I-072

手形状の面積時系列を用いた本人認証

Verification Method Using Square Measure Sequence of Hand Shape

荻原 昭夫† 松村 博之† 汐崎 陽†
Akio Ogihara Hiroyuki Matsumura Akira Shiozaki

１．まえがき

現在，銀行や郵便局の ATM ではキャッシュカードと暗証番号を用いて本人認証が行なわれている．しかし，現状の本人認証においては，悪意のある第三者がキャッシュカードや暗証番号を入手した場合，本人に成りすまして現金等を引き出す事が可能であるという問題点を有している．そして近年では，スキミングと呼ばれる手法によるキャッシュカードの複製や，暗証番号の盗撮などの犯罪が社会問題となっている．

そこで，我々は本人認証の安全性を高める事を目的とし，キャッシュカード・暗証番号に続く第三の認証要素として生体情報[1]の利用を考えている．本論文では，ATM において暗証番号を入力する際の手の動きにより生じる“手形状の面積の時間変化パターン”を利用した本人認証手法を提案する．提案手法では，暗証番号の入力操作自体が特徴提示操作となるので，ATM 利用者に新たな操作を要求すること無く，現状よりも高い安全性を提供することが可能である．

２．手形状面積時系列を用いた本人認証

提案手法は，本人認証に先立って事前に行なう「登録過程」と，実際に認証処理を行なって本人であるか否かを判別する「認証過程」からなる．

2.1 登録過程

本人認証システムの正規利用者は，各自の認証情報（生体情報）を事前に登録する必要がある．しかし，登録操作は普段通りに暗証番号を入力するだけで良く，他の複雑な操作は一切不要である．本人認証システムは，提示された暗証番号の入力動作から，下記の手順に従って認証情報を抽出し，登録を行なう．

[Step1] 正規ユーザに普段通りに暗証番号を入力してもらい，その動作をビデオカメラ経由でキャプチャーしてコンピュータに取り込む．

[Step2] キャプチャーされた動画像より，「手が撮影画面に入る直前のフレーム」から「画面外に出た瞬間のフレーム」までを分析対象区間として切り出す．

[Step3] 切り出された動画像から，各フレームの静止画像を取り出す．さらに，インタレース画像であるフレーム画像から，ノンインタレース画像である複数のフィールド画像を求める．（図 1 参照）

[Step4] 各フィールド画像に対して二値化，ノイズ除去，ラベリング処理を施して，図 2 中段に示すような二値画像を求める．

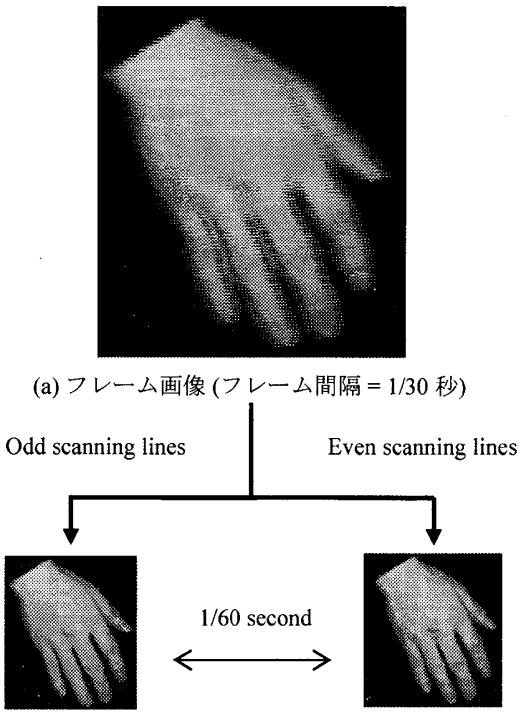

図 1 インタレース方式のフレーム画像から得られるノンインタレース方式のフィールド画像

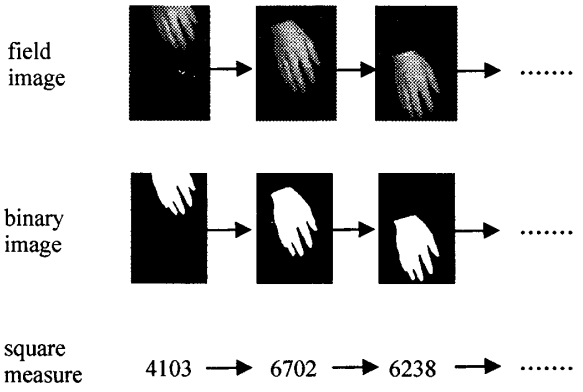

図 2 フィールド画像（上段）と二値画像（中段）と手形状の面積時系列（下段）

† 大阪府立大学大学院工学研究科, Graduate School of Engineering, Osaka Prefecture University

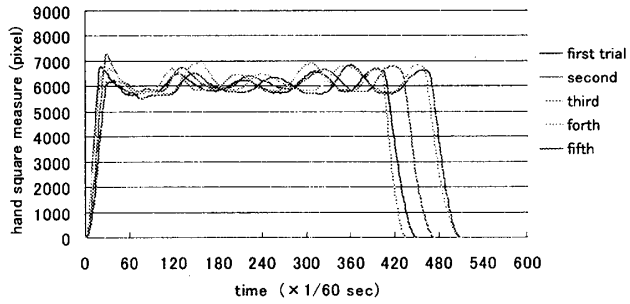

図３　手形状の面積時系列の抽出例（試行回数＝5回）

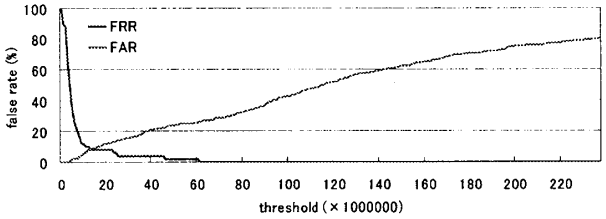

図４　本人認証実験における閾値とFRR（本人棄却率）およびFAR（詐称者受理率）との関係

[Step5] 各二値画像における白画素の総数を計数することにより，手形状の面積を求める．

[Step6] 図 2 下段に示す手形状の面積時系列を「登録データ」として記憶する．

手形状の面積時系列の抽出例として、暗証番号の入力動作5回から得られた 5 個の手形状の面積時系列を図 3 に示す。

2.2　認証過程

提案手法を適用することにより，正規利用者に特別な追加操作を要求すること無く，より安全な本人認証を提供することが可能である．認証過程では，下記の手順に従ってATM利用者が正規利用者か否かを判別する．

<Step1>　利用者（この時点では正規利用者か不正利用者かはまだ不明）は，ATM にキャッシュカードを挿入し，暗証番号を入力する．この時，本人認証システムは暗証番号の入力動作を撮影しておく．もしキャッシュカードまたは暗証番号のどちらかが正しくない場合は，不正利用者と見なして，この時点でATM操作を直ちに拒否する．

<Step2>　キャッシュカードと暗証番号の両方が正しい場合は，上記の<Step1>で得た動画像に対して，2.1 節で示した[Step2]～[Step5]の画像処理を施して手形状の面積時系列を抽出する．抽出した手形状の面積時系列を「認証データ」と呼ぶことにする．

<Step3> 事前に登録されている「登録データ」と「認証データ」との距離をDPマッチング[2]により求める．

<Step4> 得られた距離が閾値よりも大きい場合は，不正利用者と見なして ATM 操作を拒否する．距離が閾値以下の場合は，正規利用者と見なしてATM操作を受け付ける．

３．実験結果

提案手法の有効性を確認するために，以下に示す認証実験を行なった．なお，認証過程の<Step1>におけるキャッシュカードおよび暗証番号は正しいものとし，手形状の面積時系列を用いた認証部分について実験を行なった．

成人男性 10 名（被験者 A～J）に暗証番号「5601」を入力してもらい，暗証番号の入力動作をディジタルビデオカメラ(Sony DCR-TRV7)を使用して上方から撮影した．各人10回ずつ撮影し，前半 5 回から「登録データ」を作成し，後半 5 回から「認証データ」を作成した．なお，動画像のスペックは 30 フレーム／秒，720x480 画素，24 ビットフルカラー画像である．

登録データと認証データがともに同一の被験者のものである正当な組み合わせ 250 事例（被験者 10 名×登録データ 5 個×認証データ 5 個）と，登録データと認証データが異なる被験者のものである不正な組み合わせ 2250 事例（被験者 10 名×登録データ 5 個×認証データ 5 個×本人以外の被験者数 9 名）の合計 2500 事例について本人認証実験を行なった結果を図 4 に示す．横軸は 2.2 節<Step4>で使用する閾値の値であり，縦軸はその際の「正規利用者を不正利用者であると誤判別する割合を意味する本人棄却率(FRR: False Rejection Rate)」と「不正利用者を正規利用者であると誤判別する割合を意味する詐称者受理率(FAR: False Acceptance Rate)」である．図 4 において等誤り率(FRR = FAR における誤り率:8.0%)となる閾値に設定した場合，92.0%の精度で不正利用者を判別可能である．正規利用者ごとに異なる閾値を設定可能であるので，より高い安全性を求める利用者は閾値を小さく設定する事で不正利用者の判別率を高めることができる．ただし，この場合はFRR の低下を伴うので，許容可能な範囲で閾値の調整を行なう事が重要である．一例を挙げると，FRR が 50%となる閾値に設定した場合，FAR は 1.0%未満となり 99.0%以上の精度で不正利用者を判別可能である．

４．むすび

本論文では，ATM における暗証番号の入力動作から抽出される“手形状の面積時系列”を特徴量として用いた本人認証手法を提案した．提案手法の有効性を確認するために認証実験を行ない，等誤り率となる閾値に設定した場合に 92.0%の精度で不正利用者を判別可能であるという結果が得られた．

今後は，手形状から得ることのできる面積以外の特徴量を併用した本人認証手法を検討する予定である．

参考文献

[1] 瀬戸洋一，“サイバーセキュリティにおける生体認証技術，”共立出版, 2002.
[2] 上坂吉則, 尾関和彦，“パターン認識と学習のアルゴリズム，”pp.91-103, 文一総合出版, 1990.