

掌紋認証における生体検知手法に関する一検討

杉本 彩歌¹ 上松 晴信² 奥井 宣広²
大木 哲史¹ 三宅 優² 西垣 正勝¹

概要：多くのスマートフォンには他人による不正使用を防止するために生体認証機能が搭載されている。身体的特徴の1つとして掌紋を利用した認証方式が提案されている。掌紋は、スマートフォンのカメラなどで特徴が取得できるため、特別な装置を必要せずに認証が行える、一方で、ユーザがSNSなどに掲載した自身の写真などをもとに、なりすましが行われる可能性がある。本稿では、スマートフォンで撮影を行う掌紋認証におけるプレゼンテーション攻撃に対する生体検知手法を検討する。身近な媒体を用いたなりすましを想定し、印刷画像ならびにディスプレイ表示画像を用いた攻撃を考える。攻撃画像（印刷画像やディスプレイ画像）においては、インクの滲みによる解像度の劣化、攻撃画像の撮影によるモアレ（干渉縞）が生じるという特徴に注目した。

A liveness detection method for palm print authentication

AYAKA SUGIMOTO¹ HARUNOBU AGEMATSU² NORIHIRO OKU²
TETSUSHI OHKI¹ YUTAKA MIYAKE² MASAKATSU NISHIGAKI¹

1. はじめに

今やスマートフォンは各ユーザが1人1台以上を所有するに至っており、スマートフォンを利用してオンラインショッピングやネットバンキングが日常的に行われている。それに伴いスマートフォン内にクレジットカード情報や電子マネー情報などの重要な情報が保存されるようになった。スマートフォンには様々なセキュリティ機能が搭載されている。一般的に利用されている個人認証として、パスワードやPINがある。これらの認証は、記憶を用いた認証方式であり、忘却や盗難の恐れがある。また、スマートフォンはキーボード持たないため、パスワードを入力させるという操作は利便性が低い。このような理由から、指紋認証や顔認証など生体認証によるセキュリティ機能が搭載されたスマートフォンが普及している。

本稿では、数多く存在する生体認証のモダリティの中から、掌紋を用いた認証に注目する。掌紋は、スマートフォンなどのデジタルカメラを用いて非接触での特徴の取得が可能である。一方でSNSなどに掲載された写真から不正者が掌紋情報を取得可能であるという問題点がある（写真から指紋の取得が可能である[1][2]以上、掌紋も同様に可能であると言えよう）。そこで本稿では、スマートフォンで撮影した掌紋画像を用いた生体認証における生体検知手法について検討する。その第一歩として、一般的な攻撃者（身近な媒体を用いたプレゼンテーション攻撃）を想定し、掌紋画像を印刷した普通紙、掌紋画像を印刷した光沢紙、掌紋画像を表示したディスプレイを用いたなりすまし

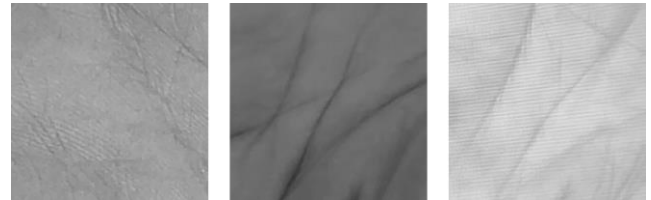


図 1 攻撃画像の掌紋領域
(右：普通紙，中央：光沢紙，左：ディスプレイ)

に対し、簡素な画像処理（エッジ検出，2 値化，自己相関）のみによって、どの程度の生体検知が可能となるのか調査する。

2. 緒言

2.1 攻撃方法

本稿では、身近な媒体を用いたプレゼンテーション攻撃を想定する。今回は、普通紙、光沢紙、ディスプレイを考える。なお、印刷に用いられるプリンタ、表示に用いるディスプレイも一般的に普及している市販品を用いる。

それぞれの媒体に対し、生体検知の観点からの特徴を以下に記す。

- 普通紙

普通紙にプリンタのインクが噴霧された際に、インクが滲む。これにより「普通紙に印刷された掌紋画像（以下、普通紙攻撃画像）」は「本物の掌をスマートフォンのカメラで撮影した際の掌紋画像（以下、実物画像）」よりも解像度が劣化することになる。

¹ 静岡大学
Shizuoka University
² 株式会社 KDDI 総合研究所
KDDI Research, Inc.

- 光沢紙

光沢紙の場合はインクの滲みはわずかであるため、紙面に微細なインクの粒子が規則正しく並んでいる状態となる。一方、デジタルカメラも撮像素子が規則正しく並んでいる構造となっている。このため、「光沢紙に印刷された掌紋画像（以下、光沢紙攻撃画像）」をスマートフォンのカメラで撮影した場合には、部分的にモアレ（干渉縞）が生じた画像が得られる。

- ディスプレイ

ディスプレイは発光素子が規則正しく並んだ構造となっている。このため、光沢紙の場合と同様、「ディスプレイに表示された掌紋画像（以下、ディスプレイ攻撃画像）」をスマートフォンのカメラで撮影した場合には、全体的にモアレ（干渉縞）が生じた画像が得られる。

図 1 に各攻撃画像の例を示す。今回は攻撃画像のサイズを 300×300 pixel としている。本稿では、上記の攻撃画像と実物画像の差異を検出するための画像処理について調査を行う。

2.2 生体認証と生体検知

本稿では、掌紋認証の前処理あるいは後処理として生体検知を行うことを想定する。生体認証と生体検知の両方にパスした掌紋画像のみが本人の掌紋として受理される。生体認証に要する時間が生体検知に要する時間よりも早い場合は、生体認証の後処理として生体検知を行うほうが効率的であり、生体検知に要する時間が生体認証に要する時間よりも早い場合は、生体認証の前処理として生体検知を行うほうが効率的である。

本稿では、4.1 節に後述するように、調査実験のために収集した攻撃画像のデータセットの品質が低かったため、生体認証を先に適用することとする。生体認証によって事前に実験対象となる掌紋画像を絞ることによって、実験を簡素化することが目的である。

3. 画像処理

3.1 Sobel フィルタ

Sobel フィルタは 1 次微分フィルタである[4]。2.1 節で述べたように、普通紙攻撃画像には、解像度劣化により実物画像よりも掌紋のエッジが若干不鮮明になるという特徴がある。光沢紙攻撃画像およびディスプレイ攻撃画像には、モアレにより実物画像の掌紋には存在しないエッジが映るという特徴がある。そのため、Sobel フィルタによってエッジ検出を行うことでこれらの特徴を顕著にする。

実物画像および攻撃画像に対し、X、Y 両方向からカーネルサイズ $K=7$ の Sobel フィルタを適用する。更に、フィルタ後の画像を 2 値化することでエッジ強調を実現する。2 値化にあたっては、全画素に対して共通の閾値を用いて 2 値化を行う方法と、局所領域ごとに閾値を設定して 2 値

化（大津の 2 値化[5]）を行う方式の 2 種類を試行する。以下、Sobel フィルタを適用した結果に対して共通閾値による 2 値化を行う方法を処理①、Sobel フィルタを適用した結果に対して大津の 2 値化を行う方法を処理②とする。処理①および処理②を適用した結果の画像例を図 2 に示す。

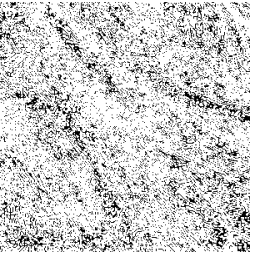
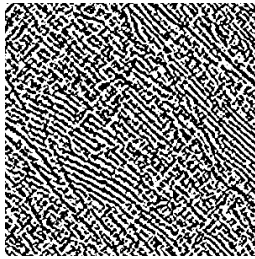
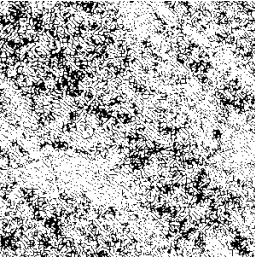
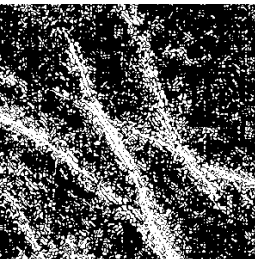
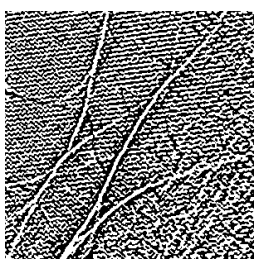
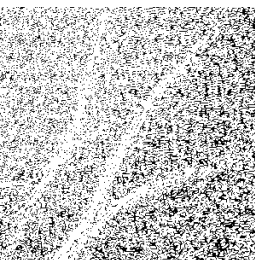
	処理①	処理②
本物		
普通紙		
光沢紙		
ディスプレイ		

図 2 Sobel フィルタを適用した結果

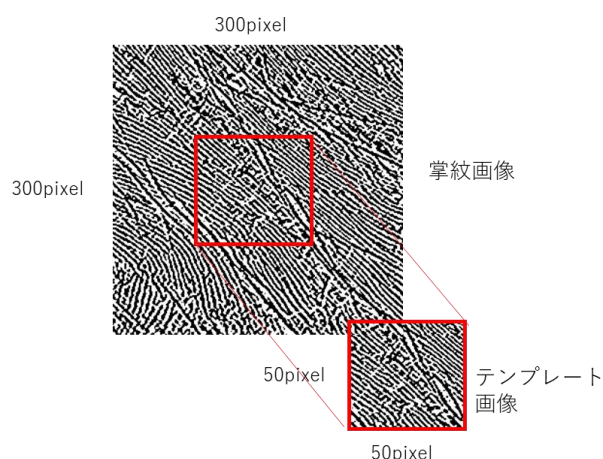
3.2 自己相関

図 2 の処理①の画像から、普通紙攻撃画像においては鮮明度が若干低下していることが、光沢紙攻撃画像においては掌紋の模様が崩れていることが、ディスプレイ攻撃画像においては横方向のモアレ線が生じていることがわかる。今回は、これらを検知するために、自己相関を利用することを考える。具体的には、画像の中心 50×50 pixel の領域をテンプレートとして、X 方向に 1 pixel ずつずらした領域との誤差（輝度の差の 2 乗和）を計算する（図 3）。

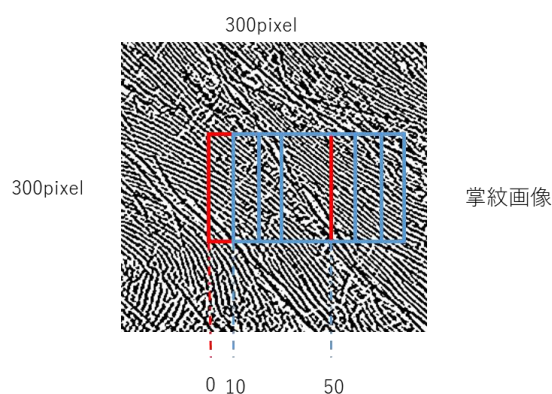
普通紙攻撃画像においては、鮮明度が若干低下している

ことから、実物画像と比べて、自己相関が高くなる（誤差は小さくなる）ことが期待される。光沢紙攻撃画像においては、模様が雑然となっていることから、実物画像と比べて、自己相関が高くなる（誤差は小さくなる）ことが期待される。ディスプレイ攻撃画像においては、横方向のモアレ線が生じていることから、自己相関が周期的に高くなる（誤差は小さくなる）ことが期待される。

処理②の画像に対しても、同様に自己相関を計算する。



手順 1：掌紋画像の中央を切り出しテンプレート画像とする



手順 2：テンプレートをX方向に10pixelから50pixelまで1pixelずつずらした領域との誤差を計算していく

図 3 自己相関を求める方法

3.3 生体検知手順

掌紋認証を行った後に生体検知を行う場合の生体検知手順を説明する。

- I. 掌をスマートフォンのカメラで撮影する
- II. 掌紋領域を抽出することによって掌紋画像を作成する
- III. 掌紋認証[3]を行う

IV. 認証に成功した掌紋画像に対して Sobel フィルタを適用し、2 値化を行うことによって処理①、処理②の画像を作成する

V. 処理①、処理②の画像の自己相関を求める

4. 実験

掌紋認証においては、Sobel フィルタや自己相関を利用した簡素な画像処理によって、どの程度の生体検知が達成されるのかを確認するために予備実験を行った。

4.1 データセット

実物の掌を撮影することによって実物画像を用意した。実物画像を市販のプリンタで普通紙に印刷し、それを撮影することによって普通紙攻撃画像を用意した。同様に、実物画像を市販のプリンタで光沢紙に印刷し、それを撮影することによって光沢紙攻撃画像を用意した。更に、実物画像を市販のタブレット端末に表示し、それを撮影することによってディスプレイ攻撃画像を用意した。それらの緒言を表 1 に記した。画像の撮影（3.3 節の手順 I に該当）には LG エレクトロニクス社の Nexus 5 に内蔵されているデジタルカメラを用いた。撮影画像からの掌紋領域の抽出（3.3 節の手順 II に該当）については、今回は、実験実施者（著者）が目視にて行った。掌紋領域は 300×300 pixel とした。

今回、調査実験のために用意した実物画像、攻撃画像のデータセットは品質が低い状態であった。そこで今回は、実験を簡素化することを優先し、生体検知を生体認証の後処理として適用することとした。掌紋認証を事前に適用して、認証を通過しない画像については実験対象から除外することによって、生体検知実験の対象となる掌紋画像の総数が絞られる。今回は、実験実施者（著者）が表 1 の画像セットを目視で検査し、掌紋が映っていない画像、ピントの合っていない画像を「掌紋認証を通過しない画像」として除外した（3.3 節の手順 III に該当）。表 1 には、掌紋認証を通過した画像数についても併記してある。今回のデータセットにおいては、光沢紙攻撃画像とディスプレイ攻撃画像の中に掌紋認証を通過する画像は存在しなかった。

掌紋認証を通過した画像に対して Sobel フィルタ、2 値化を適用して、処理①および処理②の画像を生成した（3.3 節の手順 IV に該当）。更に、各画像の自己相関スコアを計算した（3.3 節の手順 V に該当）。

表 1 実験に使用した掌紋画像

画像の種別	印刷／ディスプレイの解像度	画像の総数	掌紋認証を通過した画像数
本物	—	400 枚	104 枚
普通紙	2400×1200dpi	380 枚	27 枚
光沢紙	9600×2400dpi	221 枚	0 枚
ディスプレイ	1080×1920pixel	400 枚	0 枚

4.2 結果

3.3 節の手順 V の時点で、テンプレート画像を X 方向に 10 pixel から 50 pixel まで 1 pixel ずつ平行移動させながら、それぞれの画像領域とテンプレート画像との誤差を計算した。図 4～図 7 に、処理①および処理②の実物画像、攻撃画像のそれぞれの誤差の変化をグラフ化して示す。なお、図 4～図 7 においては、視認性に鑑み、それぞれ特徴的な画像の結果のみを選んで描画してある。

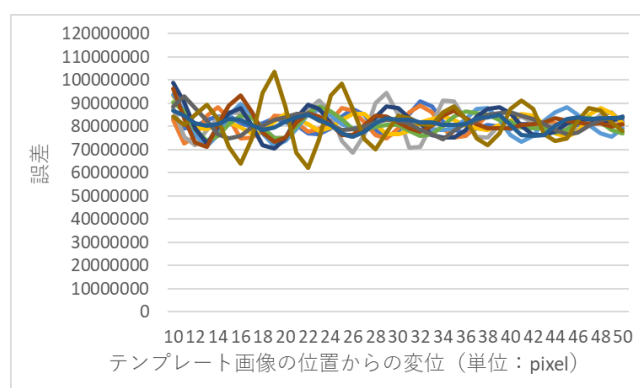


図 4 処理①の実物画像の自己相関

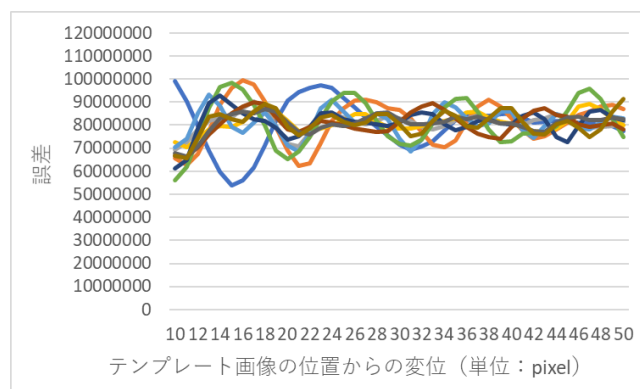


図 5 処理①の普通紙攻撃画像の自己相関

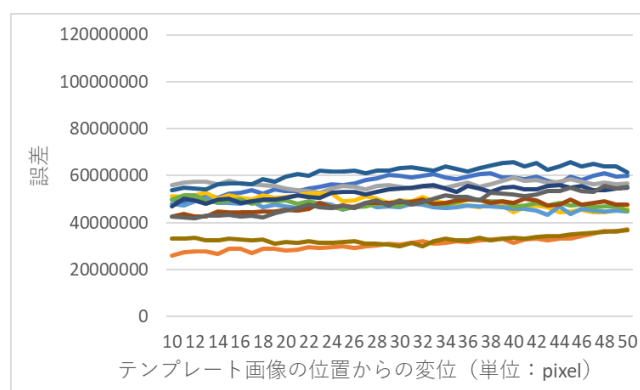


図 6 処理②の実物画像の自己相関

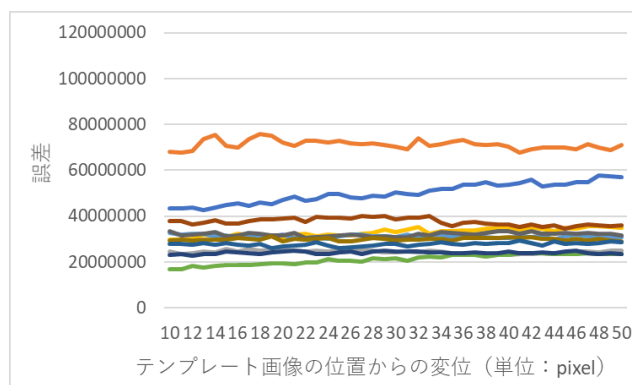


図 7 処理②の普通紙攻撃画像の自己相関

4.3 結果

図 4 および図 7 から、処理①の画像に関しては、閾値を 70000000 として、自己相関スコアグラフの最小値が閾値より高い画像を実物画像と判断するという方法を採用できる可能性がある。このとき、表 2 のようになる。

表 2 処理①の画像の自己相関スコアに基づく生体検知を行った結果

画像の種別	画像の総数	掌紋認証を通過した画像数	生体検知を通過した画像数
本物	104 枚	73 枚	31 枚
普通紙	27 枚	7 枚	20 枚

図 6 および図 7 から、処理②の画像に関しては、閾値を 40000000 として、自己相関スコアグラフの最大値が閾値より高い画像を実物画像と判断するという方法を採用できる可能性がある。このとき、表 3 のようになる。

表 3 処理②の画像の自己相関スコアに基づく生体検知を行った結果

画像の種別	画像の総数	掌紋認証を通過した画像数	生体検知を通過した画像数
本物	104 枚	92 枚	12 枚
普通紙	27 枚	10 枚	17 枚

表 2 の検査と表 3 の検査を併用し、AND 型の融合判定による実物画像の生体検知を行うとすると、表 4 のようになる。

表 4 処理①, ②の画像の自己相関スコアに基づく生体検知の融合 (AND) 判定を行った結果

画像の種別	画像の総数	掌紋認証を通過した画像数	生体検知を通過した画像数
本物	104 枚	69 枚	35 枚
普通紙	27 枚	5 枚	22 枚

5. おわりに

スマートフォンで撮影した画像を用いた掌紋認証に対し、簡素な画像処理に基づく生体検知の可能性について調査した。その第一歩として、一般に普及しているプリンタでの印刷物やディスプレイを用いたプレゼンテーション攻撃を想定し、Sobel フィルタと自己相関を利用した生体検知に関する実験を行った。

本稿は、まだ、生体検知に利用可能な画像処理や特徴量を検討した段階であり、未学習サンプルを対象とした評価実験に至っていない。また、掌紋領域の抽出や掌紋認証の実行に関する処理も手動で行っていた。今後、これらの観点から調査ならびに検討を更に深めていくことを予定している。

参考文献

- [1] 大金建夫, 越前功: BiometricJammer: ユーザの利便性を考慮した指紋の盗撮防止手法, コンピュータセキュリティシンポジウム 2016 (CSS2016) 論文集, vol.2016, no.2, pp.355-362 (2016)
- [2] Chaos Computer Club: Fingerprint biometric hacked again (online), <https://www.ccc.de/en/updates/2014/ursel> (参照 2016-08-02)
- [3] 上松晴信, 神田龍一, 松井利樹ほか: 指間の線を利用した掌紋認証の提案, コンピュータセキュリティシンポジウム 2016 (CSS2016) 論文集, vol.2016, no.2, pp.185-191 (2016)
- [4] デジタル画像処理編集委員会 (監修): デジタル画像処理, pp.116-117, 画像情報教育振興協会 (CG-ARTS 協会) (2004)
- [5] 大津展之: 判別および最小 2 乗基準に基づく自動しきい値選定法, 電子情報通信学会論文誌 D, vol.J63-D, No.4, pp.349-356 (1980)