# BiometricJammer:
# ユーザの利便性を考慮した指紋の盗撮防止手法

国立情報学研究所
大金 建夫　越前 功

# 発表内容

1. 研究背景と研究方針
2. 指紋認証の原理
3. 提案手法
4. 評価
5. 課題と今後の予定
6. 補足資料

# 1. 研究背景と研究方針

# 研究背景

## 指紋センサーの普及

行政・司法

http://politicsofcolor.com/wp-content/uploads/2015/04/dongjae-feat1.jpg

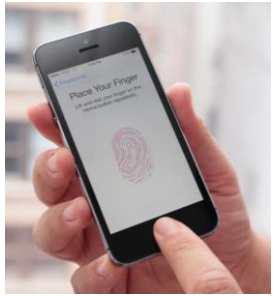
入退出管理

https://www.nisseicom.co.jp/column/column_security/07.images/column_image-02.jpg

PC

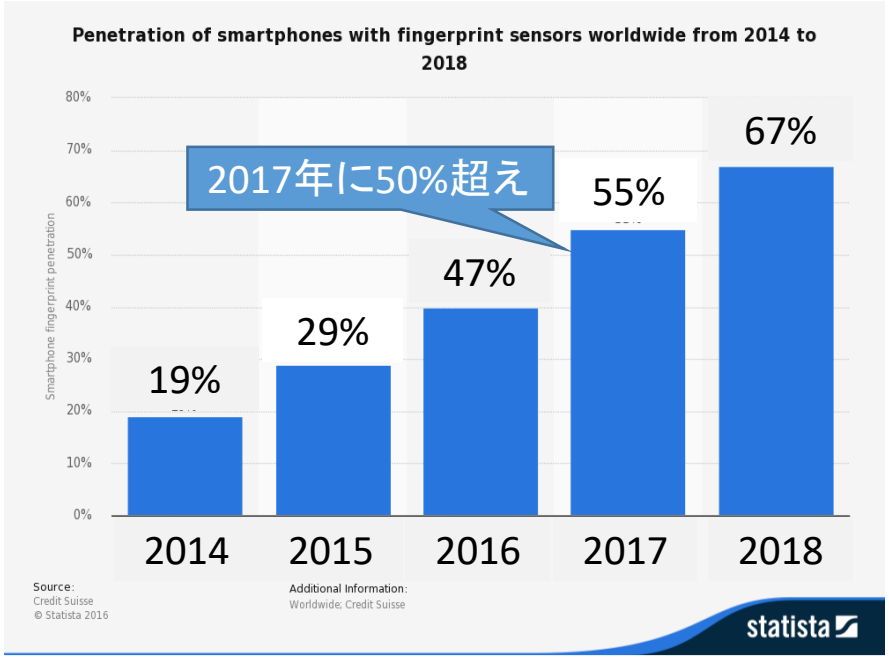
https://ja.wikipedia.org/wiki/%E7%94%9F%E4%BD%93%E8%AA%8D%E8%A8%BC#/media/File:Reading_Fingerprint.jpg

スマートフォン




http://payprotec.com/wp-content/uploads/2014/06/Septimius_02_610x436.jpg

## 指紋センサー搭載スマートフォンの普及率[1]




http://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/

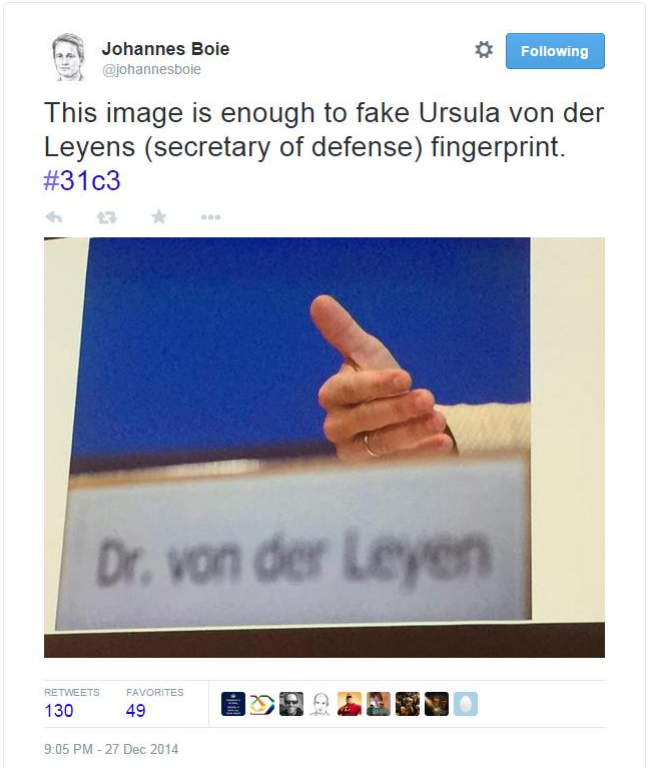
指紋認証機器の小型化、パーソナル化

指紋センサー搭載スマートフォンの急速な普及

[1] Fingerprint sensor penetration in smartphone market to rise above 50% in 2017
http://www.digitimes.com/pda/a20160818PD208.html

# 研究背景

## 撮影された画像からの指紋窃取の脅威




https://www.shellandco.net/wp-content/uploads/2014/12/tweet_finger.png

https://www.youtube.com/watch?v=pIY6k4gvQsY

https://www.youtube.com/watch?v=pIY6k4gvQsY

ドイツのハッカーstarbug (Jan Krissler)による指紋ハックのデモ（2014年12月）[2]

- 市販のデジタルカメラを使って3mの距離から撮影した写真に、公に入手した数枚の写真を使い、画像を補完。
- 指紋の検出には商用ソフトVeriFingerを使用。
- 画像からゴム状の偽指を作成し、iPhone 6の指紋センサーで認証するデモを同時に披露[3]。
- 2つを組み合わせたデモ（撮影された写真を使った指紋認証）を行っていない。

[2] Fingerprint Biometrics hacked again
https://www.ccc.de/en/updates/2014/ursel
[3] Chaos Computer Club breaks Apple TouchID
http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

# 研究背景

## 偽指―指紋センサーの既知の脆弱性―

http://ichef-1.bbci.co.uk/news/660/media/images/74270000/png/_74270693_fake.png

http://regmedia.co.uk/2013/09/22/iphone5_touchid_crack.png?x=648&y=348&crop=1

https://i.ytimg.com/vi/KBMqoUYxUJs/sddefault.jpg

http://www.zdnet.com/article/apples-advanced-fingerprint-technology-is-hacked-should-you-worry/

指紋の凹凸を正確に型取りすることにより、指紋センサーに誤認識される指紋の複製（偽指）を作成可能[4][5]。

- 素材はシリコン、ゼラチン、樹脂、油脂、粘土、糊など多数。

他人の持ち物などから残留指紋を入手し、作成した偽指を使って成りすましや不正ログインが可能。

[4] Putte and Keuning. “Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned,” in Proc. Working Conf. on Smart Card Research and Advanced Applications (4th), Proc. IFIP TC8/WG8.8, pp. 289-303, 2000.
[5] Matsumoto et al.. “Impact of Artificial “Gummy” Fingers on Fingerprint Systems,” in Proc. Of SPIE, vol. 4677, pp. 275-289, 2002.

# 研究背景

## 従来の指紋ハック

残留指紋の収集

https://en.wikipedia.org/wiki/Fingerprint#/media/File:Dacty_poederen.JPG

偽指の作成

http://www.zdnet.com/article/apples-advanced-fingerprint-technology-is-hacked-should-you-worry/

## 盗撮による指紋ハック

盗撮・写り込み

指紋の復元

偽指の作成

- 攻撃者は、攻撃対象の指紋を物理的に入手する必要がない。
- 偽指に対抗する認証技術は存在するが、意図しない盗撮自体を防ぐ技術は存在しない。（→生体検知による偽指対策）

# 従来対策：手袋の着用

## 通常の手袋

https://www.kaunet.com/images/goods/main/large/K2704302.jpg

シンプルな手袋でも盗撮の防止が可能

装着したままでは指紋センサーに反応しない

## タッチパネル対応手袋

http://direct.sanwa.co.jp/images/goods/200-PEN001BK_MX.JPG

装着したままタッチパネルの操作が可能

指紋センサーには非対応

## 手袋用電導シール

https://www.kickstarter.com/projects/nanotips/taps-touchscreen-sticker-w-touch-id-ships-before-x

特殊なパターンによってApple TouchID 指紋センサーで認証可能

本人の指紋ではない

装着したまま全ての指紋センサーで認証可能という決定的な製品は存在しない

# 研究方針

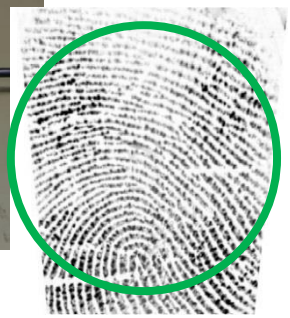
目的：ユーザの利便性を確保しつつ、盗撮による指紋の不正な取得を防止

- 接触式の指紋センサーによる指紋認証が可能であること。
- 撮影された写真から取得した指紋の認証が不可能であること。
- 指紋センサーや認証システムを変更せず、ユーザーの意思によって適用可能であること。

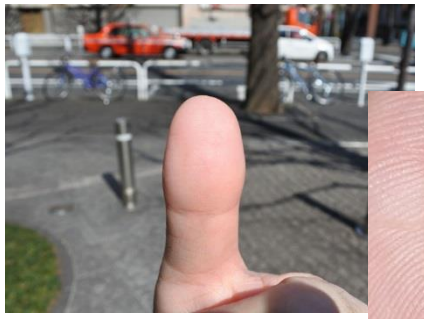
手段：装着可能なジャミングパターンの提案

指紋センサー

認証可



デジタルカメラ

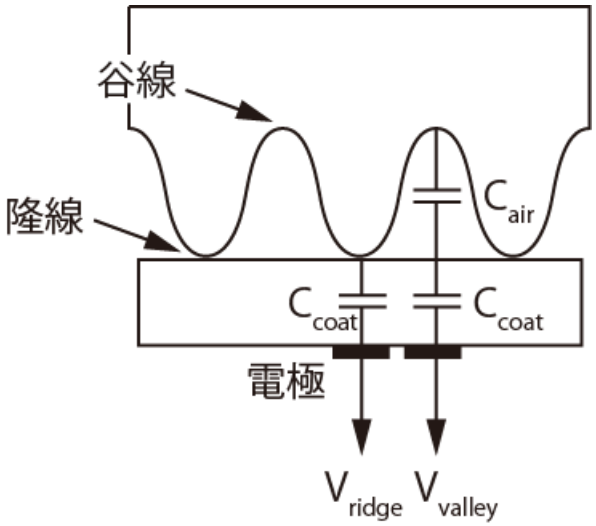


認証不可

# 2. 指紋認証の原理

# 指紋センサーの原理[6][7]

静電容量方式

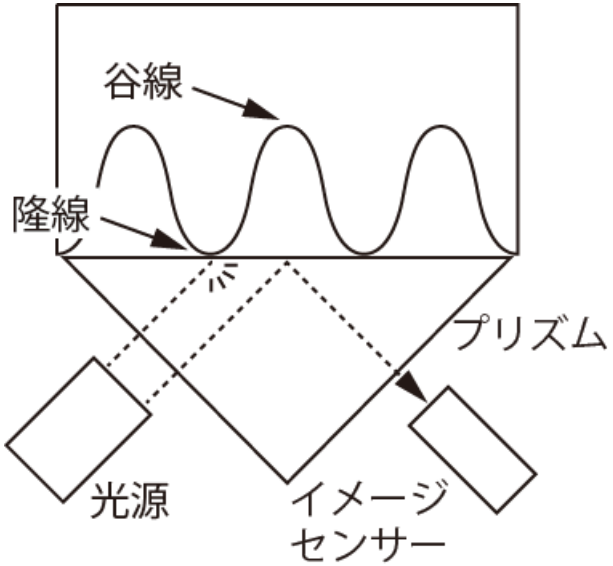



皮膚と電極との間の静電容量の違いを検出する。

・隆線では指紋センサーの被覆材による静電容量のみ。

・谷線では上記に加え、空気の静電容量が影響する。

光学方式



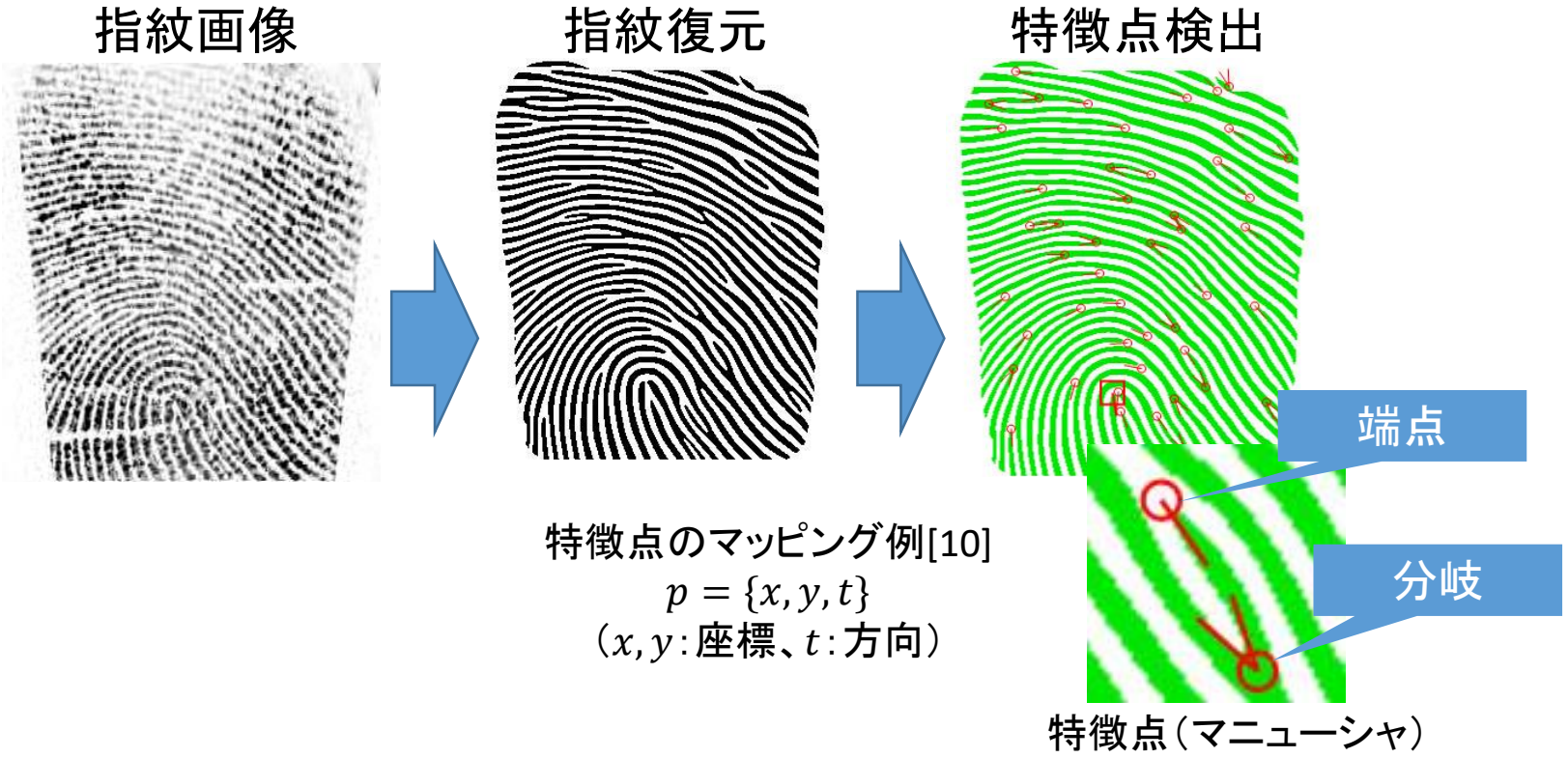

光の反射特性の違いをイメージセンサーで検出する。

・隆線では皮膚の水分の影響で全方向に散乱。

・谷線ではプリズムと空気層の境界面で全反射。

[6] 特許庁　標準技術集　バイオメトリック照合の入力・認識
www.jpo.jp/shiryou/s_sonota/hyoujun_gijutsu/biometric/1-1-2.pdf
[7] 藤枝一郎 “画像入出力デバイスの基礎 光学と半導体物理の理論からディスプレイとイメージセンサを理解する” 森北出版，2005

# 特徴点の検出[8][9]




特徴点のマッピング例[10]

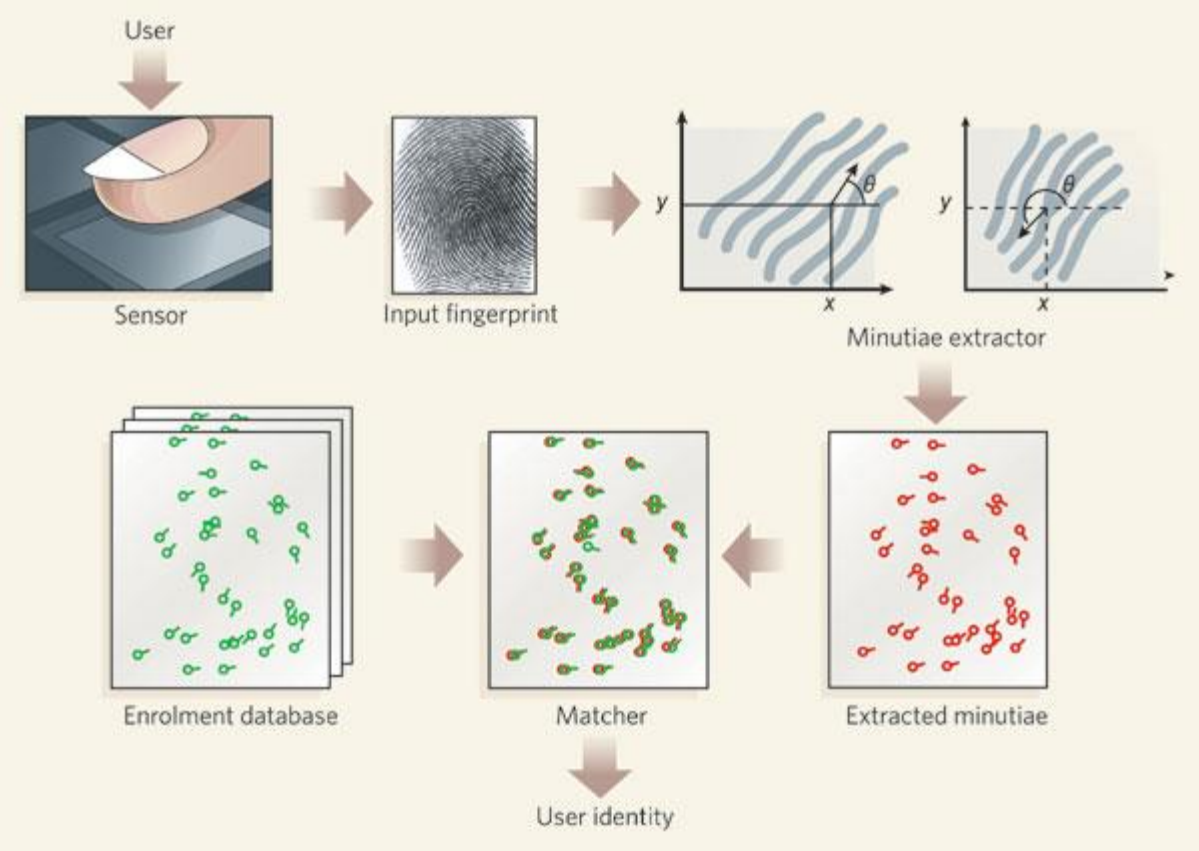
$p = \{x, y, t\}$

（$x, y$：座標、$t$：方向）

特徴点（マニューシャ）

[8] Jain et al.. “On-line Fingerprint Verification,” IEEE Transactions on Pattern Analysis Machine Intelligence, vol.19, no.4, pp. 302-313, 1997.
[9] Hong et al.. “Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” IEEE Transactions on Pattern Analysis Machine Intelligence, vol.20, no. 8, pp. 777-789, 1998
[10] National Institute of Standards and Technology, “User’s Guide to Expert Controlled Distribution of NIST Biometric Image Software (NBIS-EC),” http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51096

# 指紋のマッチング

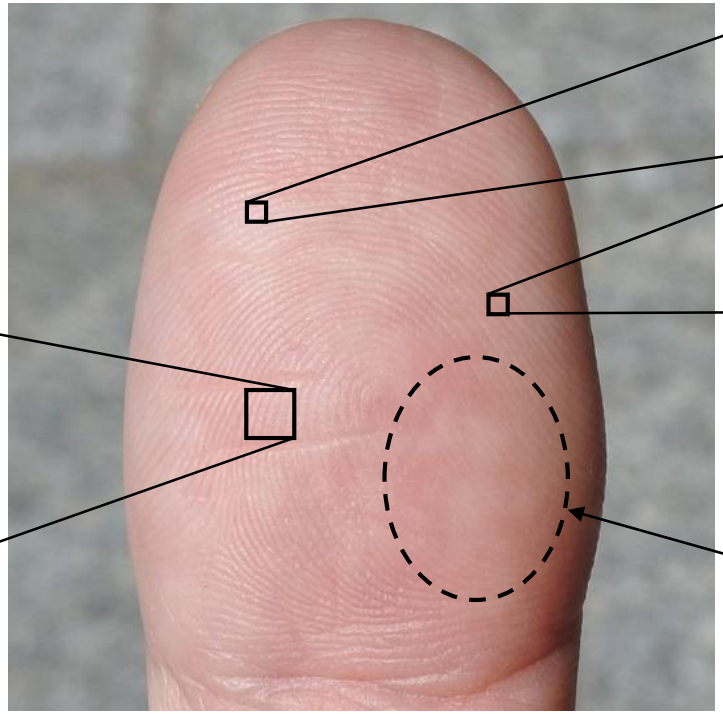



http://www.nature.com/nature/journal/v449/n7158/box/449038a_BX1.html

- 登録された指紋と入力画像の指紋の特徴点同士を比較することにより、本人と判定。
- 点群間のパターンマッチングなので、データ量が少なく、高速。
- 指紋画像を保存しないため、指紋データ漏洩の危険が少ない。

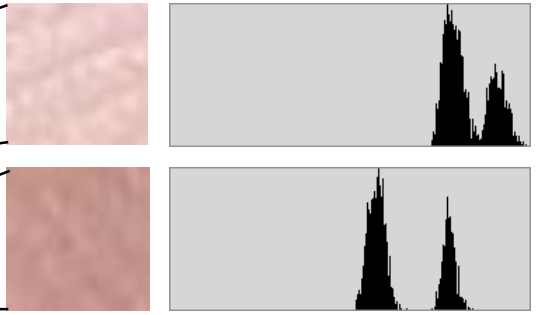
# 撮影された指紋画像からの指紋の取得

指紋の構造ではなく陰影をサンプリングするので、ノイズが乗りやすい



撮影画像

（ヒストグラム）

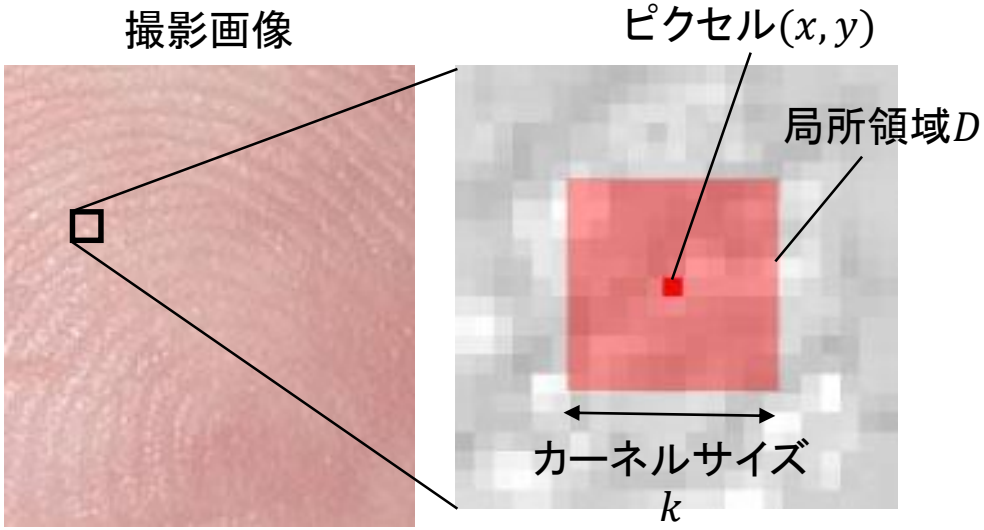


隆線と谷線のコントラストが局所的に一定しない

汗や血管などによって色ムラが発生し、地の色が大きく変化する

撮影された指紋画像から直接指紋を認識することは不可能。

# 適応的閾値処理




- 空間フィルタリングの一種
- あるピクセル$(x, y)$の閾値$d(x, y)$を、画素$I(x, y)$の局所領域$D$における平均値として表す。

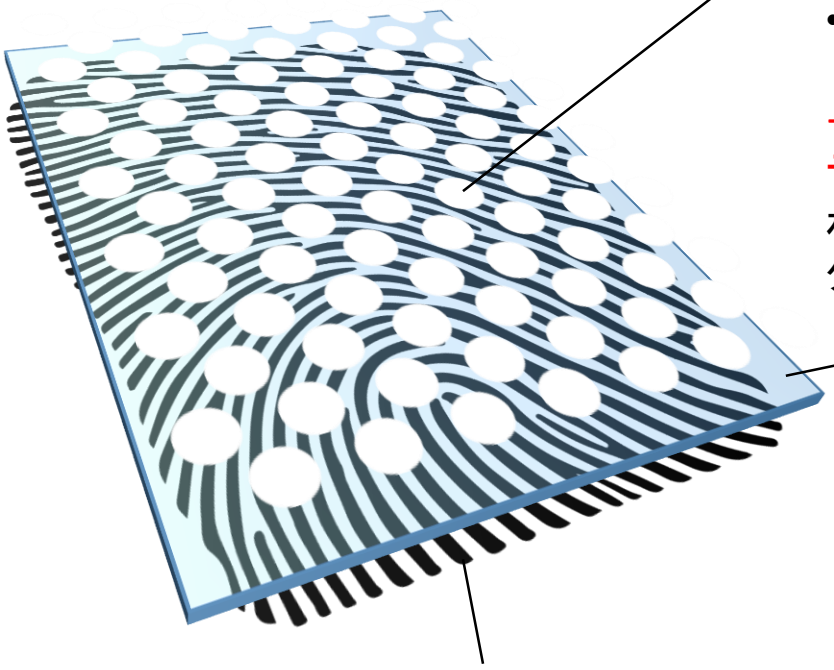
$$d(x, y) = \frac{1}{N} \sum_{x,y \subset D} I(x, y)$$

$k = 3$　　$k = 11$　　$k = 99$

カーネルサイズ$k$として隆線間隔に近い値を取ると、ノイズを除去して指紋を強調することが可能になる。

# 3. 提案手法

# 提案手法




パターン

- 可視光領域に光散乱特性
- 指紋の全てを被覆する必要はない

→妨害効果の程度や視覚的なデザインを変更可能

材料の候補：酸化亜鉛、酸化チタン

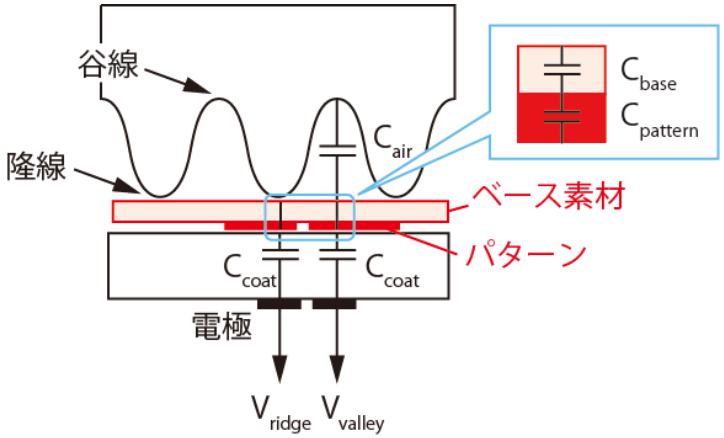
ベース素材

- 可視光領域で光を透過
- 接触時には指紋の隆線にもれなく密着し、余分な気泡を残さない

→接触式の指紋センサーによる認証を妨げない

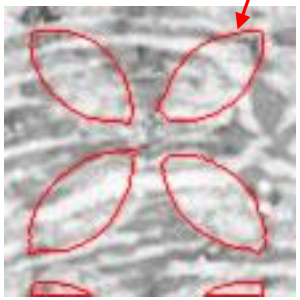
材料の候補：ゴム・シリコン・食品添加物

# 指紋センサーの透過性（静電容量方式）




取得イメージ

パターンの輪郭



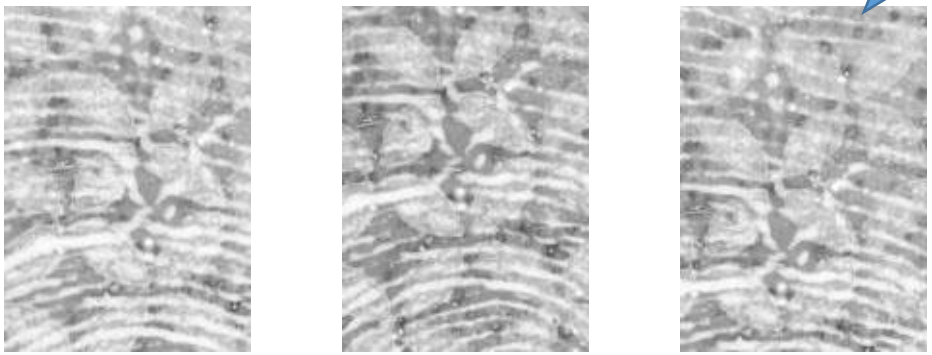
- コーティング層および空気層の静電容量に加えて、ベース素材およびパターンの静電容量が影響する。
- 空気層と比較して、他の3種類の比誘電率には大きな違いがないので、実質的には膜厚の問題となり、指紋イメージの取得に影響しない。

（→比誘電率一覧）

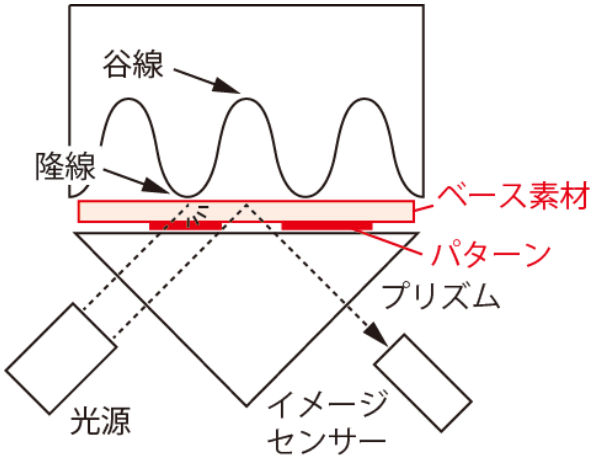
膜厚の影響

膜厚の増加に応じて谷線が細くなっていく

薄い ⟷ 厚い



# 指紋センサーの透過性（光学方式）




- ベース素材の屈折率はプリズム（光学ガラス）とほぼ同じであるため、全反射条件に影響しない。
- ベース素材およびパターンの反射率は、材質により4～18%程度であるから、ほとんどの光が透過し、指紋イメージの取得に影響しない。

（→屈折率および反射率一覧）

取得イメージ

- パターンの素材はほぼ透過。
- パターンの表面が不均一なため、細かい気泡が発生し隆線が乱れる。

膜厚の影響

薄い ⟷ 厚い

# 妨害効果の考察

サンプルパターン

ドットが皮膚より暗い

同程度の明るさ

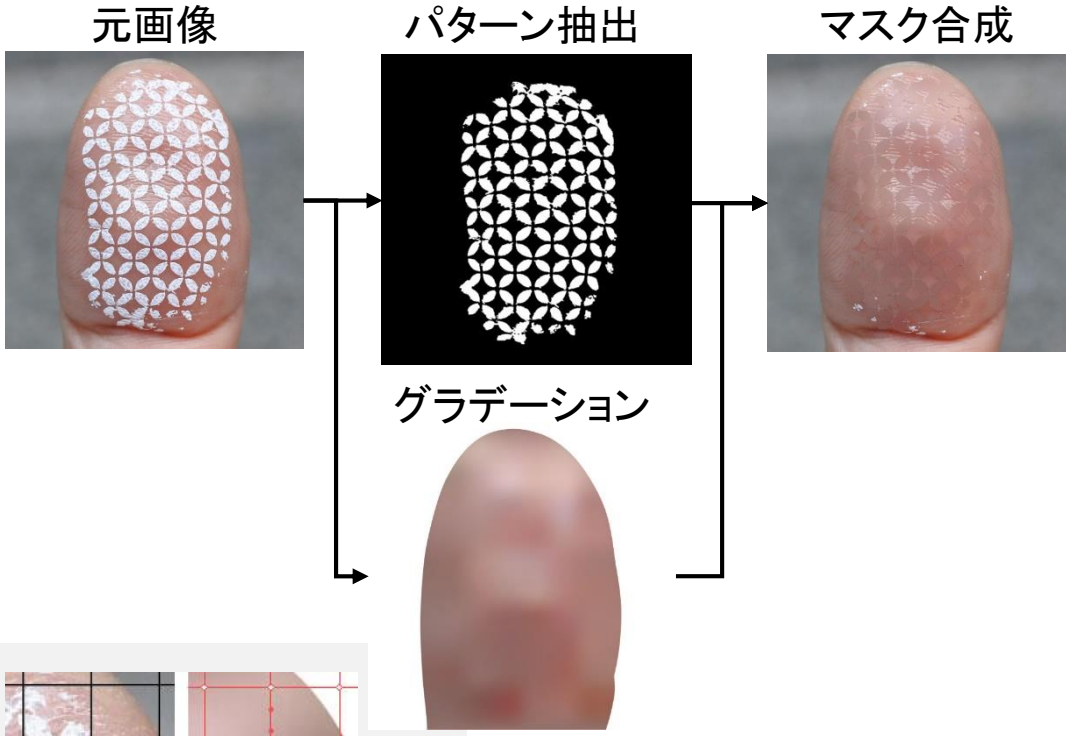
ドットが皮膚より明るい

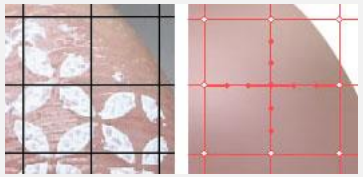
効果が弱い

指紋画像にドットパターンを重畳し、適応的閾値処理を実行。

1. 偽の特徴点の発生。ドットが重畳されることにより、ノイズ要素を隆線と誤って認識。
2. 本来の特徴点の消失。端点や分岐の判定に曖昧さが発生し、検出結果から排除される。
3. 特徴点の種類の変更。ドットによって判定の閾値が変化し、端点と分岐の判断が変更される。

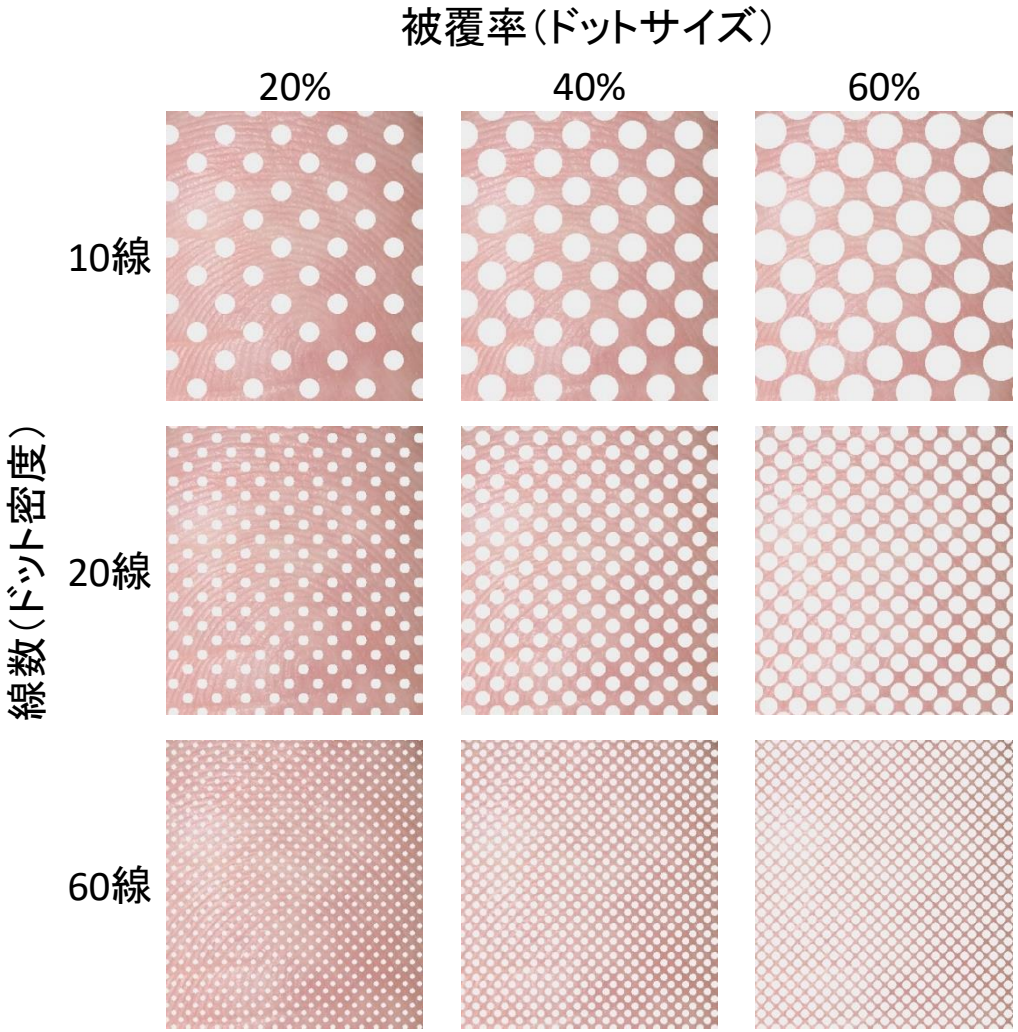
# パターンの塗りつぶしによる妨害効果の回避



近傍の色をサンプリングしてグラデーションを作成

# 塗りつぶしに耐性のあるパターンの検討

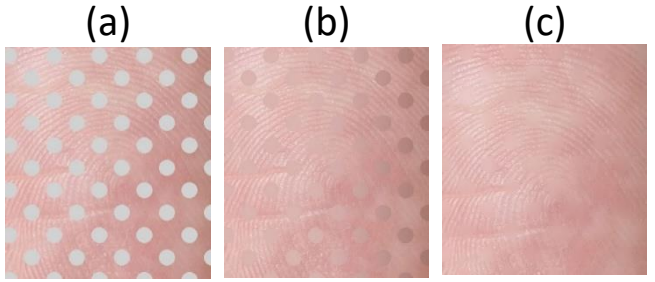



指紋画像に可変サイズのドットパターンを重畳し、認識できるかどうかのシミュレーションを実施。

塗りつぶしの種類

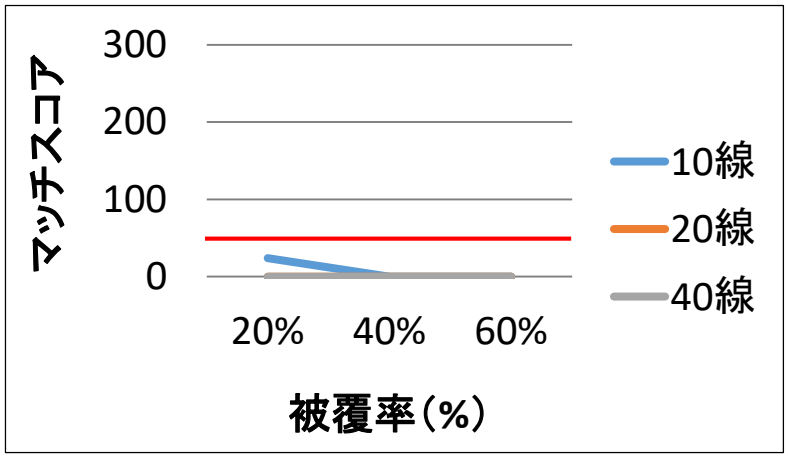
(a) 明るいグレー
(b) 皮膚の平均色
(c) ドットの周囲の色

※(b)(c)は塗りつぶしによる妨害効果の回避手法を想定。

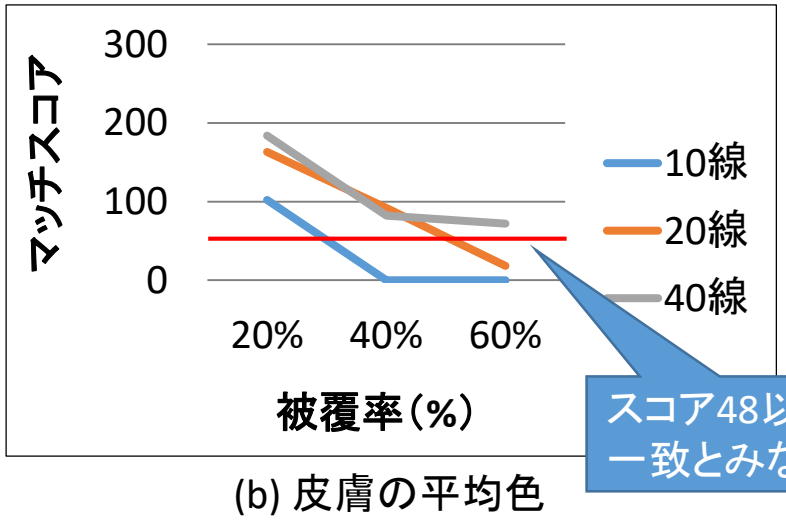



※線数：1インチ当たりのドット数

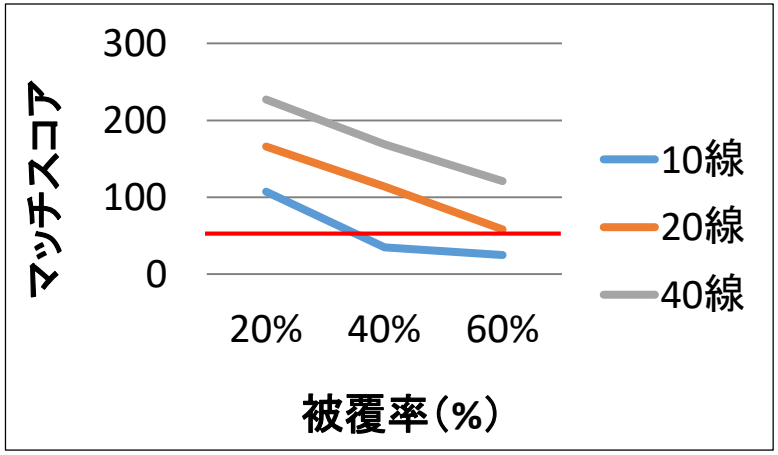
# パターン設計：マッチング結果




(a) 明るいグレー




(b) 皮膚の平均色




(c) ドットの周囲の色

・被覆率が高いほど妨害効果が高い
・同じ被覆率では線数が少ない（ドットサイズが大きい）ほど妨害効果が高い

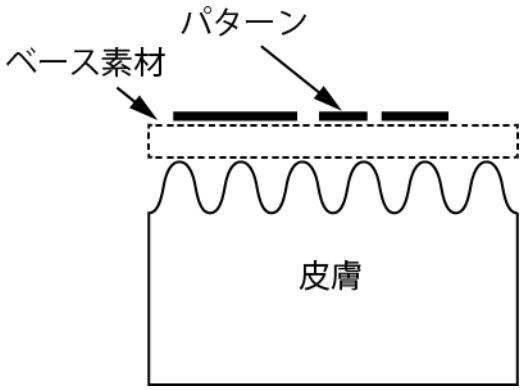
被覆率40%以上かつドットサイズが大きいパターンが必須

# 4. 評価

# 評価用プロトタイプの作成

外観

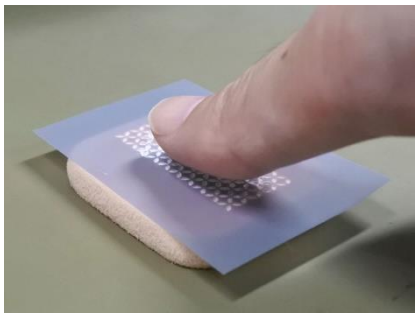
構成図




製作手順

①ベース素材（アクリル系の下塗り材）を指表面に塗布。

②パターン用のアクリル絵の具を化粧用のパフに染み込ませる。



③ネイルアート用のステンシルシートを使い、指先にパターンを転写。

# 評価：撮影画像とのマッチング

テンプレート

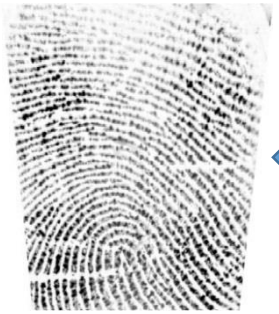
入力

入力画像の種類

未装着

装着

装着、塗りつぶし



マッチング

※適応的閾値処理後

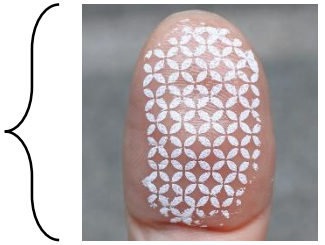
BiometricJammerを装着した指で，
撮影された画像からの指紋認証を
妨害できるかどうか？

# 評価：指紋センサーとのマッチング

テンプレート

入力

入力画像の種類



装着

マッチング
（3×3＝9回）

BiometricJammerを装着した指で，指紋センサーによる正当な指紋認証に成功するかどうか？

# 評価環境

## 装着具

ベース素材：アクリル樹脂
パターン：アクリル塗料（酸化亜鉛の顔料を含む）
被覆率：40%

## デジタルカメラ

Canon EOS 70D
画素数：2020万画素
ISO感度設定：自動
露出設定：自動
フォーカス設定：1点AF
レンズ：EF-S 18-135mm F3.5-5.6 IS STM（テレ端固定）

## 撮影環境

被験者：学生4名
撮影距離：1m～5m（0.5m間隔）
日照条件：屋外，薄曇～晴
（被写体照度7800～31600ルクス）

## 指紋復元・マッチングプログラム

Neurotechnology VeriFinger[11]
（商用ソフト）

## 指紋センサー

DigitalPersona
EikonTouch 710
（静電容量方式）

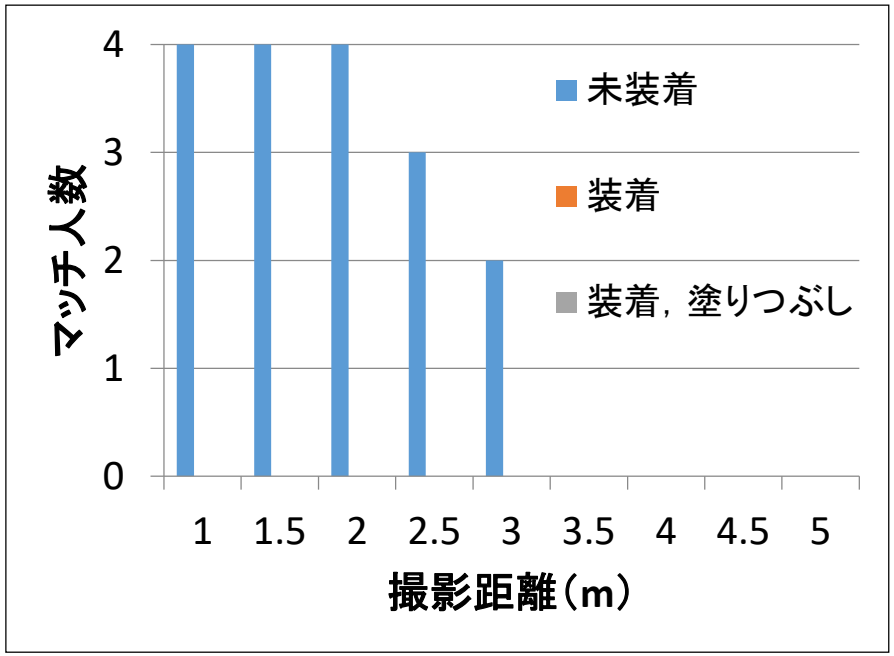
DigitalPersona
U.are.U 4500
（光学方式）

[11] Neurotechnology, VeriFinger SDK
http://www.neurotechnology.com/verifinger.html

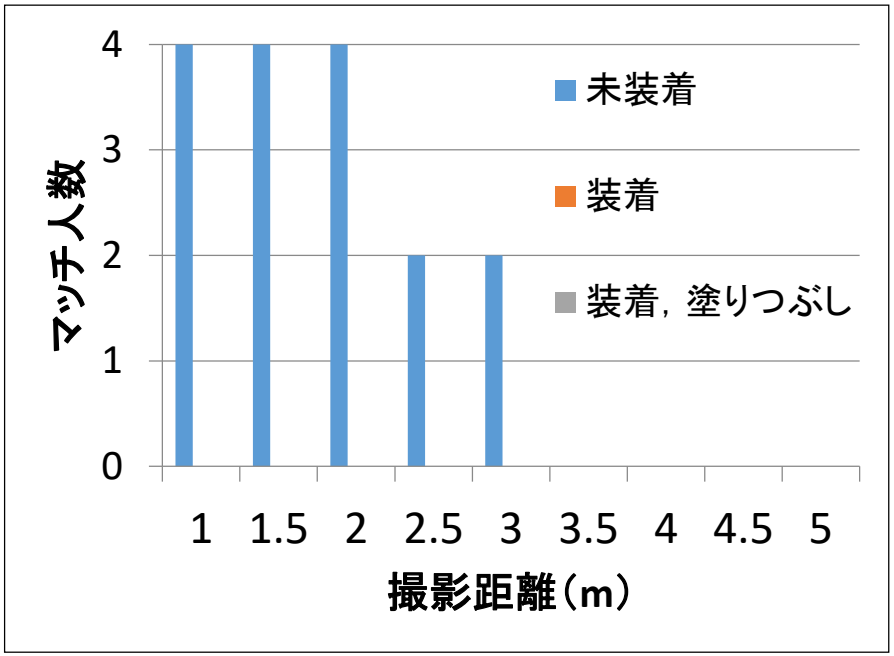
# 評価結果：撮影画像とのマッチング

## (a) 撮影距離ごとのマッチ人数

静電容量方式




光学方式

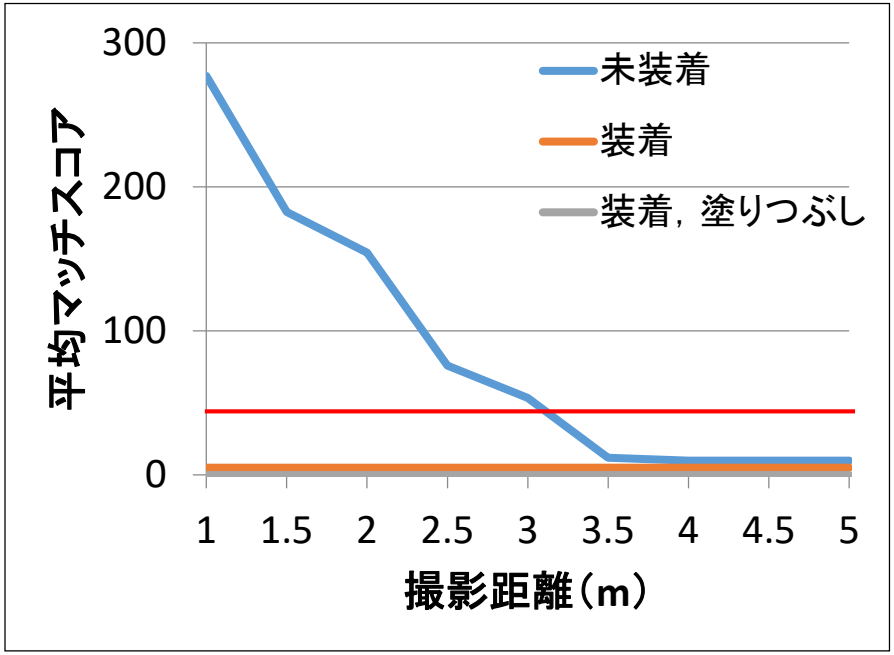



- 市販のデジタルカメラを使い、3m以下の距離で撮影された画像から指紋を復元可能。
- BiometricJammerの装着により、すべての距離で復元可能な指紋の取得を防止。

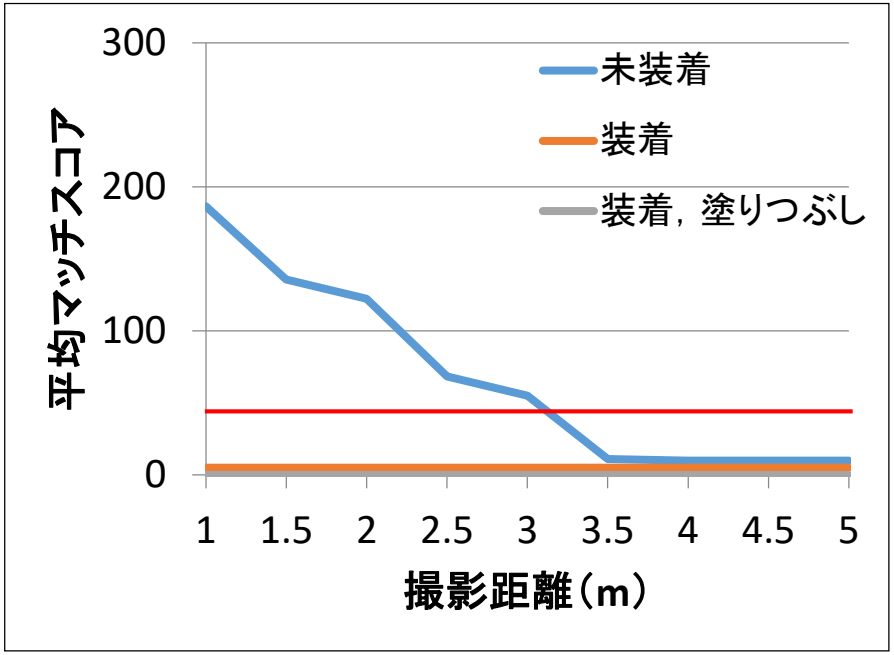
# 評価結果：撮影画像とのマッチング

## (b) 撮影距離ごとの平均マッチスコア

静電容量方式




光学方式




- VeriFingerの判定基準：スコア48 = FAR0.01%で一致と判定
- BiometricJammer装着時、および装着画像に塗りつぶし加工を行ったものについては、全て特徴点の検出に失敗（マッチスコア0とする）

# 評価結果：指紋センサーとのマッチング

静電容量方式

| 被験者 | 成功数 | 最少スコア | 最大スコア |
|---|---|---|---|
| A | 9 | 262 | 441 |
| B | 8 | 44 | 211 |
| C | 9 | 163 | 276 |
| D | 9 | 59 | 158 |

光学方式

| 被験者 | 成功数 | 最少スコア | 最大スコア |
|---|---|---|---|
| A | 9 | 196 | 333 |
| B | 3 | 19 | 80 |
| C | 9 | 263 | 370 |
| D | 9 | 179 | 375 |

赤字: 一致（スコア48以上）

失敗例：テンプレート作成時に指の置き方（圧力・方向）が不安定

BiometricJammerの装着により、接触式の指紋センサーによる認証を妨げることはない

# 5. 課題と今後の予定

# 課題

## 使用済み製品の廃棄の問題

塗膜タイプ

指紋の凹凸にあわせて整形されるため、型取りと同様の立体形状が残る。

シールタイプ

表面に指紋の油分が付着し、きわめて鮮明な残留指紋となる。

不用意に捨てられた使用済み製品を入手することにより、プライバシーを保護するためのBiometric Jammerが偽指の作成を容易にしてしまう。

剥がすときには水に溶ける、あるいはボロボロに破れて復元不能になるといった対策が必要。

# 課題

## 人体に対する安全性の問題

プロトタイプに使用したアクリル樹脂（アクリル酸メチル）は、人体に接触して使用した場合の有害性が指摘されている[12]。

有望な素材

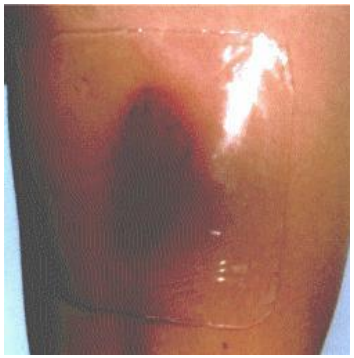
シリコン

http://ameblo.jp/c-toys/entry-10896923057.html

ラテックス

http://www.blast.jp/ja/theme02-column22/

食品添加物（CMC, アルギン酸など）



http://www.rist.or.jp/atomica/data/pict/08/08040117/13.gif

技術要件をクリアしつつ、人体に着用しても安全な素材の選定と評価が必要。

[12] CERI有害性評価書　アクリル酸メチル
www.cerij.or.jp/evaluation_document/yugai/96_33_3.pdf

# 今後の研究

## 指紋

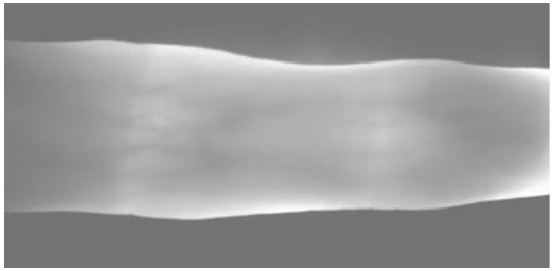
https://en.wikipedia.org/wiki/Fingerprint

## 掌紋

https://commons.wikimedia.org/wiki/Category:Palm_prints#/media/File:Female_right_palm_print_-_1.gif

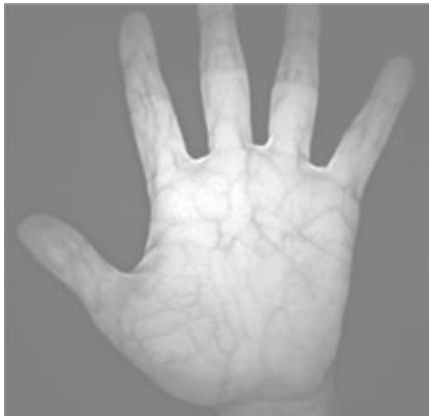
**各種生体情報の特徴に合わせた**
**不正取得防止技術の確立**

## 指静脈



http://www.mathworks.com/matlabcentral/fileexchange/35716-miura-et-al-vein-extraction-methods

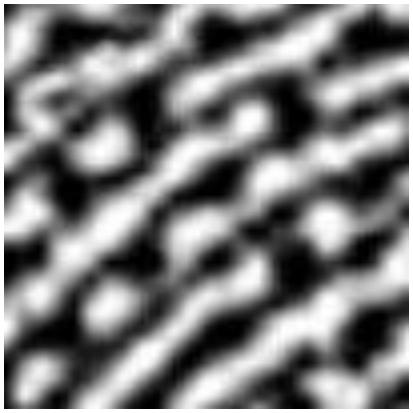
## 手のひら静脈



http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.8983&rep=rep1&type=pdf

# 6. 補足資料

# ドットサイズの要件



1本の隆線に乗っている場合

他の隆線と離れているため、特徴点の検出に影響を与えない。

2本の隆線に乗っている場合

隆線の接続に曖昧さが発生するので、特徴点の検出を妨害できる。

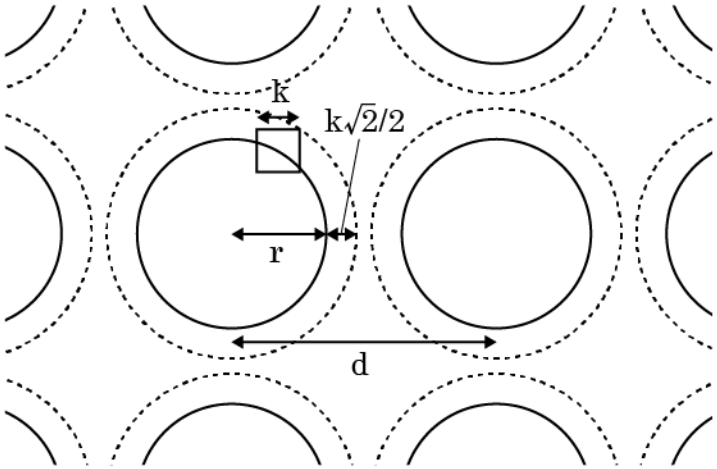
特徴点の検出を妨害するためには、ドットが2本以上の隆線に乗っていなければならない。
ドット半径を$r$、隆線間隔を$h$とすると、

$$2r > 2h$$

すなわち

$$r > h$$

# ドット密度の要件




ドット配列の影響範囲

マニューシャ・マッチング方式では、数個の特徴点だけでもマッチするので、画像全体にわたってノイズを重畳しなければならない。
ドット半径を$r$、フィルタのカーネルサイズを$k$、隆線間隔を$h$とすると、

$$\mathrm{r} + \frac{k\sqrt{2}}{2} > \frac{d}{2}$$

すなわち

$$r > \frac{d}{2} - \frac{k\sqrt{2}}{2}$$

# パターン設計:ドット要件の判定結果

サイズ要件の判定結果

| パターン | r | h | $r > h$ |
|---|---|---|---|
| 10線20% | 12.615 | 10.0 | True |
| 10線40% | 17.841 | 10.0 | True |
| 10線60% | 21.850 | 10.0 | True |
| 20線20% | 6.307 | 10.0 | False |
| 20線40% | 8.920 | 10.0 | False |
| 20線60% | 10.925 | 10.0 | True |
| 40線20% | 3.153 | 10.0 | False |
| 40線40% | 4.460 | 10.0 | False |
| 40線60% | 5.462 | 10.0 | False |

密度要件の判定結果

| パターン | r | $\frac{d}{2} - \frac{k\sqrt{2}}{2}$ | $r > \frac{d}{2} - \frac{k\sqrt{2}}{2}$ |
|---|---|---|---|
| 10線20% | 12.615 | 17.222 | False |
| 10線40% | 17.841 | 17.222 | True |
| 10線60% | 21.850 | 17.222 | True |
| 20線20% | 6.307 | 4.722 | True |
| 20線40% | 8.920 | 4.722 | True |
| 20線60% | 10.925 | 4.722 | True |
| 40線20% | 3.153 | -1.528 | True |
| 40線40% | 4.460 | -1.528 | True |
| 40線60% | 5.462 | -1.528 | True |

スライド22,23で検討したドットパターンについて、ドットサイズおよび密度要件を満たすかどうかを判定。

撮影距離 1m
隆線間隔 h=10(ピクセル)
カーネルサイズ k=11(ピクセル)

2つの要件を同時に満たすのは、10線40%、10線60%、20線60%の3種類

↓

マッチング結果とおおむね一致

# 生体検知による偽指への対策

a.　指紋の変形に基づく手法

[13] Antonelli et al.. “Fake finger detection by skin distortion analysis,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 3, pp. 360-373, 2006.

b.　発汗に基づく手法

[14] Derakhshani et al.. “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” Pattern Recognition, vol. 36, no. 2, pp. 383-396, 2003.

c.　テクスチャの粗さに基づく手法

[15] Moon et al.. “Wavelet based fingerprint liveness detection,” Electronics Letters, vol. 41, no. 20, pp. 1112-1113, 2005.

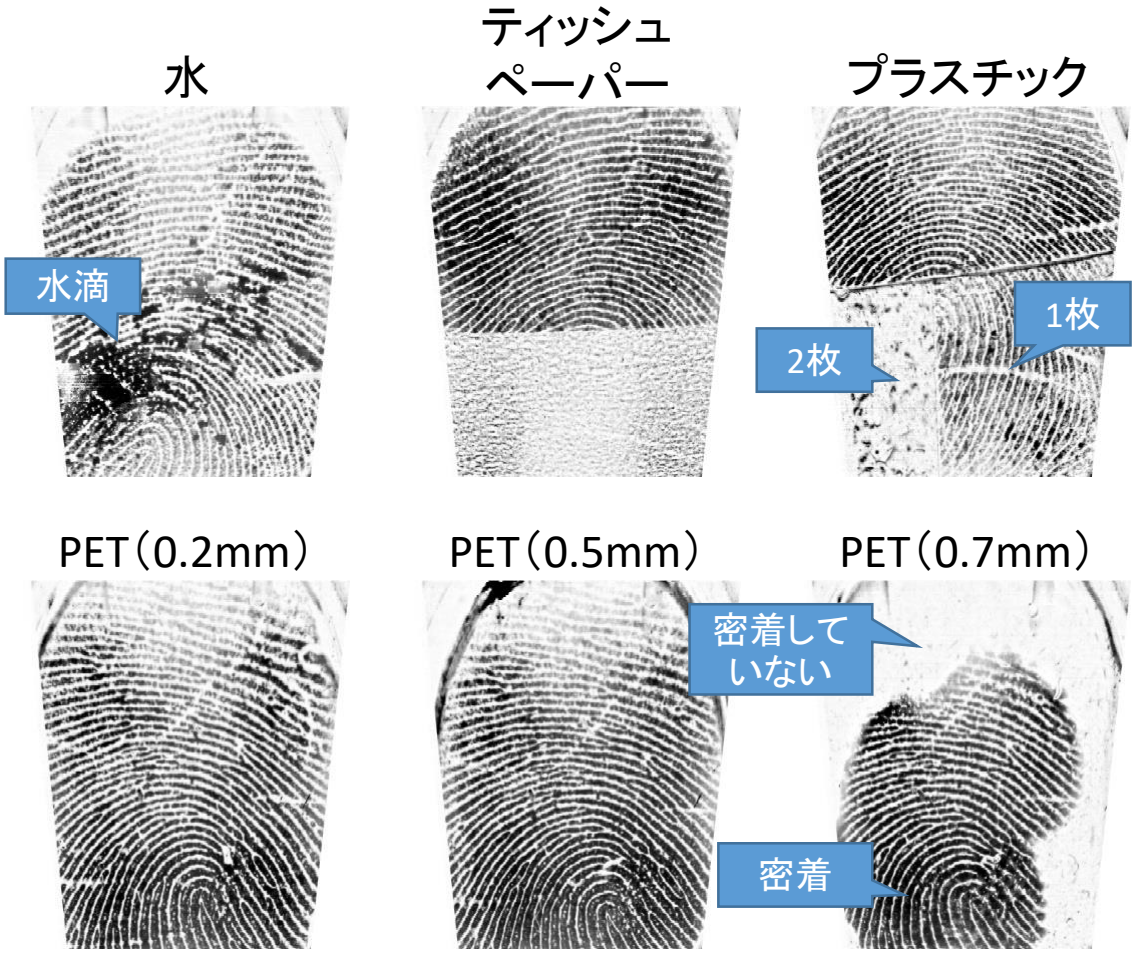
d.　隆線の密度に基づく手法

[16] Abhyankar and Schuckers. “Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques,” in Proc. Int. Conf. on Image Processing, pp. 321-324, 2006.

e.　細孔の密度に基づく手法

[17] Manivanan et al.. “Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering,” Electronics Letters, vol. 46, no. 18, pp. 1268-1269, 2010.

# さまざまな素材に対する光学センサーの透過性




・空気層の介在によって全反射が起き、明線となる。
・水分の介在によって全反射条件が崩れ、暗線となる。

・素材が接触面に密着していない場合は、空気層によって画像の不明瞭化および白トビが発生する（上段右）。
・素材が接触面に密着している場合は、素材の厚さに関わらず画像の質は一定である（下段）。

# 比誘電率一覧[18]

| 物質 | 比誘電率 | 備考 |
|---|---|---|
| 空気 | 1.0 | |
| アクリル | 2.7～4.5 | ベース素材 |
| シリコン | 2.4 | ベース素材およびコーティング |
| 酸化亜鉛 | 1.7～2.5 | パターン |
| 酸化チタン | 100 | パターン |

酸化亜鉛

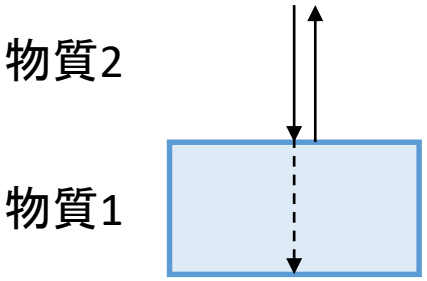
酸化チタン

※パターン素材の比較（静電容量方式）
酸化チタンの方が比誘電率が高く、指紋画像にムラが発生する。

[18] 山本電機インスツルメンツ　比誘電率表
http://www.yei-jp.com/technology/hiyudenritu/hiyudenritu.html

# 屈折率および反射率一覧[19]

| 物質 | 屈折率 | 反射率（対空気） | 備考 |
|---|---|---|---|
| 空気 | 1.0 | — | |
| 光学ガラス | 1.5 | 0.04 | プリズム |
| アクリル | 1.5 | 0.04 | ベース素材 |
| シリコン | 1.43 | 0.03 | ベース素材 |
| 酸化亜鉛 | 2.0 | 0.11 | パターン |
| 酸化チタン | 2.5 | 0.18 | パターン |




※物質1の物質2に対する反射率は、物質1, 2の屈折率をそれぞれ$n_1, n_2$とすると、

$$R_{ref} = \left(\frac{n_1 - n_2}{n_1 + n_2}\right)^2$$

[19] フィルメトリクス　屈折率一覧表
http://www.filmetricsinc.jp/refractive-index-database

# 写真からの指紋検出に対する妨害効果

写真　　（二値化後）

本方式

●幾何学形状をノイズとして重畳することにより、指紋の検出に失敗させる

●エッジの強調による隆線の断片化およびパターン領域における特徴点の隠蔽効果

●画像処理によるパターンキャンセル対策のため、パターン面積を広くとる必要