解 説

応
般

写真からの指紋復元の脅威とその対策技術

越前　功・大金建夫（国立情報学研究所）

カメラによる生体情報の取得

生体認証が普及し，PC やスマートフォンなど個人用の機器にも標準搭載されることが多くなっている．中でも指紋認証の普及は目覚ましく，スマートフォンにおける指紋センサ搭載機種の普及率は 2018 年には 2/3 を超えると予測されている☆1．一方で画像センサの高画素化も進み，従来接触式の指紋センサでしか読み取れなかった指紋情報を，遠隔から撮影し窃取される可能性が懸念されている．2014 年には，ドイツのハッカーが，市販のデジタルカメラで撮影されたドイツの国防相の指の写真から，指紋情報の復元に成功したという発表を行っている☆2．さらに，外部に露出していない虹彩，指静脈や手のひら静脈などの生体情報についても，小型で携帯可能な虹彩センサや静脈センサの普及により，当該センサを悪用すれば，当事者に気づかれない状態で，当事者の生体情報を窃取できる可能性がある（本稿を執筆している際にもデジタルカメラの夜間撮影モードを用いて虹彩情報の取得に成功したという発表があった☆3）．生体認証に用いられる生体情報は終生不変であるため，いったん漏えいしてしまうと，なりすまし攻撃（Presentation Attacks）の脅威となり，当事者の生涯にわたって大きな不利益をもたらす危険性がある．

図 -1 は 30cm の距離から，800 万画素のカメラを搭載したスマートフォンで撮影した筆者（越前）の写真と，その写真から復元した指紋情報である．このような写真は，自撮り写真やスナップ写真などでよく見られるピースサインをしたポーズであるが，指と顔が近接しているため，顔と同様に指紋にもフォーカスが合いやすく，復元した指紋情報から隆線と呼ばれる線状の隆起がはっきりと認識できる．さらに，このようなポーズで撮られた写真は指と顔が同時に写り込むため，顔識別技術によって SNS 上の顔画像などと照合することで，1 枚の写真から指紋情報とその持ち主の氏名や生年月日といった個人情報も取得できてしまう恐れがある．

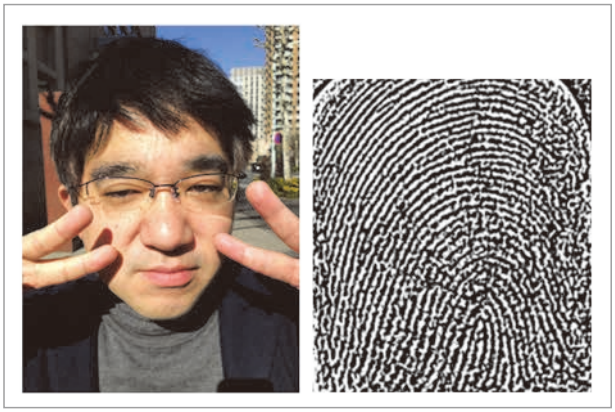
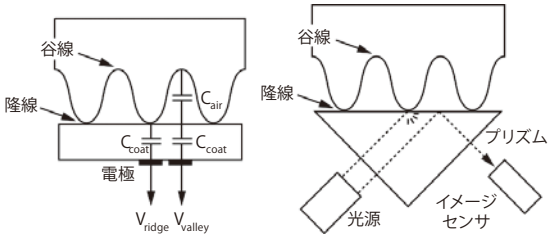


図 -1　30cm の距離からスマートフォンで撮影した筆者（越前）の写真とその写真から復元した指紋情報（左手中指）

本稿では，指紋照合の原理を概観した後，写真から照合可能なレベルで指紋情報が復元できることを示す．さらに，このような指紋情報の復元や復元した指紋情報を用いたなりすまし攻撃を防ぐための対策技術として，指への着用により撮影された指紋画像から指紋情報の復元を防止する指紋盗撮防止技術についても解説する．

☆1　クレディ・スイスによる調査（2016 年 1 月）．
☆2　https://www.ccc.de/en/updates/2014/ursel
☆3　https://www.ccc.de/en/updates/2017/iriden



（a）静電容量方式　（b）光学方式

図 -2　指紋センサの原理

（a）静電容量方式　（b）光学方式

図 -3　指紋センサで取得された画像の例

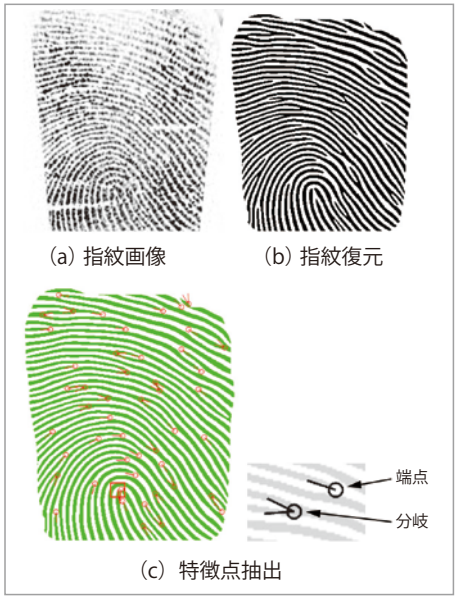
指紋照合の原理

現在広く使われている指紋センサの原理を**図 -2** に示す．静電容量方式の指紋センサ（図 -2（a））は，電極と皮膚の間の距離に応じて変化する電位差を測定し，ピクセルの輝度にマッピングする．一方，光学方式の指紋センサ（図 -2（b））は，プリズムを使った光の全反射条件の違いを利用し，反射光をピクセルの輝度にマッピングする．いずれも指紋の凸部が接触面に触れていることを物理的に識別するため，高いコントラストの指紋画像を得ることができる（**図 -3**）．

取得された指紋画像から指紋を認識する手法としては，マニューシャ・マッチングが主流である（**図 -4**）．これは，指紋画像から特徴点（マニューシャ）を検出し，その配置を比較することによって識別を行う．特徴点としては隆線の端点および分岐が利用される．

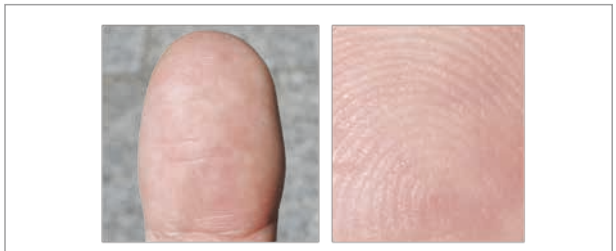
指紋画像にはノイズが多く含まれているため，特徴点の検出に先立って画像の強調処理を行う．抽出された特徴点は，x, y 座標および方向 t を用いて

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



（a）指紋画像　（b）指紋復元
（c）特徴点抽出

図 -4
マニューシャ・マッチング



（a）全体　（b）拡大図

図 -5　撮影された指紋画像の例

と表され，特徴点のリスト（指紋テンプレート）に保存される．指紋のマッチングは，これらの点群間のパターンマッチング問題とみなすことができる．

写真からの指紋復元の脅威

❖ 照合可能な指紋情報の復元

デジタルカメラで撮影された指紋画像の例を**図 -5** に示す．接触式の指紋センサと違って，デジタルカメラなどの光学デバイスは指紋の物理的な凹凸でなく陰影をサンプリングするため，撮影された画像における指紋はノイズを多く含みコントラストも低い．しかし，空間フィルタリングなどのノイズ除去技術を使うことによって，指紋センサで取得した指紋画像並みの画像を再現することができる．

ここでは，空間フィルタリングの一種である適応的二値化について説明する．あるピクセル (x,y) に

（a）k=3　（b）k=11

（c）k=99

図 -6　適応的二値化

おける閾値 $d(x, y)$ を，画素 $I(x, y)$ の局所正方領域 D における平均として

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

と表す．撮影された指紋画像に適応的二値化を施した結果を**図 -6** に示す．D の一辺の長さをカーネルサイズ k とすると，k が実際の隆線間隔（図では約 11 ピクセル）に近いとき，指紋の隆線が認識できることが分かる．

次に，写真から復元した指紋情報が指紋照合可能なレベルにあるのか，以下の簡易評価を行った．

4 名の被験者の指（右手親指）を 1m から 5m まで 0.5m 間隔でデジタルカメラにより撮影し，指紋センサによる取得画像と同等の解像度（約 500ppi）に拡大または縮小した後，カーネルサイズ k=11 として適応的二値化を行った．特徴点の抽出およびマッチングには商用の指紋照合ソフトウェアである Neurotechnology 社の VeriFinger を使用した．指紋センサ（静電容量方式）によりあらかじめ被験者から取得した登録画像と，異なる距離で撮影した指紋画像とのマッチングを行った．評価環境の詳細を**表 -1** に示す．

図 -7 に撮影距離ごとにマッチングに成功した人数（最大 4 人）を示す．図が示すように，2m 以下の距離ではすべての被験者でマッチングに成功し，一部の被験者では最長 3m の距離でマッチした．このことから撮影距離が 3m より近いケースにおいては，撮影された写真から指紋照合可能なレベルで指紋情報を復元することは困難ではないことが分かる．

デジタルカメラ	Canon EOS 70D（2020 万画素，ISO 感度自動，露出自動，1 点 AF）
レンズ	Canon EF-S 18-135mm F3.5-5.6 IS STM（焦点距離 135mm 固定）
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）
マッチングの条件	FAR（False Acceptance Rate）：0.01% 以下

表 -1　評価環境

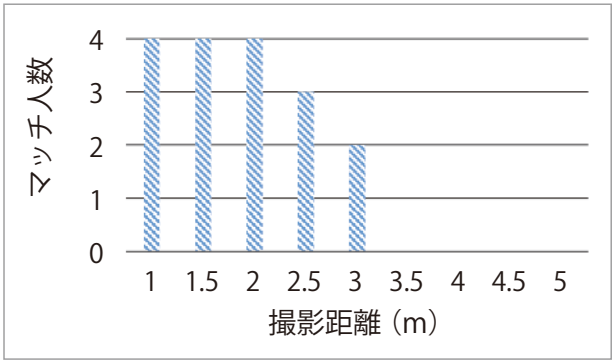


図 -7　撮影距離別のマッチ人数

さらに焦点距離が長い望遠レンズを用いることで，撮影距離が 3m より遠いケースにおいても指紋情報を復元できる可能性があるだろう．

なお，屋内などの暗所ではカメラの ISO 感度を高く設定して撮影する必要があり，その結果高感度ノイズが発生するため，今回の評価結果よりも指紋が復元可能な距離は短くなると予想される．

❖ 偽指を用いたなりすまし攻撃

指紋センサの入力時に，自身の指ではない偽の指（偽指）を用いることで，他人になりすます脅威は 2000 年頃から知られており，Putte ら [1] や松本ら [2] は，市販の指紋センサがシリコーンやゼラチンといった入手および造形が容易な素材で作られた偽指によって認証可能であることを報告している．最近では Cao ら [3] がインクジェットプリンタと導電性インクによって紙に印刷した指紋を使って最新のスマートフォンのロックを解除することに成功している．これまで偽指を作成するための指紋情報は，コップなどに付着した遺留指紋や，対象者の協力を得て入手した指紋を用いることを想定していたが，写真から偽指を作成したケースは筆者らの知る限り

図 -8　市販のスタンプ作成機による偽指の作成手順

存在しない．

そこで，筆者らは市販のスタンプ作成機を使って，写真から復元した指紋情報から偽指を作成し，指紋センサを通してなりすましが可能か簡易評価を行った．**図 -8** に写真から偽指を作成する手順を示す．図 -8（a）の撮影写真から図 -8（b）の適応的二値化画像の作成については，前節で述べた方法と同一である．図 -8（c）の偽指の作成については，市販のインクジェットプリンタを用いて透明なプラスチックシートに図 -8（b）の二値化画像を印刷してスタンプの原版とした．スタンプ作成機は紫外線を照射することで，原版の印刷されていない部分を透過してスタンプ素材の光硬化樹脂を部分的に硬化させる．硬化していない部分を水で洗浄することによって指紋の隆線および谷線をスタンプの凹凸として再現することができた．

図 -9 に作成した偽指と登録指紋との VeriFinger によるマッチング結果の例を示す．この偽指は，スマートフォンによる撮影写真（図 -1）から作成したものである．マッチング対象となる本人の指紋はあらかじめ指紋センサを使って登録を行い，登録時と同じ指紋センサによる偽指のスキャン画像を入力として，それらの間のマッチングを行った．図が示すように，双方の画像に共通な特徴点の配置が検出され（図の線分でつながれた図形），これらの画像から抽出された特徴点のパターンが類似していることが分かる．これは偽指の作成過程において画像のディテールが劣化しても，隆線の端点と分岐という特徴はそのまま維持されるためである．なおこの例では，FAR が 0.01% 以下の条件で本人の登録指紋とのマッチングに成功した．

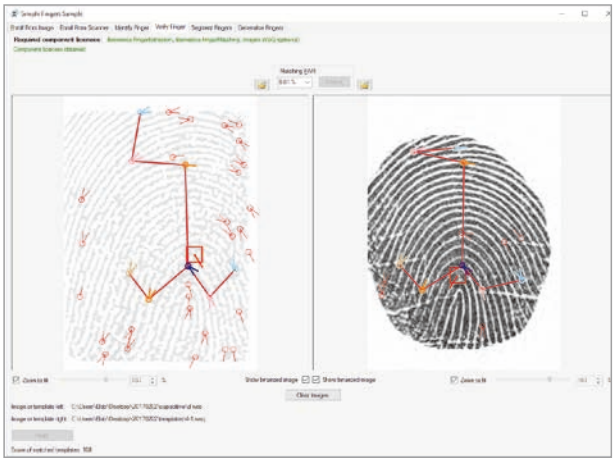


図 -9　VeriFinger によるマッチング結果（左：偽指のスキャン画像，右：本人指紋のスキャン画像）

写真からの指紋復元の対策技術

❖ 対策技術の概要

前章のように，写真から指紋照合可能なレベルで指紋情報を復元することは技術的に可能であり，このような脅威に対する対策が今後望まれる．単純な対策としては，手袋の着用が考えられるが，指紋認証の際に手袋を外さなければならず，ユーザの利便性を損なう．別の対策として，指紋センサに生体検知技術☆4 を導入することで，偽指によるセンサへの入力を防ぐ方法が考えられるが，多様な偽指に対する有効性やコスト面での問題があり，普及には至っていない．

そこで，筆者らは以下の要件を満たす対策技術を検討した．

(1) 指に着用することで撮影された指紋画像と登録指紋との照合ができない
(2) 一方で，指に着用しても接触式の指紋センサを経由すれば登録指紋との照合は可能

上記を満たす手段を検討した結果，指へジャミングパターンを装着する手法を提案した[4]．**図 -10** に提案手法の概要を示す．これは可視光領域において光を反射する素材で作られた，装着可能なジャミングパターンである．素材はある程度の透明度を持ち，実際の指紋と比較して違和感のない見た目を与える．

☆4 たとえば，指の血流の有無や変化を検知する生体検知方法が提案されている．

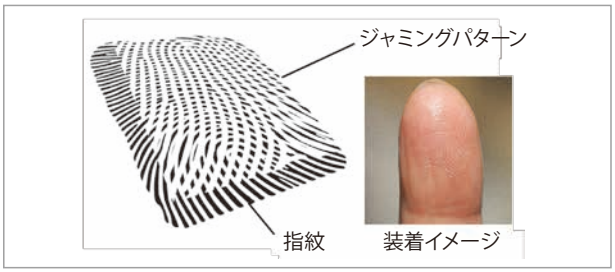


図 -10　提案手法の概要


図 -11
シルクスクリーンによる転写イメージ

また，パターンの形状は機械によって作成された疑似指紋である．このような構成によって，撮影された写真において，本人の指紋と疑似指紋との識別を困難にする．

指先という立体形状に隙間なく貼り付け，また指の弾性変形に追従するためには，装着時に液体であり，その後乾燥してゲル化する素材が望ましい．具体的な素材の候補としては，シリコーンゴム，ラテックス，医療用人工皮膚等が挙げられる．

素材を指先に転写する手段としては，印刷などで利用されるシルクスクリーン方式を採用した．これは液状の素材に重ねたスクリーンに指を押し付けることにより，スクリーンに開けられた微小な穴を通して素材を転写する方式である（**図 -11**）．高解像度（約 300ppi）の疑似指紋パターンに対応し，素材により数マイクロメートル～ 100 マイクロメートルの膜厚を実現できるが，素材の粘度に応じて目詰まりやにじみが発生し，取り扱いは難しい．また押し付ける指の圧力が人によって異なるため，転写されるジャミングパターンの太さが安定しない問題があり，今後の課題となっている．

❖ ジャミングパターンの効果

提案手法による写真撮影時の妨害効果を**図 -12** に示す．上段は提案手法，下段は筆者らが昨年 10 月

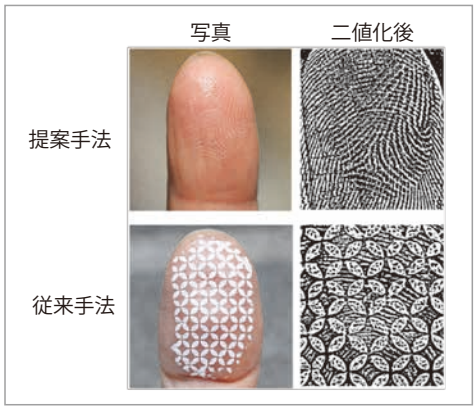


図 -12
ジャミングパターンの効果

に提案した従来手法[5]である．従来手法では幾何学パターンのエッジが強調されることによって指紋の特徴点が隠蔽されるのに対し，提案手法では本人の指紋に疑似指紋パターンを重畳することによって新たな偽の特徴点を作り出す．従来手法では重畳された幾何学パターンは周期的であり，周波数分離によるパターン除去や，パターンの部分を皮膚の色で塗りつぶすことで妨害効果を弱める攻撃手法が予想される．一方，提案手法では重畳されたパターンが疑似指紋であり，その素材は半透明であるため，本人の指紋と疑似指紋を識別することが困難である．なお，ジャミングパターンのデザインに関しては以下の点に注意する必要がある．

- ジャミングパターンは疑似指紋のような複雑な形状であることが望ましい．周期的な幾何学形状だと，従来手法と同様にパターンの予測に基づく無効化攻撃が可能になる．
- ジャミングパターンは装着するたびに異なるパターンであることが望ましい．疑似指紋でも繰り返し同一のパターンが使われていれば，同じジャミングパターンを装着した複数の異なる指の指紋画像を比較することで，共通のパターンを推測することが可能になり，指紋画像からジャミングパターンを除去できてしまう可能性がある．
- ジャミングパターンの空間周波数は，周波数分離などによるパターンの無効化を困難にするため，実際の指紋の空間周波数に近いことが望ましい☆5．

☆5　指紋の隆線間隔は約 0.4 ミリメートル程度といわれている．

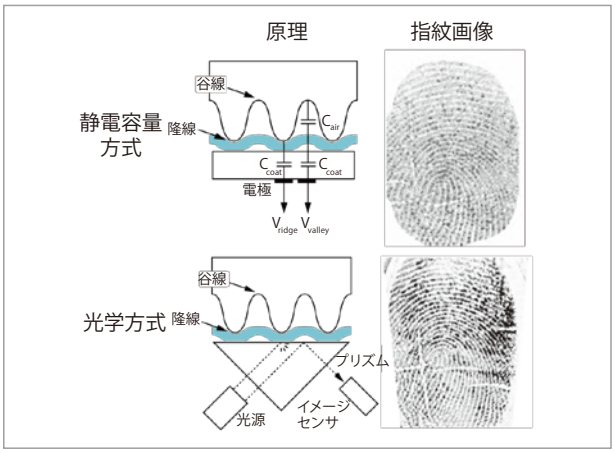


図 -13　指紋センサにおけるジャミングパターンの影響

❖ 指紋センサによる認識

接触式の指紋センサによる指紋の読み取りに対するジャミングパターンの影響を**図 -13** に示す．シルクスクリーンによる転写方式では，ジャミングパターンは主に指紋の隆線上に転写される．

静電容量方式の指紋センサでは，電極と皮膚の間の距離を測定するため，ジャミングパターンの存在は隆線と谷線の区別にほとんど影響しない．なお，転写されるパターンの厚みが増加すると取得イメージの品質が低下する．筆者らが複数の静電容量式指紋センサで検証した結果，厚さ 0.05 ミリメートル以下であれば良好な指紋画像を取得できることを確認した．

光学方式の指紋センサでは，空気層の有無によって隆線と谷線を区別するため，接触面に密着している個所すべてが暗線（隆線）となる．もしジャミングパターンが指紋の谷線に転写されると，素材が接触面に吸着し，本来の谷線が暗線として検出される．ただしジャミングパターンは指紋の谷線上ではやや窪み，接触面との間にわずかな隙間があれば明線となるため，ジャミングパターンを薄くすることによってこの影響を低減することができる．図 -13 が示すように，両方式の指紋センサとも取得画像には疑似指紋による偽の特徴は見られないため，登録指紋との指紋照合に影響はない．

今後の課題

バイオメトリクス技術が発達し，生体情報を個人の識別や認証に活用することにより，私たちの生活に利便性や安全性をもたらす一方，生体情報を不正に窃取され悪用されるリスクもまた増大している．今回筆者らは，意図しない写真撮影による指紋の窃取という問題に着目し，ユーザの利便性を確保しつつ指紋の不正な取得を防止する技術を提案した．

個人の識別や認証に使われる生体情報としては指紋のほかに虹彩や指静脈，手のひら静脈，歩容，顔，音声などがある．今後は生体情報ごとの特徴に合わせた意図しない取得や流通を防止する技術の確立が望まれる．

参考文献

1) van der Putte, T. and Keuning, J. : 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).
2) Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S. : Impact of Artificial “Gummy” Fingers on Fingerprint Systems. in Proc. of SPIE, Vol.4677, pp.275-289 (2002).
3) Cao, K. and Jain, A. K. : Hacking Mobile Phones Using 2D Printed Fingerprints, MSU Technical Report, MSU-CSE-16-2 (2016).
4) 国立情報学研究所ニュースリリース，2017 年 3 月 17 日，http://www.nii.ac.jp/news/release/2017/0317.html
5) 大金建夫，越前　功：ユーザの利便性を考慮した指紋の盗撮防止手法，情報処理学会コンピュータセキュリティシンポジウム 2016（CSS2016）論文集 , pp.355-362（2016 年 10 月）.

(2017 年 6 月 1 日受付)

越前　功（正会員） iechizen@nii.ac.jp

1997 年東工大大学院修士課程修了．日立製作所システム開発研究所を経て，現在，国立情報学研究所 所長補佐．同研究所 情報社会相関研究系 研究主幹／教授．博士（工学）．

大金建夫　oogane@nii.ac.jp

2011 年より国立情報学研究所にて映画盗撮防止技術，顔検出防止技術，生体情報盗撮防止技術の実装および評価を担当．現在，国立情報学研究所 特任専門技術員．