

通常の指紋認証を妨げずに写真からの指紋復元を防ぐには BiometricJammer：ユーザーの利便性を 考慮した撮影画像からの指紋認識防止手法

大金 建夫, 越前 功
Tateo Ogane, Isao Echizen

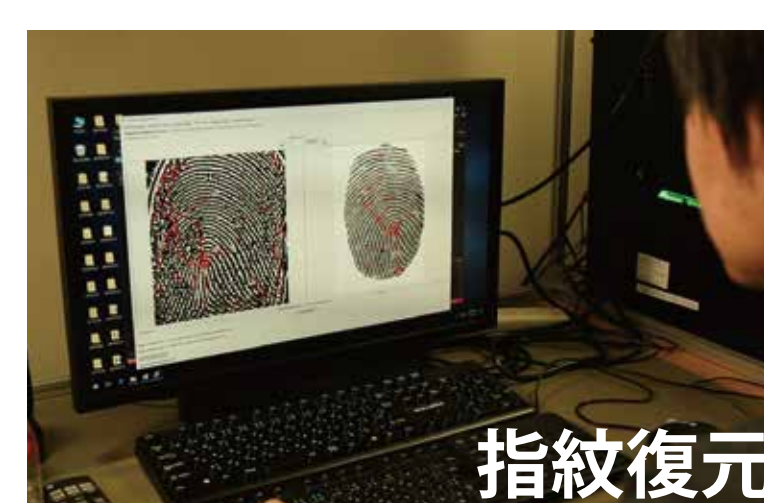
どんな研究？

デジタルカメラなど身近な機器によって、本人の知らないところで指紋などの生体情報が撮影され不正利用される脅威から、自らを守るためのウェアラブルデバイス「BiometricJammer」を開発しています。



研究背景

自撮りや盗撮などで写り込んだ指先の画像から、指紋を復元できる場合があります。同時に写った顔や掲載されたコメントなどから指紋の持ち主を特定できるため、指紋の盗難や不正利用に対する懸念が高まっています。

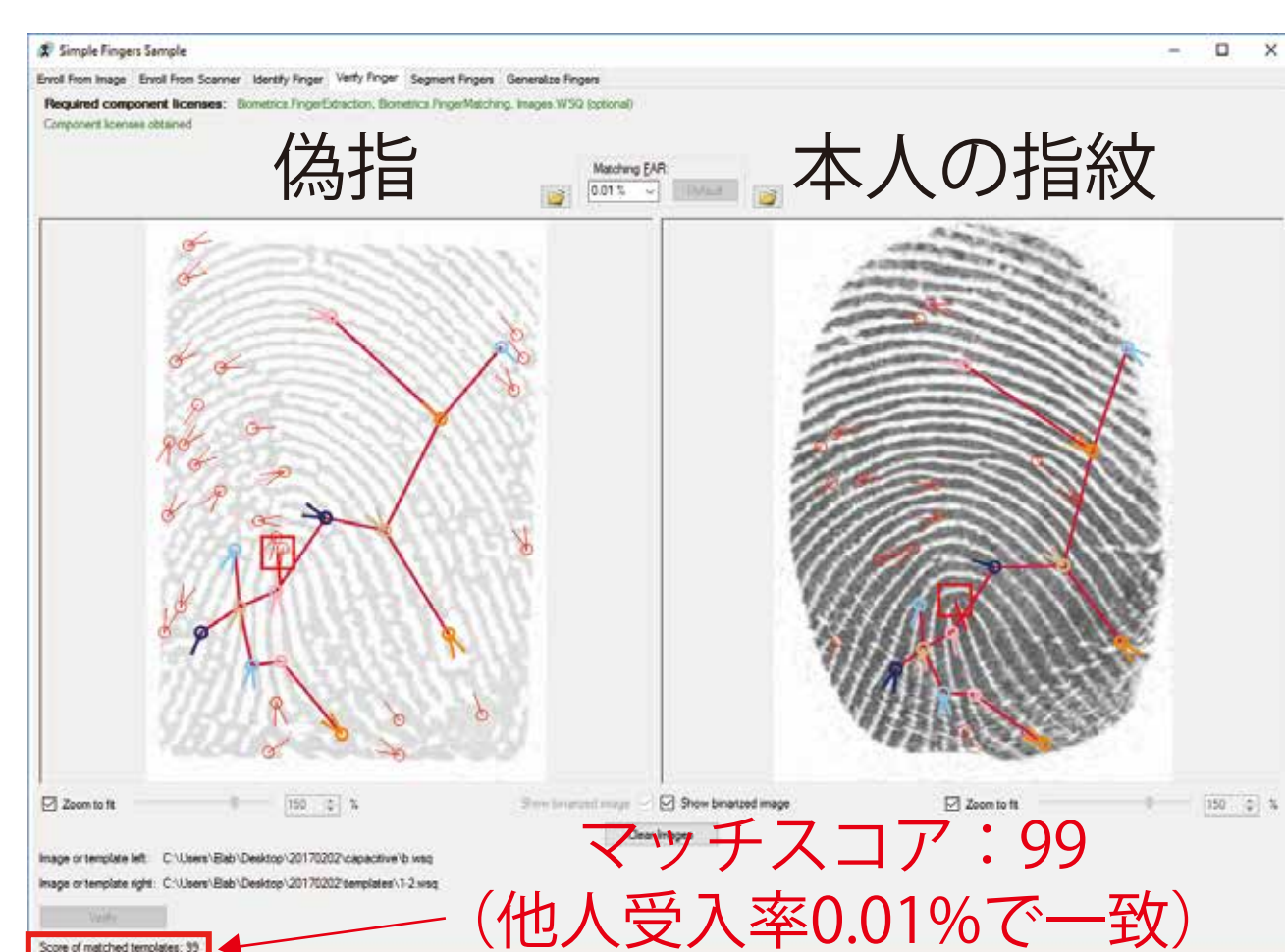


本当に写真から指紋を復元することができるのですか？

撮影画像（撮影距離5.4m）



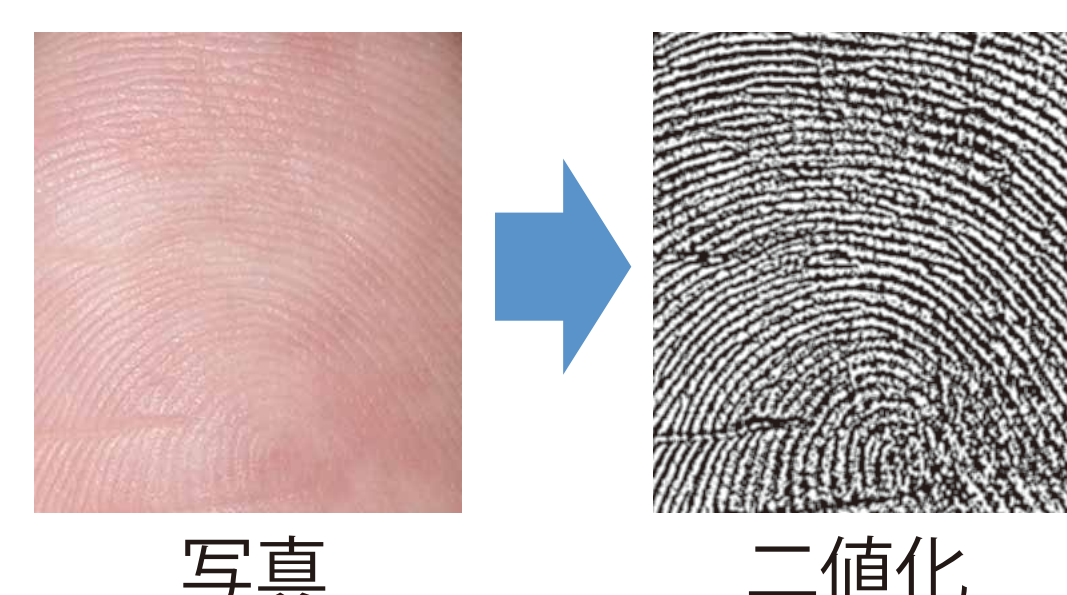
写真に写った指先に簡単な画像処理を施すことによって、指紋認証に十分な品質の指紋情報を得ることができます。それを使ってスタンプやシール状の「偽指」を作成すると、指紋認証システムに対するなりすましが可能になります。



指紋認証の原理（マニユージャ・マッチング）



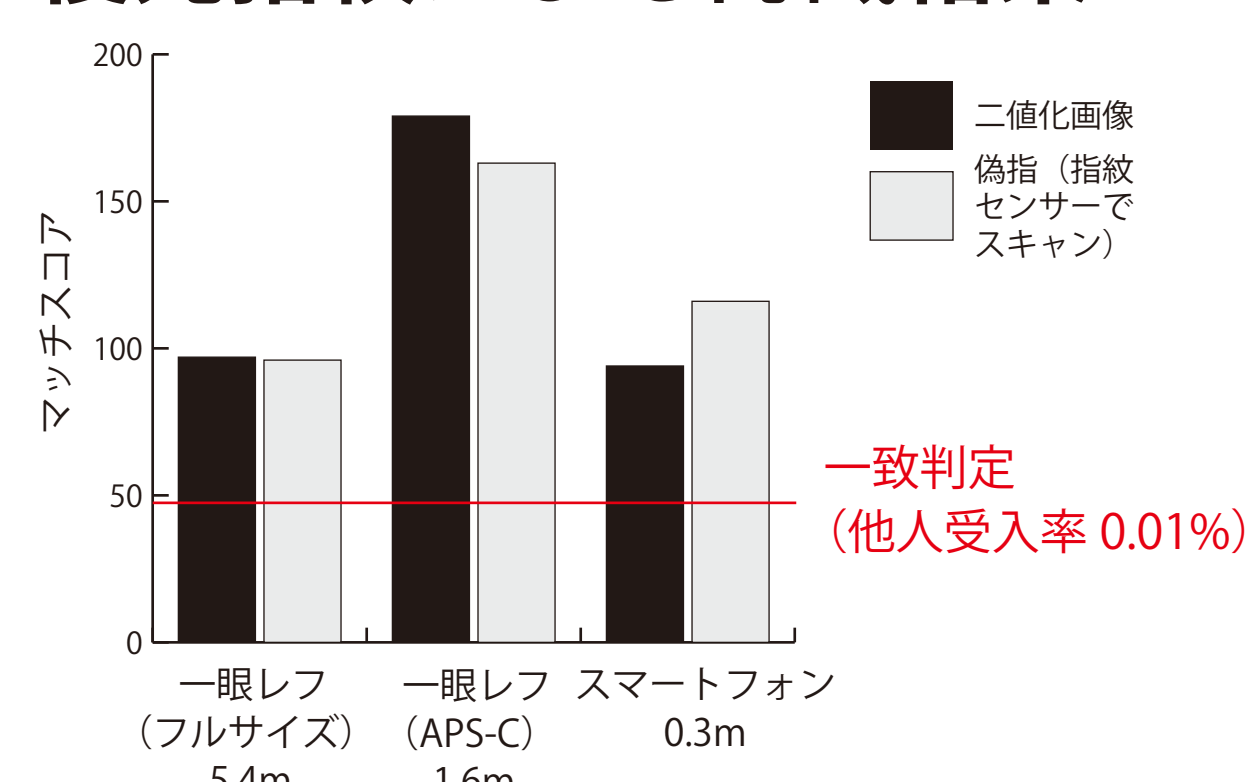
写真からの指紋復元



写真の解像度やコントラストの条件が適切ならば、適応的二値化によって指紋を復元することができる

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

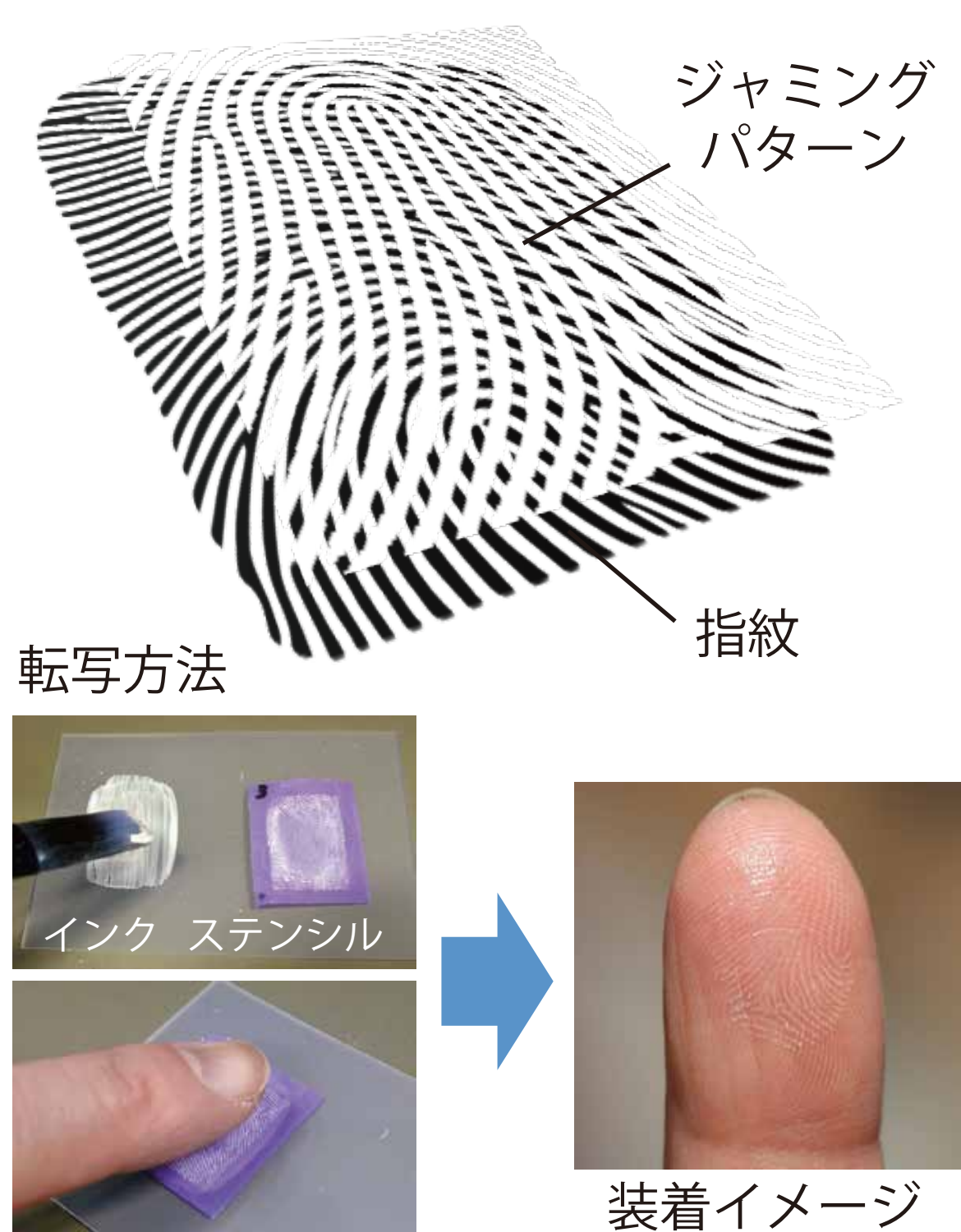
復元指紋による認識結果



指紋を復元できる条件

- ☑ 指先にピントが合う
 - ☑ 解像度が高い（1cmあたり200ピクセル以上）
 - ☑ コントラストが高い（日中屋外／強い照明下）
- 通常のスナップ写真では非常に困難

対策手法「BiometricJammer」とはどういうものですか？



光を反射する薄い素材で作られたジャミングパターンを指先に貼り付けることによって、接触式の指紋センサーには正しく反応しつつ、撮影された写真から指紋を復元できないようにします。

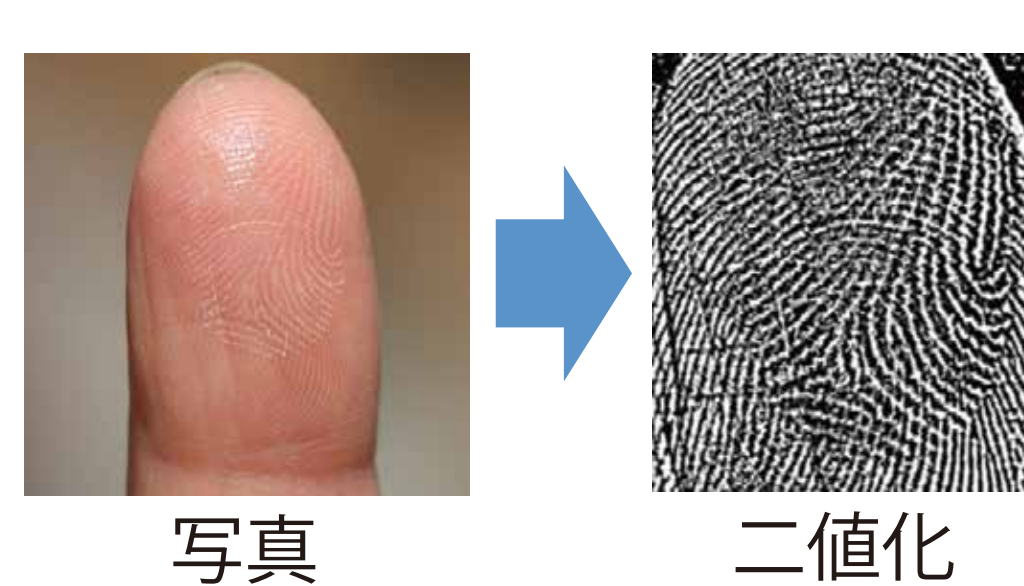
特許情報

特願 2017-51969「生体特徴盗撮防止装着具及び盗撮防止方法」（出願人：大学共同利用機関法人情報・システム研究機構、発明者：越前功、大金建夫）

特徴

- ☑ 写真から指紋を復元できない
- ☑ 通常の指紋認証が可能（接触式の指紋センサー）
- ☑ 目立たない
- ☑ しわが寄らない
- ☑ 装着したまま日常生活が可能

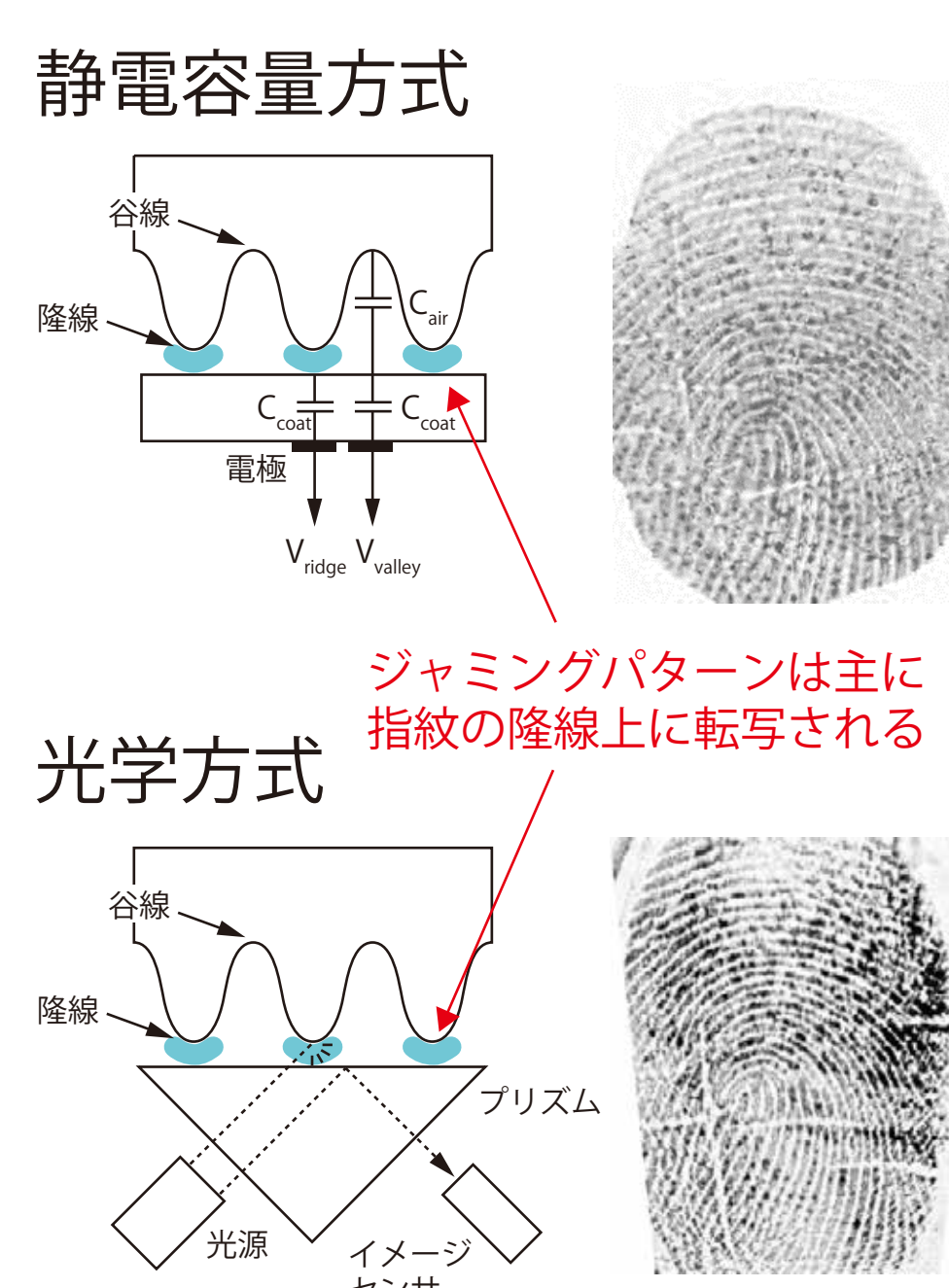
指紋復元の防止



本人の指紋にジャミングパターンを重畳することによって偽の特徴点を作り出す。

- プログラムによって作成された疑似指紋なので、パターン形状の予測が困難。
- 空間周波数が実際の指紋に近く、周波数分離による除去が困難。
- 半透明であるため、目視でも本人の指紋との識別が困難。

指紋センサーによる認識



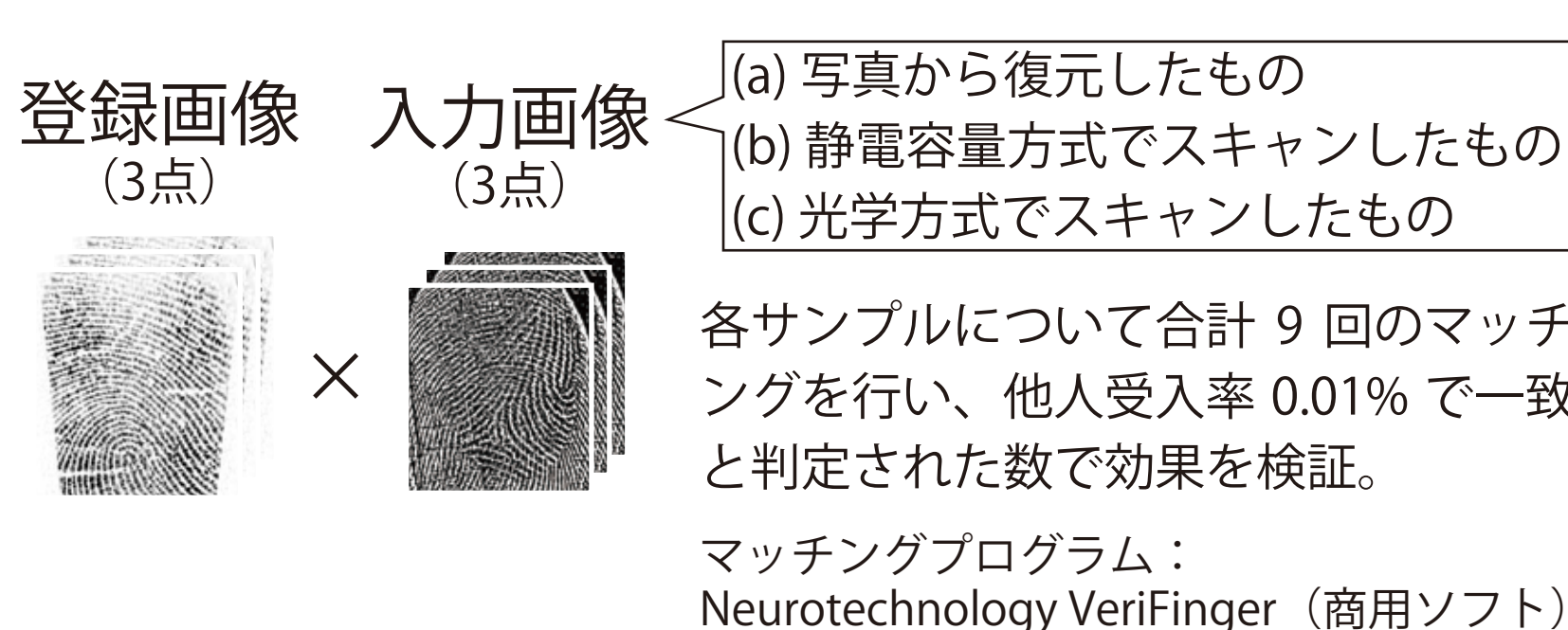
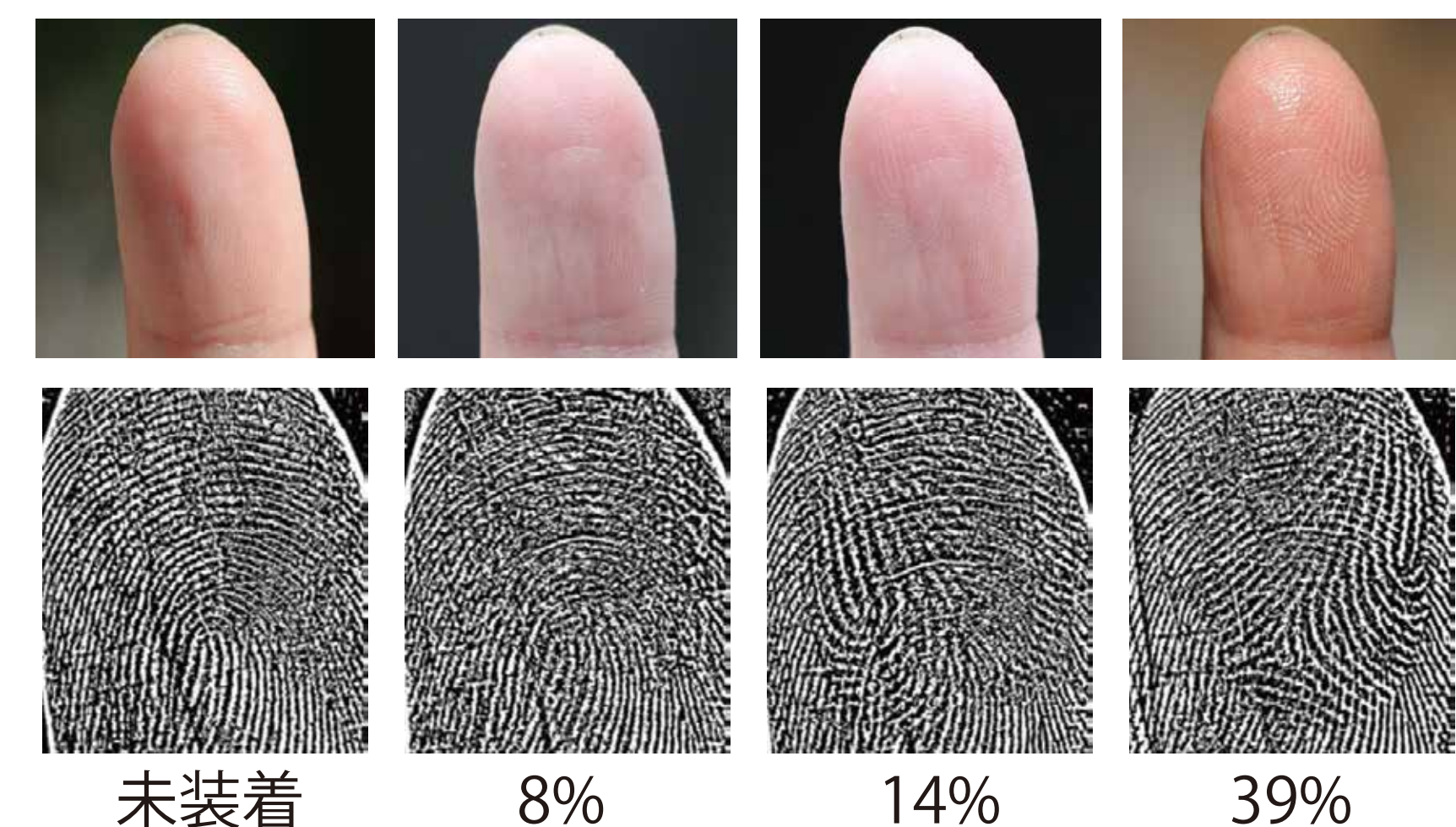
皮膚と電極間の距離に応じて異なる静電容量をピクセルの輝度に変換する。ジャミングパターンの素材は全体の距離を広げるだけなので、十分薄い場合は画質に影響しない（約0.05mm以下）。

光源からの光は、プリズムと空気層の境界で全反射するので、谷線で輝度が高くなる。ジャミングパターンの素材はプリズムに密着するので、谷線に転写されると画質が劣化する可能性がある（不透明度の調整によって回避可能）。

実際にどの程度の効果がありますか？

指紋復元の防止と指紋センサーによる認識という2つの要件を両立するため、ジャミングパターンの透明度を変えた複数のサンプルを作成し、効果的な設定を調査しました。

サンプル



マッチング結果

不透明度	写真	指紋センサー（静電容量方式）	指紋センサー（光学方式）
未装着	9	9	9
8%	9	9	9
14%	0	9	9
39%	0	9	6

指紋センサーでは全て認識
写真から復元した指紋は認識しない

CeBIT 2017に出展

3月20～24日にドイツ・ハノーバーで開催された国際情報通信見本市「CeBIT2017」において、「NII-BioSec：サイバー／フィジカル境界における生体情報保護」をテーマに研究成果を出展し好評を博しました。

