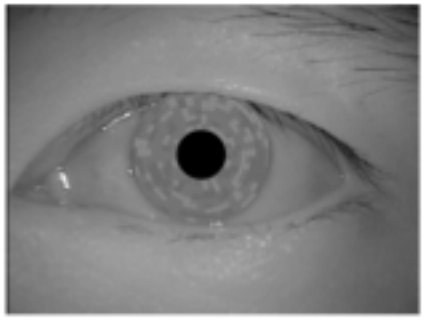
生体特徴の偽造物による変更や秘匿



例) 木工用ボンドによる
偽造指紋の作成



Source) Chaos Computer Club



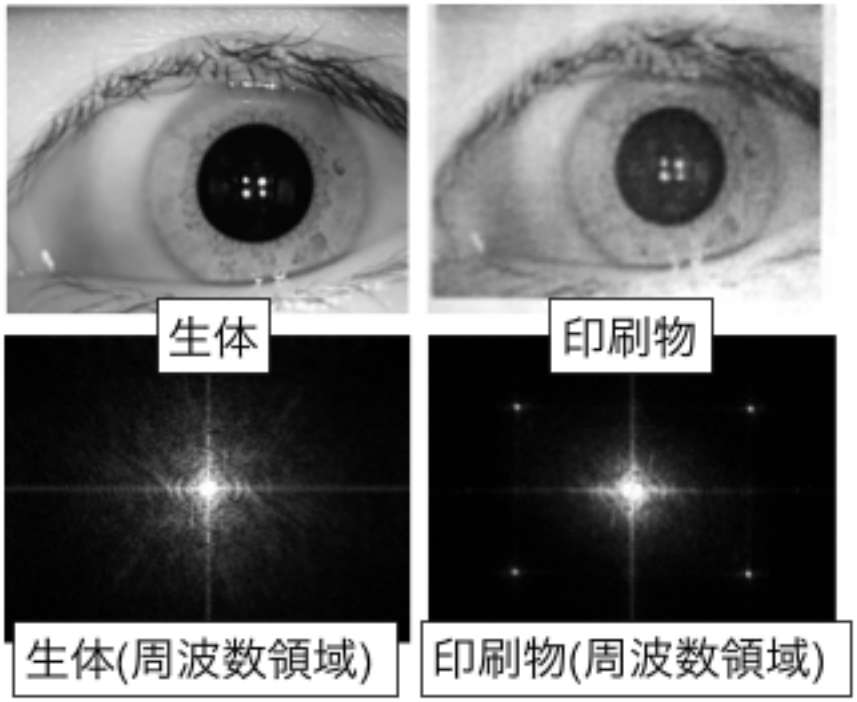
Nesli, et al, IEEE International Conference of the Biometrics Special Interest Group(BIOSIG), 2013.

Presentation Attack Detectionの分類
(1) 生体固有の特徴

生体のみが持つ固有の特徴を用いて偽造物を判定する方式

例)
- 汗腺が存在するか
- 皮膚の電気抵抗
- 隆線構造
- 光の反射や吸収

周波数領域による印刷物判定



X. He, et. al, Advances in Biometrics, 2009.

Presentation Attack Detectionの分類
(1) 生体固有の特徴

テクスチャベース

対象の外観を測定して検知に利用

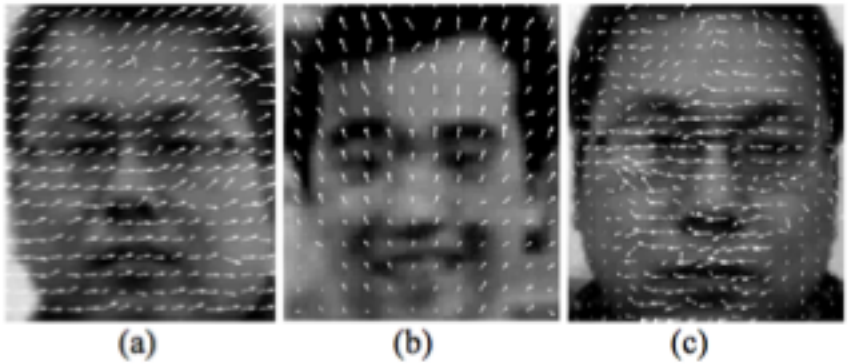
Maatta, et.al, IJCB2011.

図：LBP画像空間における生体と印刷物の違い
左(生体)と右(印刷物)の顔画像は非常に似通っているが、LBP画像空間においては違いが顕著となる

モーションベース

対象の動きを測定して検知に利用

Bao, et.al, IASP2009.



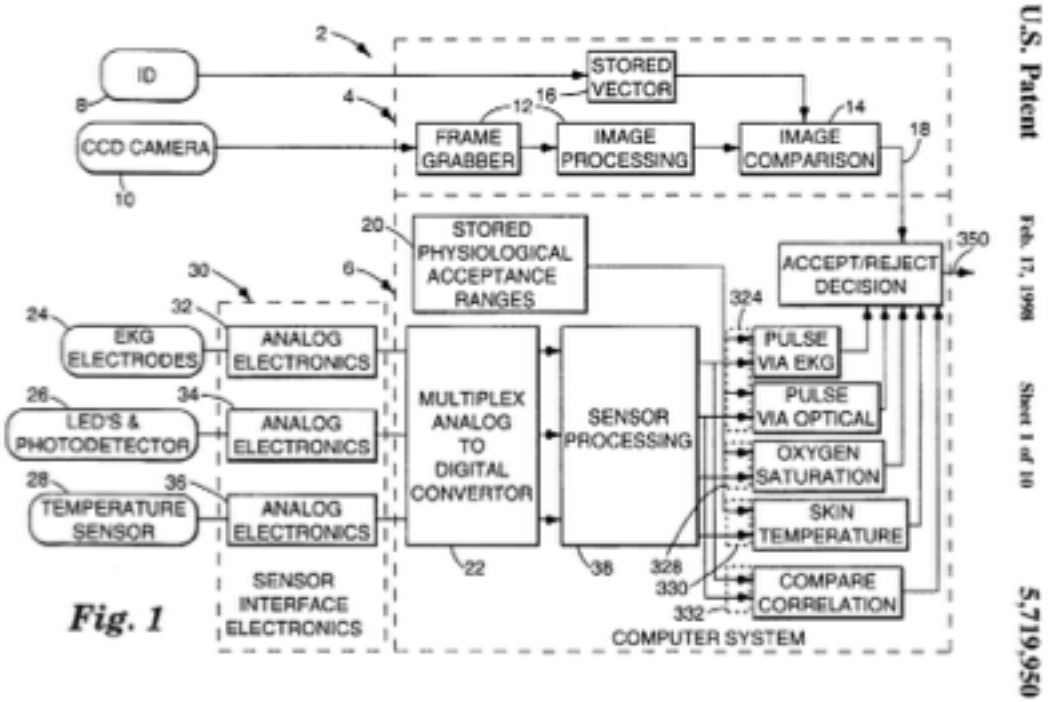
図：オプティカルフローによる動きの違いの可視化
(a)印刷物を手で持って提示したもの、(b)は同じものを固定して提示したもの、(c)は実際に生体を提示したもの。他2つと比較して複雑な動きをしていることがわかる

両者を組み合わせる(統合)することで更に高精度な検知も可能

Presentation Attack Detectionの分類
(2) 生体の無意識動作

血圧，血流，脳波，心電図波形，照明の変化によらない瞳孔の収縮など

図：ECGと指紋リーダーの組み合わせ



図： 脈拍・心電図・対応の組み合わせによる検知(US Patent)

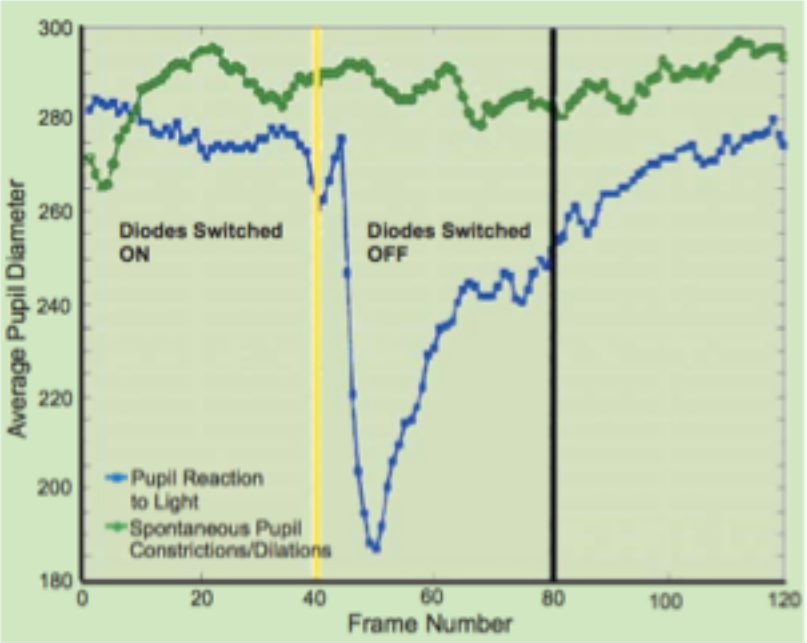
Ref 1) C. X. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos, "Securing handheld devices and fingerprint readers with ECG biometrics," presented at the Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on, 2012, pp. 150–155.
Ref 2) D. Osten, H.M Carim, M.R Arneson, and B.L Blan, "Biometric, personal authentication system," Minnesota Mining and Manufacturing Company, US Patent #5,719,950, Feb. 1998.

Presentation Attack Detectionの分類
(3) チャレンジレスポンス型PAD

無意識的応答（反射）

自然あるいは無意識な本人によってコントロールできない反応を測定することで生体検知を行う

- 光による瞳孔の収縮
- 膝蓋腱反射



図：照明をあてた際の瞳孔直径の変化
スイッチをオンにした瞬間瞳孔が収縮している

Pacut, A.; Czajka, A., "Aliveness Detection for IRIS Biometrics," *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International* , vol., no., pp.122,129, Oct. 2006

意識的応答

人間の認知と意識的な行動に基づく反応を測定することで生体検知を行う

- 顔認証における瞬き検知
- 話者照合におけるキーワード発話

図：目を閉じた瞬間を検知する

The Machine Perception Toolbox, http://mplab.ucsd.edu/grants/project1/free-software/mptwebsite/introduction.html

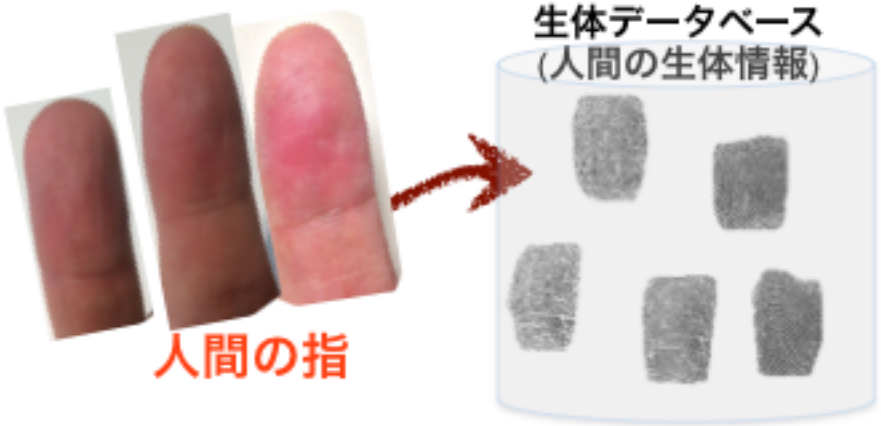
Presentation Attackの大分類

PAD機能 (Presentation Attack Detection)	本人の生体情報 あり	本人の生体情報 なし
完全 ※偽造生体を完全に受理しないPAD機能を実現する必要があり極めて困難	他人受入率(FAR)-安全 (強要による本人の生体提示を除く)	
不完全	人工物による生体の模倣	ウルフ攻撃 (提案)

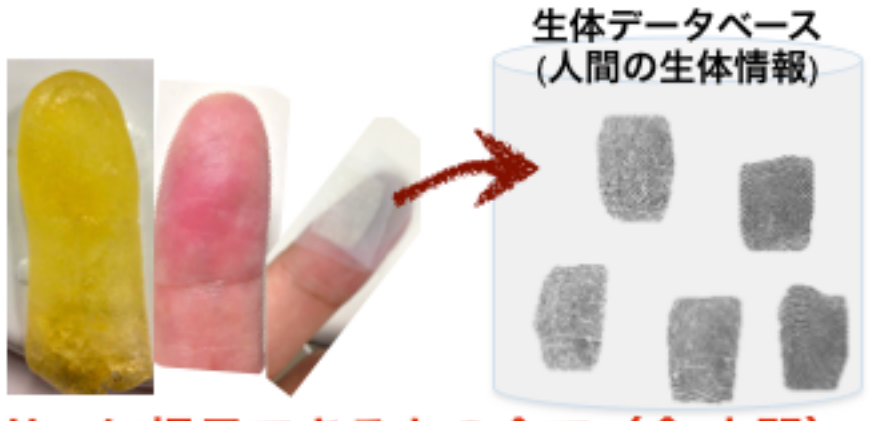
ウルフ攻撃

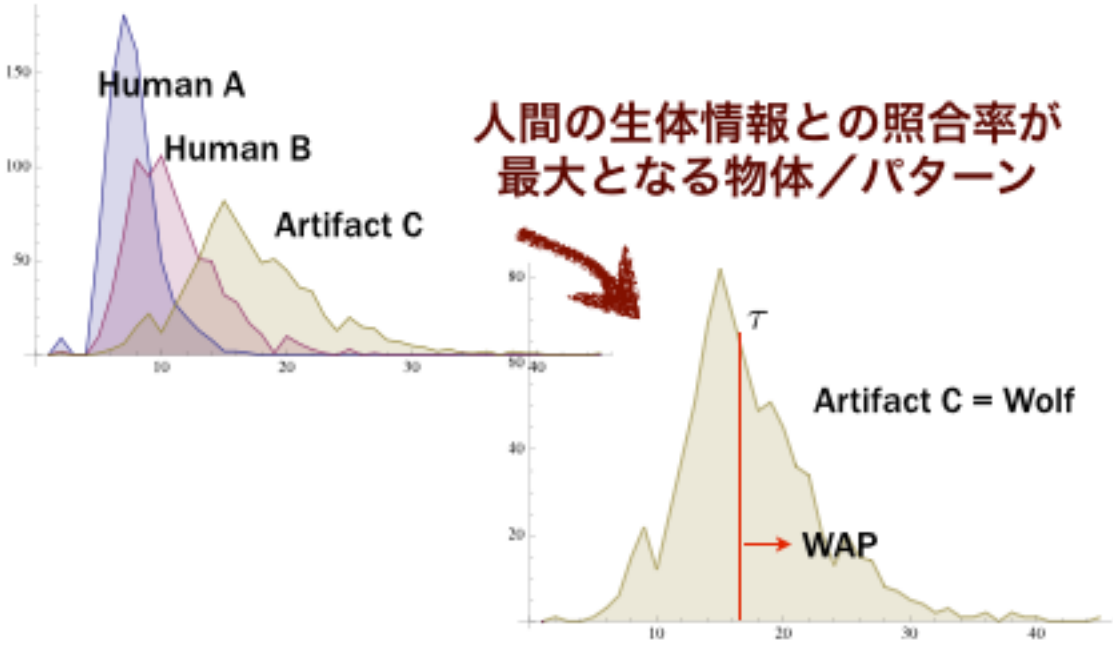
M.Une, A.Otsuka and H.Imai, "Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems," ICB2007, LNCS 4642, pp. 396-406, 2007.

FAR: 他人受入率



WAP: ウルフ攻撃確率





提案: ウルフ攻撃確率（最大のなりすまし成功率）で生体認証システムの安全性評価

デ モ

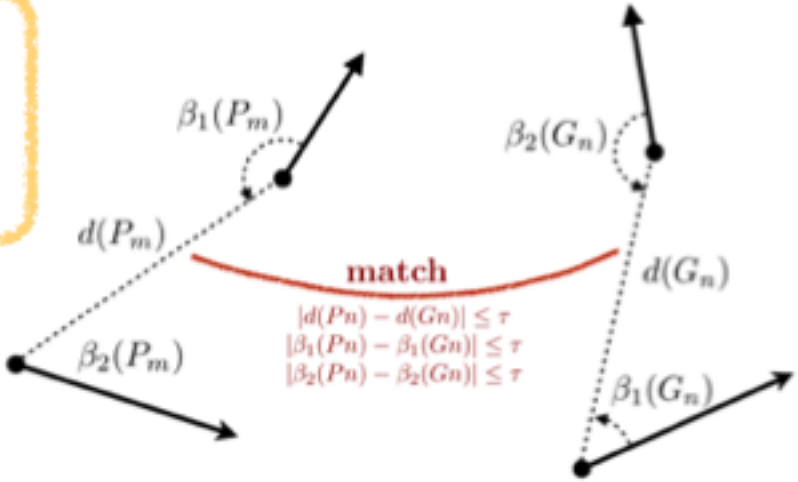
実験によるウルフ攻撃の成功確率 2014.3時点

モダリティ	攻撃対象アルゴリズム (論文等)	ウルフ攻撃 成功確率 (これまでの実験で得られた最大値)
指紋認証	C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wil- son, R. M. McCabe, S. Janet, and K. Ko, “User 's Guide to NIST Biometric Image Software (NBIS), "National Institute of Standards and Technology , " http:// fingerprint.nist.gov/NFIS/ , 2007.	42.4%
話者認証	Y. Yamazaki, Y. Fujita, and N. Komatsu, “CELP- based speaker verification: an evaluation under noisy conditions," ICARCV 2004 8th Control, Automa-tion, Robotics and Vision Conference, 2004., vol.1,pp. 408-412, IEEE, 2004.	50%
静脈認証	N. Miura, A. Nagasaka, T. Miyatake, “Extraction of finger-vein patterns using maximum curvature points in image profiles," IEICE TRANSACTIONS on Information and Systems, 90(8), 1185-1194.	92.5%
虹彩認証	J. Daugman, “How Iris Recognition Works,"IEEE Circuits and Systems for Video Technology, Vol.14, pp21-30, 2004.	42.6%

指紋認証に対するウルフ攻撃（例）

Properties of Bozorth3 (NIST)

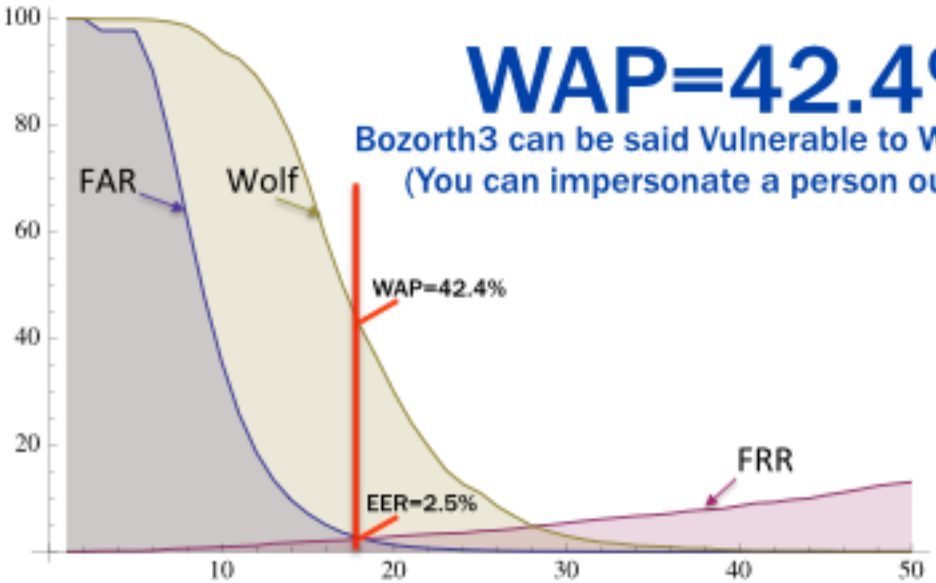
(1) Minutiae-relation matching algorithm
(2) Only up to 200 minutiae accepted
(3) Severer distance allowance of minutiae (within 15 pixels)
(4) Severer direction allowance within 11.25 degree



Our Approach:

(1) Arrange 200 minutiae s.t. area (circle of radius 15) of each minutia is disjoint and packed together, and
(2) Direction of each minutiae is determined as the most probable direction at each area around minutia, computed from Human distribution.

Artificial Fingerprint with 14x14=196 Minutiae



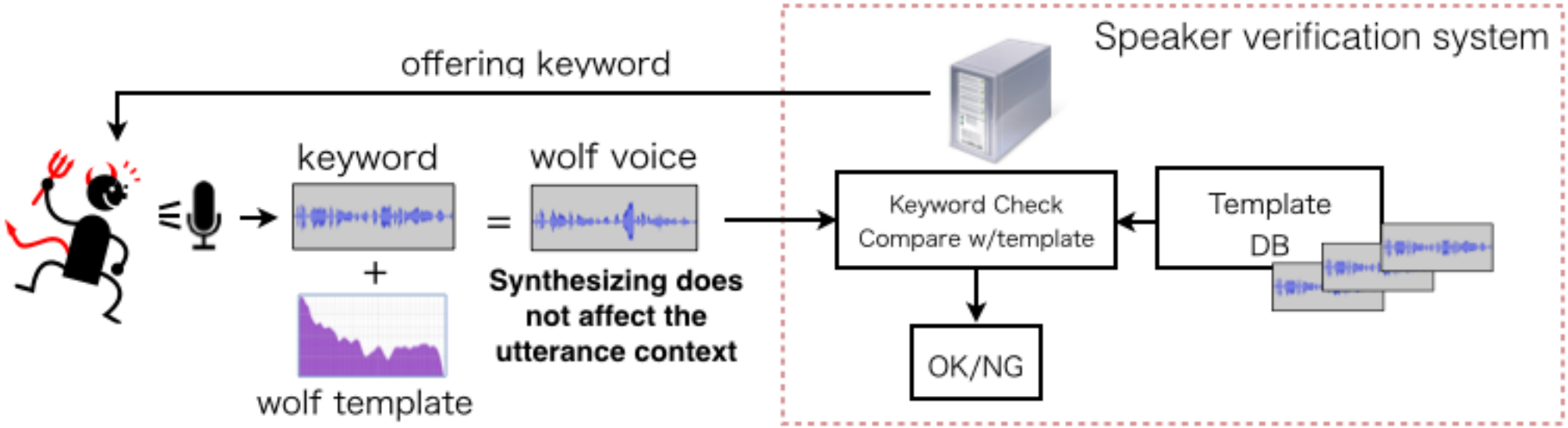
WAP=42.4%

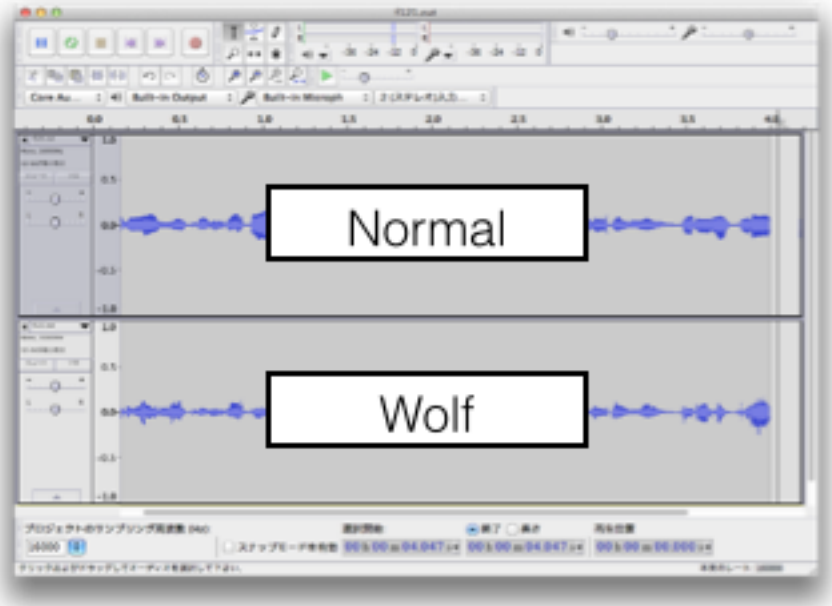
Bozorth3 can be said Vulnerable to Wolf Attack
(You can impersonate a person out of 3!)

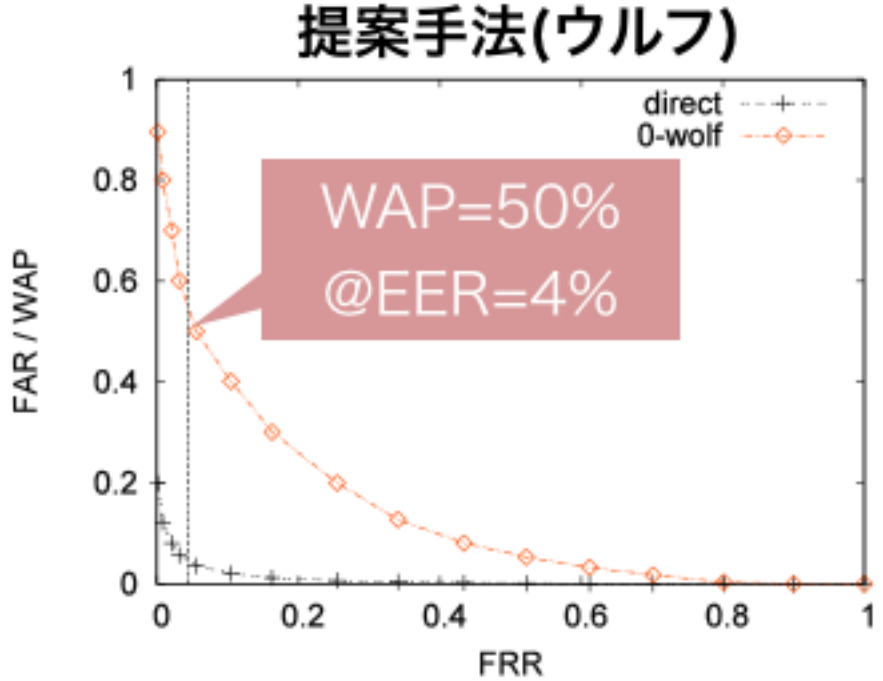
A Comparison of Cumulative Score Distributions
of Human-Wolf (Yellow) and Human-Human (Red,Blue)

中村, 井沼, 大塚, 米澤, 今井, "特徴点ベースの指紋照合アルゴリズムに対するウルフ攻撃," SCIS2013.

話者照合に対するウルフ攻撃（例）







Ohki, T.; Hidano, S.; Takehisa, T., "Evaluation of wolf attack for classified target on speaker verification systems," *Control Automation Robotics & Vision (ICARCV), 2012 12th International Conference on* , vol., no., pp.182,187, 5-7 Dec. 2012

静脈認証に対するウルフ攻撃（例）

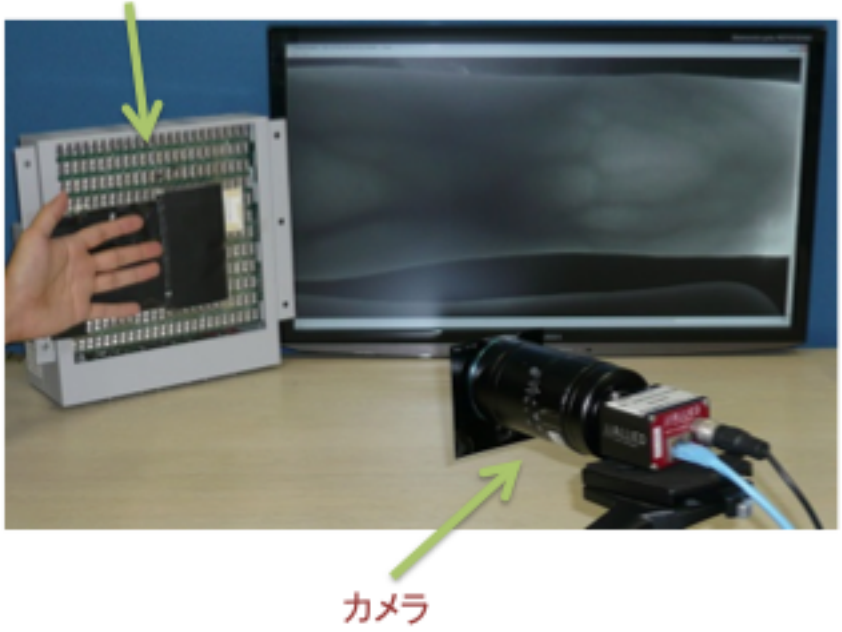
指静脈認証アルゴリズム*を実装し，
ウルフ人工物を用いた攻撃を適用

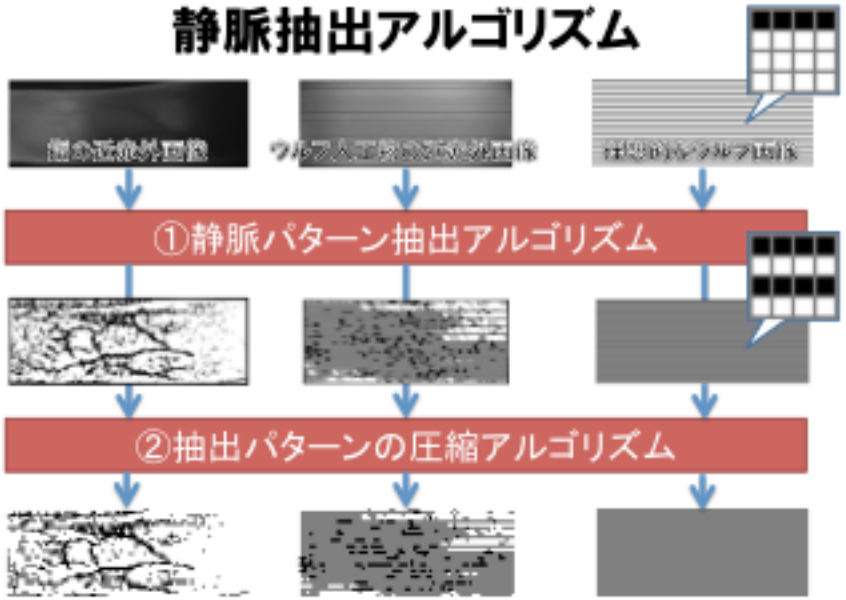
*Naoto Miura, Akio Nagasaka, Takafumi Miyatake, “extraction of finger-vein patterns using maximum curvature points in image profiles,”MVA2005

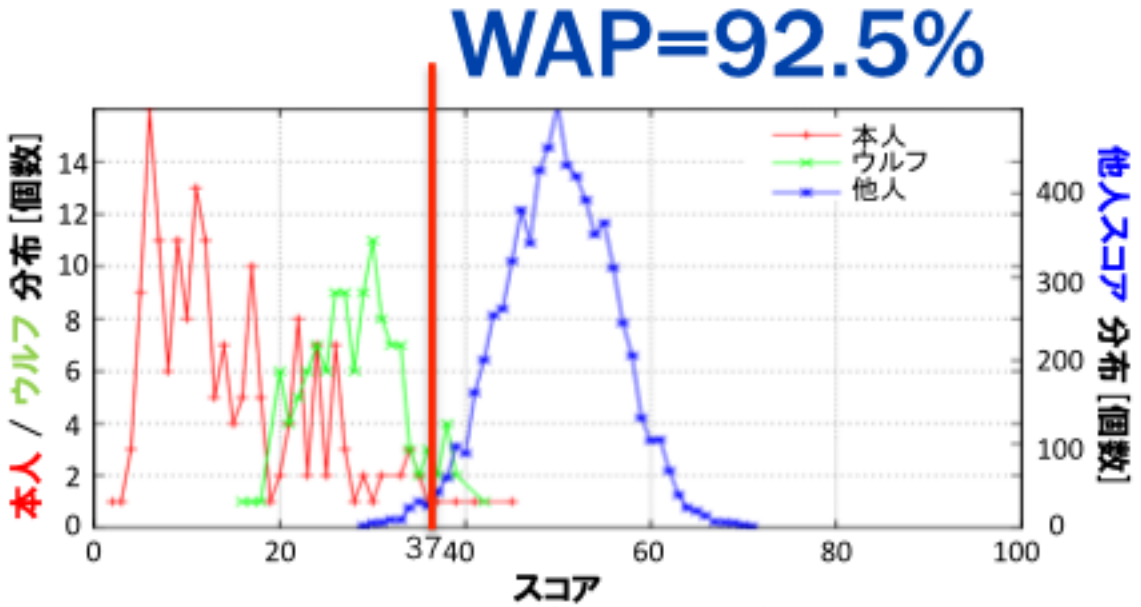
OHPシート
ウルフパターンを印刷
Dpiは130

白色プラ板
ウルフパターンの背景

ゴム板
近赤外光を減衰







Morita, R., Inuma, M., Otsuka, A., Imai, H., “Security evaluation of a finger vein authentication algorithm against the wolf attack,” SBRA2013.

虹彩認証に対するウルフ攻撃（例）

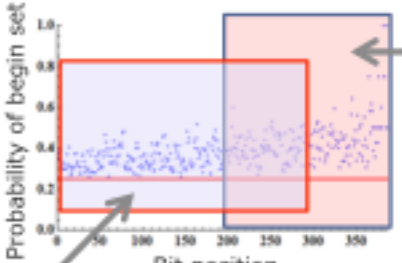
虹彩認証アルゴリズム

J.Daugman, "How Iris Recognition Worls,"IEEE Circuits and Systems for Video Technology, Vol.14, pp21-30, 2004.

- 虹彩領域を見つける
- 白目と黒目の間にあり囲まれた領域が虹彩

- 虹彩領域を極座標変換し長方形の画像に変換

- Wavelet変換後の位相情報を抽出／2値化



ウルフが利用する虹彩領域

本研究では学習元DBのうち、85%のテンプレートでマスクされる領域を選択

通常の虹彩が利用する虹彩領域

白黒の領域…アイリスコードの1と0

赤の領域　…マスクコードによって照合から除外される領域

通常の虹彩とウルフには、マスクコードに大きな違いがある

- ウルフデータを用いたなりすまし成功確率

DB	認証閾値	EER[%]	WAP[%]
虹彩DB1	0.393	0.98	42.6
虹彩DB2	0.375	0.33	14.0
虹彩DB3	0.378	0.65	33.0
ウルフDB	0.393	1.66	33.3

丹, 井沼, 大塚, 今井, "虹彩照合アルゴリズムに対するウルフ攻撃", SCIS2014.

METI基準認証事業：バイオメトリクス攻撃耐性bPAD(Biometric Presentation-Attack Detection)の安全性評価

概要

バイオメトリクス認証装置のなりすまし攻撃（擬似生体の提示、ウルフ攻撃等）に対する安全性指標を開発し、国際標準に提案する。研究期間：2013年7月～2016年2月

体制

委員会

【活動内容】
- 脆弱性情報（論文）のサーベイ
- 規格案の開発

検討委員会
委員長 横浜国立大学 松本 勉 教授
委員 日本電気、日立製作所、富士通研、東芝、バイオニクス、モフィリア、ユニバーサルロボット、IPA、AIST等）
事務局 (JAISA / AIST)

貢献

個別契約に基づく共同研究

【活動内容】
- 企業から装置の提供・技術の開示
- 実験結果の相手企業への開示・守秘義務

AIST ⇔ A社 / B社 / C社

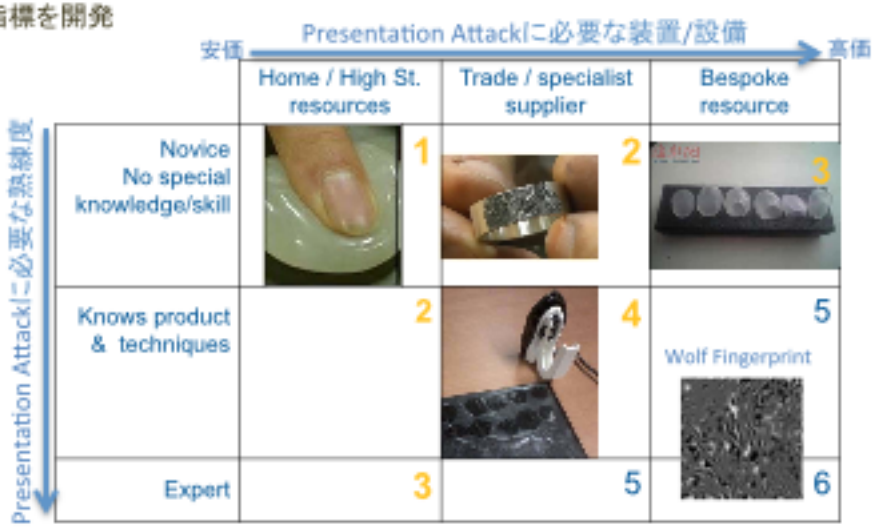
個別に共同研究契約を締結

開発する評価指標の概要

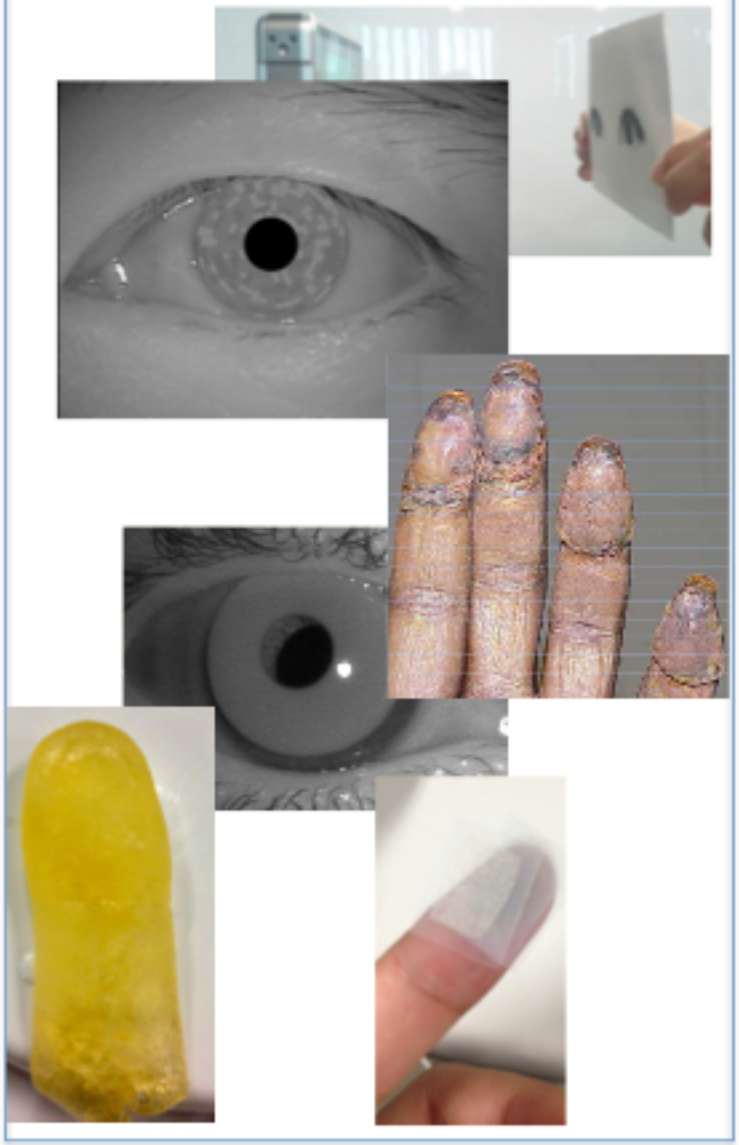
(1) Common Criteria(ISO/IEC 15408）準拠の評価体系の導入

(2) 評価内容

1) 生体情報の入手のし易さ　（容易）指紋＜虹彩＜静脈（困難）
2) 擬似生体の作りやすさ　時間、熟練度、設備／装置等
3) 擬似生体の提示し易さ　時間、熟練度、設備／装置等
等の指標を開発



なりすまし攻撃の例



ご清聴ありがとうございました

ご質問等は以下の連絡先まで

otsuka@ni.aist.go.jp
tetsushi.ohki@aist.go.jp