マイクロ生体認証の提案とその一事例報告

藤田真浩[†1]　眞野勇人[†1]　高橋健太[†2]　西垣正勝[†1]

1. はじめに

生体認証は,パスワードやトークンを用いた認証方式と比較して，忘却・紛失・盗難の恐れがないという利点がある．一方で生体認証は，生体情報の「生涯不変であり，任意に更新できない」性質に起因した「なりすまし」と「プライバシ侵害」の問題を有している．

「なりすまし」は，攻撃者が生体情報を入手して偽造生体を作成する攻撃である．実際に，攻撃者がなりすましに成功した事例も報告されており[1][2], なりすましに対する耐性を有することは生体認証システムの重要な要件である（要件 1：なりすましに対する耐性）．

「プライバシ侵害」には，追跡可能性の問題がある．生体情報は，パスワードやトークンのように変更や交換によって本人との間の紐づきをリセットできないため，匿名ユーザ群または仮名ユーザ群の中から生体情報を用いて同一ユーザを名寄せすることが可能である．すなわち，追跡可能性の観点からは，任意のタイミングで更新できる生体情報を用いることが望ましい（要件 2：追跡可能性に対する配慮）．

要件 1,2 に配慮した既存方式が，生体情報のワンタイム化である．しかし，生体情報のワンタイム化が可能なのは基本的に動的な生体情報に限られる．動的な生体情報を用いた認証は，静的な生体情報を用いた認証と比較して認証精度が低いという問題が知られている[3]．要件 1〜2 を満たす生体認証を，静的な生体情報を用いて実現できればより望ましい（要件 3：静的な生体情報の利用による認証精度の確保）．

そこで本稿では,要件 1〜3 を満足する認証方式としてマイクロ生体認証を提案する．

2. マイクロ生体認証

人間の微細部位の生体情報を生体認証へ適用する「マイクロ生体認証」を提案する．正規ユーザは自身のある微細部位の生体情報をテンプレートとしてシステムへ登録し，認証時にはその微細部位を再度提示することによって認証を行う．微細部位の利用によって，要件 1〜3 に配慮した生体認証方式が実現される．要件 1 に関しては，登録情報（微細部位の生体情報）が盗まれたとしても，不正者が微細レベルの偽造生体を作成するには大きなコストを要する．要件 2 に関しては，生体部位の更新可能回数（微小部位を 1 つずつ使っていった際に未使用部位が枯渇するまでの回数）が増加する分，ユーザは認証システムに登録する生体情報を頻繁に更新することができる．要件 3 に関しては，生体部位の静的な生体情報を利用しているため,認証精度も（動的生体認証と比較して）高い．

3. 肌理を用いた生体認証

マイクロ生体認証の第一報として，肌理の凹凸パターンを用いたマイクロ生体認証のプロトタイプシステムを構築し，評価実験を行った．

3.1 プロトタイプシステムの実装

肌理の凹凸パターンを用いたマイクロ生体認証のプロトタイプシステムを構築した．プロトタイプシステムの概要を図 1 に示す．以下に，実装において留意した点を示す．

- 肌理画像は倍率約 200 倍のマイクロスコープ（サンコー製 AM2001 Dino-Lite Basic）を用いて撮影した．
- 位置合わせのためのマークは油性染料インクで直接皮膚に印を付ける方法を採用した．
- 位置合わせ用のマークによっておおまかな位置合わせは可能であるが，若干の位置ずれや歪みは起こりうる．したがって，テンプレート画像と認証用画像の厳密な位置合わせは，目視によって行った（図 2）．
- 認証用の特徴量としては肌の凹凸を利用した．安定した特徴を抽出するために，認証用画像とテンプレート画像は，マッチング前に，以下の四つの処理を順に施した．
  (1) グレースケール化：色合い補正
  (2) ヒストグラム均一化：凹凸強調
  (3) ローパスフィルタ処理：ノイズ除去
  (4) 適応的二値化：凹凸抽出

  図 3 にこれらの処理を施した際の画像の変化の例を示す．図 3(a)が元画像であり，図 3(b)が図 3(a)に(1)〜(2)の処理を順に施した後の図,図 3(c)が図 3(b)に(3)〜(4)の処理を順に施した後の図である．
- マッチングアルゴリズムは，正規化相互相関を利用した．

3.2 実験

21 歳から 26 歳までの大学生 10 名に協力してもらい，サンプル画像を収集した.各被験者に対して前腕内側の肌理，任意 5 か所にマークを記した．実験は 3 日間にわたって行

†1 静岡大学
†2 （株）日立製作所

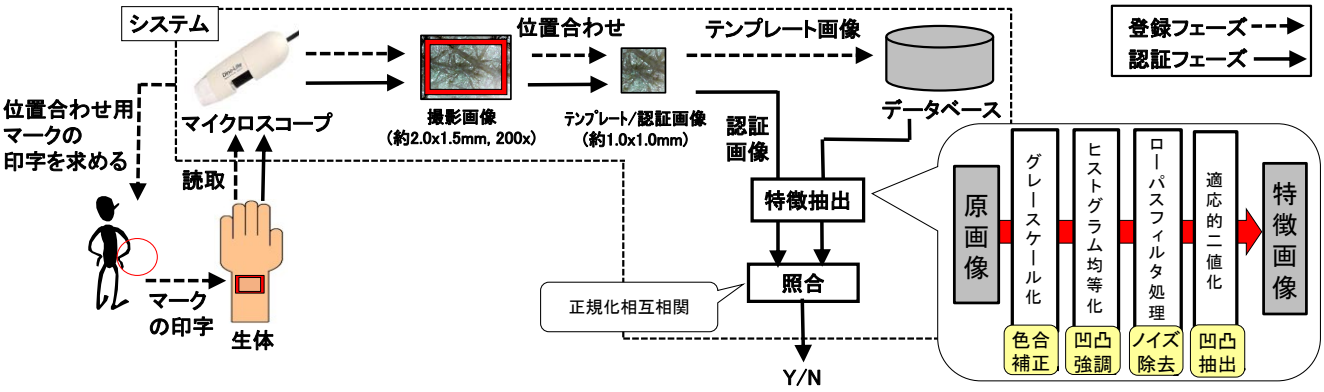

図 1　プロトタイプシステムの概要

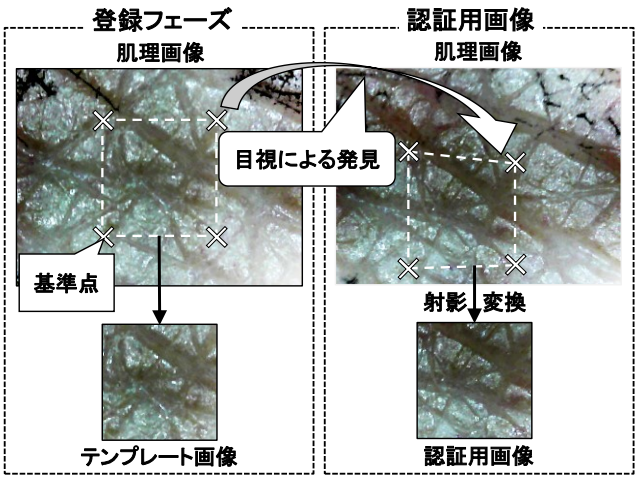

図 2 目視による位置合わせ

い，マークをつけた部位 1 か所につき 1 日 1 回肌理画像を取得した．1 回あたり 5 枚の画像を撮影し，そのうち 2 枚をサンプル画像として利用した[a]．

3 日目の撮影時（2 日目と 3 日目の間）に，被験者の肌に記したマーク（インク）の一部，計 18 か所が消失していることが確認された．それらの部位については撮影を止めた．その結果，1 日目 100 枚（50 か所×2 枚），2 日目 100 枚（50 か所×2 枚），3 日目 64 枚（32 か所×2 枚）のサンプル画像を得た．

収集した 264 枚の画像に対して leave-one-out 交差検証を用いて EER を計算した結果，本人間の照合スコアの分布と他人間の照合スコアの分布がともに正規分布に沿っているという仮定下で，　EER≒0.5%という結果を得た．

3.3 考察

プロトタイプシステムでは約 1.0×1.0mm の微細範囲の肌理を約 200 倍で拡大した画像（画像の解像度としては 5 μm）をテンプレートおよび認証画像として利用している．不正者がなりすましを成功させるためには約 1 μm レベル

[a] 3.1 節で述べたように今回は約 200 倍での接写となるため，撮影画像に手ぶれが生じやすい状況であった．このため，各部位につき 1 回当たり 5 枚の画像を撮影し，その中から手ぶれのない画像を撮影した順に 2 枚抽出するという方法でサンプル画像を取得した．

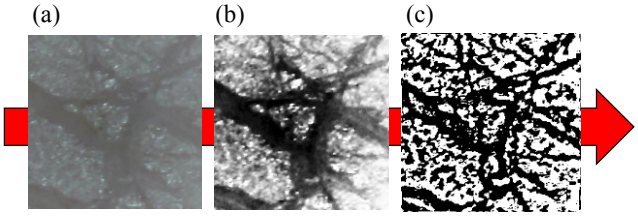

図 3　特徴抽出の例

の偽造物の生成が求められるため，偽造コストは非常に高い（要件 1 の達成）．人間の肌の総表面積は約 1.6 ㎡以上あるといわれているため[4]，仮に 1.0×1.0mm を登録面積とすると，理論上は約 2.6×10^6 通りの生体情報を利用可能となる（要件 2 の達成）．3.2 節では実際に実験を通じて EER ≒0.5%という値を得た．筆者らが確認した限り，高い認証精度を有する方式であるといえるだろう（要件 3 の達成）．

4. まとめと今後の課題

生体認証が抱える課題を解決したマイクロ生体認証を提案した．微細肌理画像を利用したプロトタイプシステムを開発し，実験を行うことでマイクロ生体認証の有用性を確認した．今後の課題としては，位置合わせの自動化，より長期的・大人数での実験，他のモダリティへの適用，などが挙げられる．

謝辞　本研究をご支援してくださった，産業技術総合研究所 大塚玲様，大木哲史様，静岡大学 中谷広正教授，佐治斉教授，村松弘明君にここで深く謝意を表します．

参考文献

1)　Putte, T. and Keuning, J.: Biometrical fingerprint recognition: don't get your fingers burned, Proc. IFIP TC8 / WG8.8 4th Working Conf. on Smart Card Research and Advanced Applications, Bristol pp. 289-303 (2000).
2) K. Zoe: Politician's fingerprint 'cloned from photos' by hacker (online), available from <http://www.bbc.com/news/technology-30623611> (accessed 2016-05-23)
3) バイオメトリクスセキュリティコンソーシアム，バイオメトリックセキュリティ・ハンドブック，オーム社，東京，2006.
4) Bender, A. E. and Bender, D. A.: Body Surface Area in A Dictionary Food and Nutrition, Oxford University Press, 1995