一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

バイオメトリクス研究会資料
Proceedings of Biometrics Workshop
BioX2013-16 (2013-08)

生体認証装置に対するなりすまし攻撃とその安全性評価法について

大木　哲史† 　大塚　　玲† 　寶木　和夫†

† 産業技術総合研究所 セキュアシステム研究部門
茨城県つくば市梅園 1-1-1
E-mail: †{tetsushi.ohki,kazuo.takaragi}@aist.go.jp, ††otsuka@ni.aist.go.jp

あらまし　近年，シリコン等の非生体素材に指紋の凹凸を付けた擬似生体や手術等により生体の一部を移植した生体を提示することにより，生体認証装置を騙してなりすます行為が可能なことが論文等で発表され，これを悪用した事件も生じている．本稿では，生体認証装置における脆弱性と，多様化する生体認証装置に対するなりすまし行為 (Presentation Attacks) の現状に関して，研究動向や標準化動向を交えて報告する．

キーワード　バイオメトリクス，プレゼンテーション攻撃，なりすまし，生体検知，偽造生体

A Survey on Biometric Presentation Attack and It's Security Evaluation Method

Tetsushi OHKI†, Akira OTSUKA†, and Kazuo TAKARAGI†

† Research Institute for Secure Systems (RISEC), National Institute of Advanced Industrial Science and Technology (AIST)
1-1-1 Umezono, Tsukuba city, Ibaraki 305-8568 JAPAN
E-mail: †{tetsushi.ohki,kazuo.takaragi}@aist.go.jp, ††otsuka@ni.aist.go.jp

Abstract　In recent days, many papers have proposed impersonation attacks on biometric sensors that use fake biometric samples, which are called 'biometric presentation attacks'. In those papers, the fake biometric samples are made by non-living body materials such as silicon or transplanted from a part of other biometric samples. In actuality, the number of crimes that use fake biometric samples is increasing. In this paper, we discuss the research trends and the standardization trends of the biometric presentation attacks.

Key words　biometrics, presentation attack, spoofing, liveness detection, fake biometric sample

1. はじめに

本稿では，生体認証装置における脆弱性と，多様化する生体認証装置に対するなりすまし行為 (Presentation Attacks) の現状に関して，研究動向や標準化動向を交えて報告する．

生体認証が普及するにつれ，より安全な生体認証システムを構築する重要性が高まってきている．従来は本人拒否率や他人受入率といった認証精度を安全性の評価基準とすることが一般的であったが，近年では認証精度だけでなく，ネットワークを介した生体認証システム (リモート生体認証) までを対象とし，入力される生体情報の安全性から，伝送路上や保管される生体情報の安全性といった，より多くの脅威に対応した安全性が求められている．これらのうち，伝送路上や保管される生体情報の安全性は，テンプレート保護型生体情報の枠組みで捉えられ，多くの研究が進められている [1], [2].

テンプレートが漏洩することによる最大の脅威は，漏えいしたテンプレートから本人の生体情報が復元され，それらから複製された偽造生体情報により，不正なりすましが行われることである．生体情報の複製とそれを用いた不正なりすましに関しては，近年シリコン等の非生体素材に指紋の凹凸を付けた擬似生体や手術等により生体の一部を移植した生体を提示することにより，生体認証装置を騙してなりすます行為が可能なことが論文等で発表され [3], [4]，これを悪用した事件も生じている．また，このような事件を背景に，電子認証ガイドライン (NIST SP800-63 [5]) では，信頼できないネットワークにおける無人のアプリケーションにおける認証要素としてバイオメトリクスを利用することを推奨していない．これは，バイオメトリクスが秘密と考えられておらず，リモート生体認証のような入力する厳密を厳重に監視できない前提がある場合，なりすまし攻撃によって容易に突破されてしまうという事実に基づいて

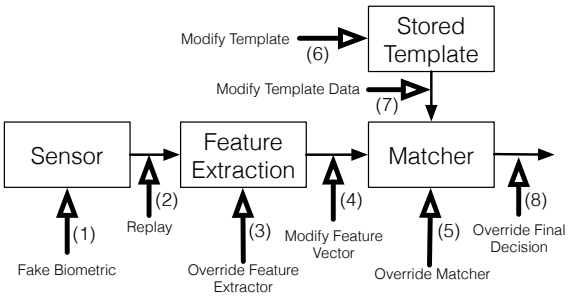


図 1　生体認証システムのアーキテクチャと 8 つの攻撃タイプ

いる．リモート生体認証といった無人のシナリオにおける安心・安全な生体認証の実現が，今後の生体認証の普及における重要な意味を持つことは確実であり，したがって，様々な不正な入力によるなりすましの可能性を考慮した上で，人工物や生体を検知する手法により，オープンネットワークにおけるリモート認証のセキュリティを保つことが非常に重要となる．

以降では生体認証装置に対するなりすまし攻撃，およびその対策技術，なりすまし耐性の評価技術と，国際標準化動向について，現状の動向をふまえて概説する．

2. 生体認証機器に対するなりすまし攻撃

文献 [6] では生体認証機器に対する攻撃のタイプを図 1(1)〜(8) に示すような 8 つのタイプに分類している．このうち，本稿で述べるなりすまし攻撃 (Presentation Attacks) とは，図 1(1) のセンサに対する入力を用いた攻撃と分類される．

ここでは，センサに入力する偽造物 (Fake Biometric) の作成と攻撃のプロセスを，(1) 偽造物の元となる情報の入手，(2) 元となる情報からの偽造物の作成，(3) 作成した偽造物のセンサへの提示，の 3 つに分類し，それぞれの場合について課題となる事項について考察する．

2.1 偽造物の元となる生体情報の入手

第一に，生体情報の入手における問題は，どのような手段で偽造物の元となる生体情報を入手するか，という点である．これに関しては元となる生体情報の入手方法から，協力的なりすましと，非協力的なりすましの 2 つに分類される [7].

2.1.1 協力的なりすまし

協力的なりすましは主に，正規ユーザと攻撃者が結託することで，攻撃者が正規ユーザになりすまし，システムに対して双方の利益となる攻撃を行う脅威である．2013 年 3 月にはブラジル・サンパウロ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，30 人以上の同僚の勤務を偽装していたことがわかった．このようなケースでは，登録者は自分の利益 (たとえば，勤怠の偽装) を目的として，攻撃者に容易に生体情報を提供することが予想される．特に社会システムとして生体認証利用が期待されている現在，社会保障の二重受給など，不当な利益を得る目的でのなりすましを防止するために，協力的なりすましへの対策が重要となる．

2.1.2 非協力的なりすまし

非協力的なりすましは主に，遺留指紋など，何らかの不正な手段で盗み出した登録者の生体情報に基づくパターンや，攻撃者が任意に作成した生体情報に依存しないパターンに基づく偽造物を用いたなりすましである．多数の登録ユーザに対して誤一致を引き起こす攻撃者である Wolf [8] や，多数の照合ユーザに対し誤一致を引き起こす登録者である Lamb などもこれにあたる．2010 年には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 名が逮捕されているが，これは入国審査がブラックリスト検査であることを利用した事例であり，非協力的なりすましを容易とするケースと言える．

上記の例からもわかるように，生体認証はアクセスコントロールのみではなく，ウォッチリストとしての機能を目的としている場合があり，このような場合のなりすましは，特定の個人の生体情報複製を目的としていないことに注意が必要である．

2.2 元となる生体情報からの偽造物の作成

次に，二番目のプロセスである偽造物の作成について考える．偽造物の作成に際しては，攻撃者は自身が持つ技術力や設備と，攻撃にかかる時間をふまえて，最も最善となる攻撃を選択すると考えられる．したがって，偽造物作成方法は，次の 2 つの観点から分類できる [9].

- 技術的困難性
- コスト

2.2.1 技術的困難性 (Expertise)

技術的困難性は必要な装置や材料といった実験設備の性能，さらにはそれらを用いた攻撃を行うために必要な攻撃者の熟練度を示す．たとえば，グミやシリコンによる偽造指紋 [3], [4] は訓練を受けていない攻撃者が安価な材料で作成可能であり，技術的困難性は低い．一方，3D 顔といった指紋とは異なり形状や質感，生体そのものが持つ特徴の再現に高度や設備が必要となるモダリティや，ウルフ [8] といった専門的な技術やそれらに基づく偽造生体を作成可能な高度な装置が必要な攻撃に関しては，技術的困難性が高いと考えられる．

2.2.2 コ　ス　ト

コストは，生体検知を突破可能な偽造物を 1 つ作成するのに必要とされる攻撃に必要な人数，および時間を示す．ここで，たとえ技術的困難性が高い場合でも，非常に少ない回数で生体検知を突破可能な偽造物が作成可能であるならば，技術的困難性が低い手法と比較してコストが小さくなることはあり得る．このため，なりすまし攻撃への耐性を評価する際には，技術的困難性とコスト，両面を考慮した評価を行う必要があるだろう．

2.3 作成した偽造物のセンサへの提示

偽造物のセンサへの提示は，認証を監視する人物がいる場合 (Attendee)，またはリモート生体認証のように，監視する人物がいない場合 (non-Attendee) が考えられ，それぞれの場合における偽造物識別困難性が異なる．特に，監視する人物が存在する場合は提示する素材の種類や形状により，偽造物識別が容易となる．

3. なりすまし対策技術

ここでは 2 章では考察したなりすまし攻撃に対する対策に関して，従来検討されている方式を紹介する．従来研究で提案さ

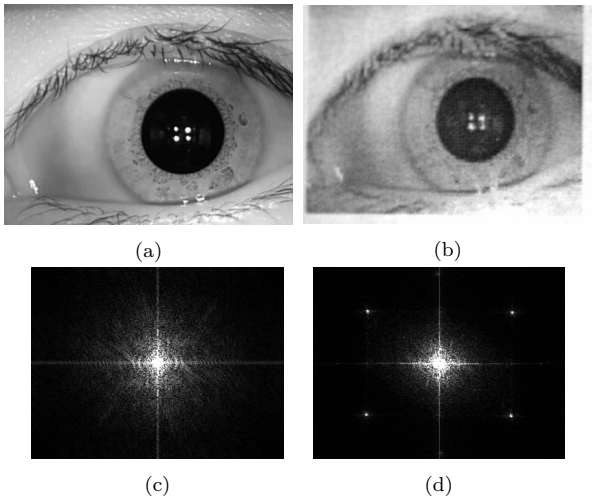
れているなりすまし対策は次の 3 つの特徴に基づく方式に分類することができる [10].

- 生体の固有特徴
- 生体の無意識動作
- 外部刺激に対する生体反応

3.1 生体の固有特徴に基づく対策

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．指紋であれば電気抵抗を用いる方式 [11], [12] や汗腺と呼ばれる指紋隆線の凸部に存在する汗の出口となる穴の存在を画像から読み取る方式 [13], [14] がよく知られている．しかし人間の電気抵抗はグミ指のそれと類似していることが松本らにより報告されている [3] ことや，皮膚表面の状態は押しつけ等による影響を非常に受けやすいという問題がある．このため近年では可視光とは異なる周波数帯域の光に対する反応を観測し，皮膚や血管といった人体特有の特徴が存在するかどうか，またその構造を含めた判定を行う手法などが提案されている [15], [16].

虹彩であれば印刷した虹彩のドットパターンを周波数領域の変化から検出することで，印刷物を検知する手法 [12], [17], [18] などがこれに分類される．他にも光の反射や吸収の度合い，色や透明度，体液に含まれる成分など，生体の静的な特徴を利用するものはこれに分類される．



(a) (b) (c) (d)

図 2 人間の虹彩とプリントした虹彩の比較．(a),(c) が人間の虹彩と対応する周波数領域．プリント虹彩 (b) の周波数領域 (d) ではドットパターンから四隅にピークが発生している [18]

3.2 生体の無意識動作

生体が定常的に発している信号のうち，観測可能なものを利用した方式．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が利用される．主に生体の動的な特徴を利用するものはこれに分類される．静電容量センサで取得された指紋画像において，汗腺から発生する汗の蒸発の時系列変化を見る方式が提案されている [19]．本手法は特別なハードウェアを必要とせず人体検知を実現できるが，発汗異常があるユーザなどには適用できない欠点もある．虹彩では瞳孔が照明変動とは関係なく，0.5Hz ほどの間隔で定常的に振動していると言われており，これを利用した検知が可能である．また近年では，ECG(Electrocardiograph:心電図) を指紋と組み合わせることで生体検知を行う方式 [20] なども提案されている．1998 年に成立した米国特許 [21] でも，生体検知は 2 種類以上の生体特徴を組み合わせて行うことが提案されており，特に，脈拍，心電図，体温の 3 つの組み合わせによる生体検知が提案されているが，透明の素材を用いることで容易に検知を回避できることなどが問題として存在する．

3.3 外部刺激に対する生体反応

3.1，3.2 の方式に対し本方式は生体の対話的な特徴を利用した方式であり，外部刺激に対する生体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や，話者照合におけるキーワード発話といった，照合対象者の協力が必要となる方式や，光による瞳孔の収縮，膝蓋腱反射等，無意識の反射運動もこれに含まれる．特に瞬き検知等，特別な動作を利用者に要求する方式はなりすましを困難とすることが可能と考えられるが，利便性低下やセンサのコストの増大を招く可能性がある点に注意が必要である．

米国で特許化されている Kallo らの生体検知手法 [22] では，指に対して微小インパルスを入力し，これに対する電気的応答を観測することで生体であるかどうかを判定する．本手法は生体以外での再現が困難である一方，インパルスに応答している人間が生体を提示している人間であるかどうかを確認する手段がない，という点が問題となる．また，電気的な刺激をユーザが許容するかも問題となるだろう．

4. なりすまし耐性の評価技術

なりすまし攻撃への耐性を評価するためには，多量の偽造物と生体を準備した上でそれらを正しく判定可能であるかどうかを評価する必要がある．ここで，信頼性が高く，かつ異なる実験結果を公正に比較可能とするためには，どの程度のサンプル数で実験を行えば充分であるかや，得られた結果を比較評価するための指標 (生体認証における FAR や FRR に相当する指標) が必要となる．ここではなりすまし耐性の評価に対する具体的な取り組みとして，LivDet2013 [23]，TABULA RASA Competition on Counter Measures to 2D Face Spoofing Attacks [24]，および TABULA RASA Spoofing Competition を紹介する．

4.1 LivDet2013

Fingerprint Liveness Detection Competition(LivDet) はイタリア Cagliari 大学，アメリカ Clarkson 大学が主催する指紋の人体検知アルゴリズムの性能を競うコンペティションであり，2009 年から 2 年置きに開催され，今年 2013 年に第 3 回が開催された．ここでは 2013 年に ICB2013 と同時に開催された LivDet2013 の概要について紹介する．LivDet2013 では企業や大学から 12 の参加者があり，ソフトウェアに基づく検知性能を競うアルゴリズム部門とハードウェアを含めた総合的な性能を競うシステム部門の 2 部門での競技が行われた．

4.1.1 使用データセット

Biometrika 社，CrossMatch 社，ItalData 社，スワイプ型センサ (非公表) の 4 つのデバイスから約 4000 枚の画像を取得．

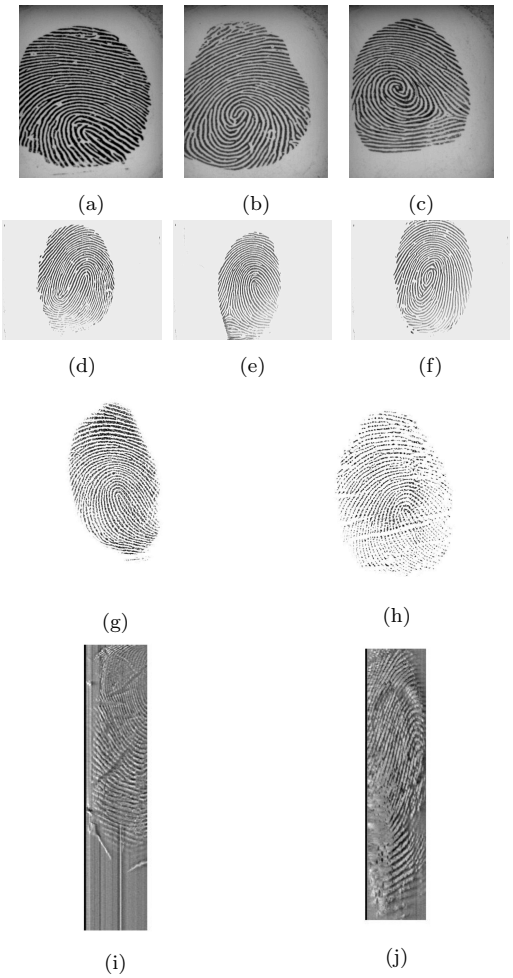


図 3　各センサ，素材による取得画像．(a,b,c) が Biometrika，(d,e,f) が ItalData,(h,i) が Crossmatch,(j,k) が Swipe 型センサによる取得画像．また，(a,d) がゼラチン，(b,e,g,i) がラテックス (合成ゴム)，(c,f,h,j) が木工用ボンドで作成した偽造指紋による取得画像 (全て [23] より)

4000 枚の画像は半分が生体，半分が Ecoflex(導電シリコン), ゼラチン, シリコン, Wood-Glue(木工用ボンド), Play-Doh(工作粘土), Latex(合成ゴム) から生成された偽造物である．なお，Biometrika 社と ItalData 社のセンサでは，非協力的なりすましを，CrossMatch 社，スワイプ型センサでは協力的なりすましを想定したサンプルを用いて画像を収集している．

4.1.2　アルゴリズム部門の評価手順

偽造物のうち一部をトレーニング用情報として参加者に提供し，これによりチューニングされた偽造物判定アルゴリズムを参加者は評価者に提出する．評価者は残りの画像を用いてアルゴリズムの判定性能を評価する．

アルゴリズム部門では，指紋画像の入力に対し，人体らしさを表すスコアを出力するアルゴリズムであることが必要とされる．評価の際には評価者がしきい値を決定し，出力されたスコアがしきい値以上であれば人体，しきい値以下であれば偽造物と判定する．したがって，アルゴリズムの人体検知性能は明らかに評価者が決定するしきい値によって変動する．以上の理由から，アルゴリズム部門においては，評価に用いるしきい値は 50 で固定されることがあらかじめ参加者に周知される．参加者はアルゴリズムのチューニング時にしきい値が 50 で最も良いパフォーマンスを示すように評価者に提出するアルゴリズムを最適化する必要がある．

4.1.3　システム部門の評価手順

アルゴリズムだけでなくハードウェアを含めた認証システムの検知性能を競う部門である．参加者は評価者より与えられたトレーニング画像を用いてチューニングしたシステムを評価者に提出する．評価者は，提出されたシステムが使用するセンサに対して，評価用サンプルをランダムに提示し，判定性能を評価する．しきい値判定を含むシステム全体のチューニングが参加者に任されているため，アルゴリズム部門のようなしきい値最適化の必要はない．

4.1.4　評価基準と結果

評価結果は，以下の評価基準に基づき評価される．

- F_{rej}：登録に失敗する確率
- $F_{corrlive}$：生体を正しく生体と判定する確率
- $F_{corrfake}$：偽造物を正しく偽造物と判定する確率
- F_{corr}：生体および偽造物を正しく判定する確率
- $F_{errlive}$：生体を誤って偽造物と判定する確率
- $F_{errfake}$：偽造物を誤って生体と判定する確率

なお，一般に $F_{corrlive} = 100 - F_{errlive}$, $F_{corrfake} = 100 - F_{errfake}$ であることから，LivDet でも $F_{errlive}, F_{errfake}$ のみが報告されている．また，F_{corr} はシステムの生体検知性能を示す指標であり，以下の式により算出される．

$$F_{corr} = 100 - \frac{(F_{corrlive} + F_{corrfake})}{2} \tag{1}$$

F_{corr}(LivDet では accuracy として評価) は，Biometrika や ItalData における非協力的な偽造物に対して全体的に高い性能を示している．非協力的な偽造物に関しては平均でも 90.5 %と高い検知性能を示しており，特に検知性能でトップの成績を示した Dermalog では平均検知率は 98.75 %であった．一方，協力的な偽造物に関しては平均 62.8 %と検知が困難であり，Swipe 型センサへの検知性能が平均 83.6 %に対し CrossMatch 社のセンサに対する検知性能が平均 50.1 %とセンサによるばらつきが大きいことが報告されている．

4.2 TABULA RASA Competition on Counter Measures to 2D Face Spoofing Attacks

TABULA RASA (Trusted Biometrics under Spoofing Attacks) プロジェクトはなりすまし攻撃に対して頑健な生体認証システムに関するプロジェクトであり，2011 年より EU の FP7 プロジェクトの下で進められている．研究者として IDIAP, CASIA，Morpho，Cagliari 大学，Southampton 大を含む 12 の企業・大学が名を連ねており，産学の連携により実践的な研究を進めている．プロジェクトの一環として，2013 年の ICB(International Conference of Biometrics, スペイン・マドリッドにて開催) では TABULA RASA プロジェクトが主催する The 2nd Competition on Counter Measures to 2D Face Spoofing Attacks [24] が開催された．コンペティションは，CA-

SIA, IGD, MaskDown, LNMIIT, MUVIS, PRA Lab, ATVS, Unicamp の 8 つの参加者で競われた．LivDet2013 とのモダリティ以外での大きな違いは，参加者のアルゴリズムがコンペティション終了後に公開される点である．

4.2.1 使用データベース

Replay Attack face spoofing database [25] を用いてそれぞれのアルゴリズムの評価が行われた．本データベースは 50 名分の登録者短時間動画データ，および各登録者に対するなりすまし攻撃を想定した短時間動画データから構成される．データベースには 3 つの異なるタイプの攻撃を想定した動画が収録されている．

- 印刷された写真を提示
- 写真をディスプレイに表示して提示
- 動画をディスプレイで再生して提示

また，それぞれの動画は，写真や動画が固定して提示された場合と，手で保持して提示された攻撃を想定し，2 つのグループにわけて撮影されている．撮影条件は，背景が一様かつ照明条件が一定な Controlled と，背景が非一様かつ照明条件が日光である Adverse の 2 つの条件が想定された．動画は 320x240pixel,25fps の解像度であり，座った状態で 13 インチ MacBook 付属のカメラを用いて取得された．

データベースはトレーニング用セットが 360 シーン，開発用セットが 360 シーン，テスト用セットが 480 シーンの合計 1200 シーンで構成されている．また学習以外に精度評価用のセットが別に用意されている．これは，偽造生体情報が実際に生体認証システムに受理される確率を評価するものであり，生体検知アルゴリズムがどの程度必要であるかを示す指標となる．偽造生体による認証システムへの受理確率が低い場合，生体検知を突破されることによる本質的な脅威は低いと言える．

4.2.2 評 価 手 順

参加者には，節で述べた全てのデータセットが提供される．ただし，テスト用画像に関してのみ，各テスト用動画のうちランダムな 100 フレームを切り出し，さらに生体か偽造物かを秘密としたものが提供された．

参加者はトレーニング用動画を用いてなりすまし対策アルゴリズムを検討し，次に開発用動画を用いて対策アルゴリズムにおける環境依存のパラメータ (判定しきい値等) をチューニングする．最後にテスト動画を用いた評価結果をレポートするという手順で競技が行われた．

また，テスト時の HTER 算出に用いるしきい値は，開発用データセットにおいて EER(Equal Error Rate) に最も近い FAR，FRR を示す値として設定された．なお，EER とは FAR と FRR の値が等しくなる際の両者の値として定義される．

4.2.3 評価基準と結果

評価結果は次の評価基準により評価された．

- FRR : 生体を誤って偽造物と判定する確率
- FAR : 偽造物を誤って生体と判定する確率
- HTER: 生体および偽造物を正しく判定する確率

ここで，HTER は Half Total Error Rate の略であり，(FAR+FRR)/2 で示される．また，4.1 の評価指標と比較すれば，FRR が F_{errliv} に，FAR が $F_{errfake}$ に，HTER が F_{corr} にそれぞれ対応する．

実験結果ではテクスチャベースとモーションベースの特徴を特徴レベル統合した CASIA と LNMIIT が HTER=0 %を達成している．さらに，その他のアルゴリズムも，8 つの参加者中 5 参加者が 2.5 %以下の HTER と非常に高い判定確率となっている．LivDet2013 との判定確率の違いが大きいが，これは顔画像が指紋と比較して偽造にかかるコストや技術的困難性が高いことに起因すると考える．

4.3 TABULA RASA Spoofing Challenge

先述した 2 つの Competition が生体認証機器のなりすまし耐性を競うものであったのに対し，本コンペティションは参加者が用意した偽造生体の既存の製品に対するなりすまし攻撃性能を競うものである．目的は，以下の 4 つのモダリティにおける，より高度な偽造技術を探求するとともに，それらへの対策技術を再考する機会を設けることである．

- 二次元顔画像 (可視光)
- 二次元顔画像 (赤外)
- 音声
- 指紋

競技では，登録者を 2 つのグループに分け，一方のグループのみの生体情報を公開し，もう一方のグループに関しては ID のみが公開された．これらの情報から，ID のみが公開されたグループのいずれかのユーザになりすませるかどうかが競われた．本コンペティションの結果として ICB2013 の会期内に指定のセンサ (2 次元可視光顔画像認証装置) への攻撃に成功したミシガン州立大学が表彰されている．

5. なりすまし攻撃耐性に関する国際標準化

生体認証機器に関する標準化に関しては，なりすまし検知の標準化，およびその安全性の評価，さらには機器の認証制度が既に検討されており，一部の国においては既に制度化されているものも存在する．その中でも注目すべき動向として，ISO/IEC 30107 および FSDPP を紹介する．

5.1 ISO/IEC 30107

ISO/IEC 30107:Presentation attack detection [26] は 2012 年より ISO/IEC JTC 1/SC 37 で開始・進行中の生体認証機器のなりすまし検知に関するプロジェクトである．本プロジェクトは，なりすまし攻撃に関する用語やセンサ部でのなりすまし検知結果を照合部へ伝えるためのデータフォーマット，また検知アルゴリズムの性能評価方式，原理までの策定を目的としている．2012 年 7 月のパリ会議では，米国，欧州各国，オーストラリア，SC27 などから合計およそ 300 件の熱心なコメントがあり，各国の関心は非常に高いことが伺える．

5.2 BSI FSDPP

FSDPP(Fingerprint Spoof Detection Protection Profile) [27] は，BSI(ドイツ) が策定したドイツ国内用の指紋認証機器のセキュリティ要求仕様である．本仕様は ISO/IEC 15408(Common Criteria) の枠組みに基づき策定されている．FSDPP では，6.2 章において指紋認証機器に対する脆弱性評価項目が

AVA_VAN.E として定義されている．また，フランスのモルフォが本認証を取得した製品 (MorphoSmart MSO301) を発売している．

6. ま と め

本稿では，生体認証における脅威のうち，生体認証機器に対するなりすまし攻撃に関して着目し，現状のなりすまし攻撃手法，攻撃対策，およびなりすまし耐性の評価手法について概説した．なりすまし攻撃手法において，技術的困難性とコストを考慮した評価が必要であることを 2 章で述べた．しかし 4 章で概説した LivDet2013 や TABULA RASA といった複数の評価コンペティションにおける評価の状況を考察する限り，現状の多くの攻撃は技術的困難性やコストの低いものに集中していることがわかる．昨今の標的型攻撃の事例などからもわかるように，特定の対象者に攻撃コストを集中させるといった攻撃は生体認証へのなりすましにおいても充分に現実的であり，このため技術困難性の高い手法や高コストの手法に関しても適切な評価が必要と考える．さらには，non-Attendee や Attendee といったセンサへの提示困難性や，人体検知を回避した際に認証を通過できる確率までを考慮可能な評価指標についても今後検討を行っていきたい．

文　献

[1] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol.29, no.4, pp.561–572, April 2007.

[2] A.K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” EURASIP Journal on Advances in Signal Processing, vol.2008, no.1, 2008. ArticleID:579416.

[3] T. Matsumoto, “Gummy and conductive silicone rubber fingers importance of vulnerability analysis,” Advances in Cryptology–ASIACRYPT 2002, pp.574–575, Springer, 2002.

[4] T. Van derPutte and J. Keuning, “Biometrical fingerprint recognition: don’t get your fingers burned,” Smart Card Research and Advanced Applications, pp.289–303, 2000.

[5] National Institute of Standards and Technology, “Nist special publication 800-63-1 electronic authentication guideline”. “http://csrc.nist.gov/publications/nistpubs/800-63-1/SP800-63-1.pdf”.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, “An analysis of minutiae matching strength,” Audio-and Video-Based Biometric Person Authentication, pp.223–228, Springer, 2001.

[7] K.A. Nixon, V. Aimale, and R.K. Rowe, “Lumidigm White Paper: Spoof detection schemes,” 2008.

[8] M. Une and A. Otsuka, “Wolf attack probability: a new security measure in biometric authentication systems,” International Conference on Biometrics (ICB’7), vol.4642, pp.396–406, Springer-Verlag Berlin Heidelberg, 2007.

[9] “Evaluating attack resistance levels of biometric systems,” 2012. http://biometrics.nist.gov/cs_links/ibpc2012/presentations/Day2/225_Mansfield.pdf

[10] B. Toth, “Biometric liveness detection,” Information Security Bulletin, vol.10, no.8, pp.291–297, 2005.

[11] H. Choi, R. Kang, K. Choi, and J. Kim, “Aliveness Detection of Fingerprints using Multiple Static Features,” Proc. of World Academy of Science, Engineering and Technology, pp.201–205, 2007.

[12] B. Tan, “New approach for liveness detection in fingerprint scanners based on valley noise analysis,” Journal of Electronic Imaging, vol.17, no.1, p.011009, Jan. 2008.

[13] B. Tan and S. Schuckers, “Liveness detection using an intensity based approach in fingerprint scanner,” Proceedings of Biometrics Symposium, Arlington, VA (September 2005), 2005.

[14] A. Abhyankar and S. Schuckers, “Empirical mode decomposition liveness check in fingerprint time series captures,” Computer Vision and Pattern Recognition Workshop, 2006. CVPRW’06. Conference on, pp.28–28, 2006.

[15] C. Jin, H. Kim, and S. Elliott, “Liveness detection of fingerprint based on band-selective Fourier spectrum,” Information Security and Cryptology-ICISC 2007, pp.168–179, Springer, 2007.

[16] H. Lee, H. Maeng, and Y. Bae, “Fake finger detection using the fractional Fourier transform,” Fake Finger Detection Using the Fractional Fourier Transform, pp.318–324, Springer, 2009.

[17] J. Daugman, “Demodulation by complex-valued wavelets for stochastic pattern recognition,” International Journal of Wavelets, Multiresolution, and Information Processing, vol.1, pp.1–17, 2003.

[18] X. He, Y. Lu, and P. Shi, “A new fake iris detection method,” Advances in Biometrics, pp.1132–1139, 2009.

[19] R. Derakhshani, S.A. Schuckers, L.A. Hornak, and L. O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” Pattern Recognition, vol.36, no.2, pp.383–396, 2003.

[20] C.X. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos, “Securing handheld devices and fingerprint readers with ECG biometrics,” Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on, pp.150–155, IEEE, 2012.

[21] 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.

[22] P. Kallo, I. Kiss, A. Podmaniczky, and J. Talosi, “Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus,” Dermo Corporation, Ltd., US Patent #6,175,641, Jan. 2001.

[23] L. Ghiani, D. Yambay, V. Mura, S. Tocco, and G.L. Marcialis, “LivDet 2013 Fingerprint Liveness Detection Competition 2013,” International Conference on Biometrics (ICB’13), 2013.

[24] I. Chingovska, J. Yang, Z. Lei, D. Yi, S.Z. Li, O. Kähm, C. Glaser, N. Damer, A. Kuijper, and A. Nouak, “The 2nd Competition on Counter Measures to 2D Face Spoofing Attacks,” International Conference on Biometrics (ICB’13), 2013.

[25] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” Proceedings of the Biometrics Special Interest Group (BIOSIG) 2012, pp.1–7, IEEE, 2012.

[26] “ISO/IEC WD 30107: Information Technology – Biometrics – Presentation attack detection,” 2012. “http://www.iso.org/iso/catalogue_detail.htm?csnumber=53227”

[27] “Fingerprint spoof detection protection profile, version 1.8,” 2009. “https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0063b_pdf.pdf”