SVM のバイオメトリクス認証への応用について
－分散システム下でのエージェント認証に向けて－

岡宅　泰邦*　本位田　真一**

Application of SVM to Biometrics Authentication
- An approach to agent's authentication in distributed environments -

Yasukuni OKATAKU* and Sinichi HONIDEN**

Abstract－ This presents a new biometric authentication method by applying support vector machine (SVM) in mobile computing environments. The server introduced as a biometric certification server (BCA server) can authenticate the person himself without necessity to store and manage the raw biometric data. The BCA server receives a model learned by SVM from user who wants to get authentication and only classifies the user pseudo-template data into two classes by the model, therefore it doesn't need to manage any original biometric data. The classification ability between the person himself and the others show good in a small experiment with the training data extracted from fingerprints

Key Words: SVM, support vector machine, biometrics authentication, mobile agent

1　はじめに

近年，モバイルエージェントをコンテンツ配信などに適用するさまざまな試みが提案されている[1)]．また，指紋等の生体情報を利用したセキュリティ機器の導入も進みつつある．生体情報は個人固有の情報であるため，認証のための秘密鍵を持ち歩く必要がなく本人認証できるという大きな利点がある．その一方，生体情報のエージェントへの活用時における課題として,下記のような欠点が挙げられる．

(a):生体情報読取装置によって読み取られる指紋や顔画像などの生体特徴情報(テンプレート)は，読み取り毎に全ビットデータが一致するとは限らないため，端末や認証局(BCA サーバ)での認証時に無視できない他人受理率(FAR: false accept rate)や本人拒否率(FRR: false reject rate)が常に存在する．また，いったん盗まれると代替が困難となる．

(b)BCA サーバは，膨大な:テンプレート情報を常時安全に管理する必要があり，その管理負荷は大きい．

(c):モバイルエージェント自身の所有者を特定できる方法がなかった．すなわち，モバイルエージェント自身の改ざん検知や暗号化はできても,そのエージェント自身が真正保持者により生成されたものかどうか判断はできない．

本論文では，生体情報の特徴を活かすとともに，その脆弱性を克服する手法を検討し，モバイルエージェントの保護への適用を検討することを目的としている．

2　モバイルエージェントの認証

上述した(a)～(c)の課題に対処する方法を本論文ではSVM（サポートベクターマシン）[2)]の適用を検討する．

(a)に対しては，複数のテンプレート情報による判定を行うことでエラー率を低減させる．また，生のテンプレート情報でなく，取り消し可能なようにテンプレートを変形することでテンプレートの取り消し可能な手法が提案されている[3)]．本論文でもSVMの適用時にも取り消し可能な方式となりうるか検討する．

(b)に対しては，BCAサーバでのテンプレート管理負担をなくすことが考えられるが，ニューラルネットを利用した方法が提案されている[4)]．証明者端末で証明者のテンプレート情報を訓練データとして学習させ，暗号化した学習済み重みベクトルを認証サーバに登録するものである.証明者は必要に応じて，重み情報の取消し・再登録を行うことにより，サーバでのテンプレート管理負担は解消される．本論文でもサーバでの管理負担の解消を目指す点では同じであるが，テンプレート学習方法にSVMを用いてその有効性と実用性について検討するものである．

(c)に対しては，モバイルエージェント（以下単に，エージェントと略す）内部にテンプレート情報を格納させ，それをサーバで認証することにより，エージェントの真正保持者が誰であるかを確認する．本論文では，サーバに登録したユーザの特徴情報（学習モデル：サポートベクター，ラグランジュ乗数，閾値から構成）で検証するためのテストデータ（テンプレート情報）をエージェントに格納して，エージェントがサーバに移動して認証を受けるものである．

*情報工学科　**国立情報学研究所，東京大学

2006 年 9 月 25 日受付

3　SVM による指紋テンプレート学習と判定

SVMソフトウェアとしてSVM^{light}[5]を用いる．

3.1 指紋テンプレートの SVM による学習と認証

サポートベクターマシンは，対象データ空間を２つのクラスに分類する機械学習方式の１つであり，本実験では，SVMソフトウェアとしてSVM^{light}を用いている．認証能力の検証実験は，学習と認証の２つのフェーズから成っている．学習フェーズでは，

1) 本人と他人の指紋テンプレートの抽出と入力データの作成，

2) SVM^{light}による学習，

を行い，学習モデルを生成する．認証フェーズでは，

3) 新たに生成した本人のテンプレート情報（SVMテストデータ）を学習モデルによる本人の判定（クラス分類），を行い，y_i (= sign ($\boldsymbol{w}^t\boldsymbol{x}_i - b$))の値を算出し，算出値$y_i$が+1 近傍かそれ以上で本人と判定するものである．ここで，$\boldsymbol{w}^t$は学習済み重みベクトル，$\boldsymbol{x}_i$は学習用テンプレートベクトル，bが閾値である．他人のテストデータでは，-1 近傍であることが多いが，類似したテンプレートや学習情報の精度により+1 近傍と判定される可能性がある．

学習と認証の 2 つのフェーズをエージェント認証に適用する場合の流れを図 1 に示す．

3.2 入力データ生成と学習

指紋テンプレートとし図 2 に示すように，隣接するマイニューシャ(minutia)である分岐点(bifurcation point)や端点(end point)間に含まれる隆線(ridge)であるリレーション(relation)数を用いる[6]．１つの指紋に含まれる分岐点と端点から 5～8 程度を選択して入力データを作成する．例えば，図 2 の番号 1 と周囲４点間のリレーションはベクトルで$\boldsymbol{z}_1 = {}^t(1, 0, 2, 3)$と表現でき，k個のマイニューシャ$\boldsymbol{z}_j$ (j = 1, 2, ..., k))から入力ベクトル $\boldsymbol{x}_i = {}^t(\boldsymbol{z}^i_1, \boldsymbol{z}^i_2, .., \boldsymbol{z}^i_k)$を作成する．

作成した証明者と複数の他人の入力ベクトル $\boldsymbol{x}_i$をSVM^{light}[3]で学習させ，ラグランジュ係数，閾値，サポートベクターから構成されるユーザの学習モデルを生成する．図 1 に示すように，学習したユーザのモデルを認証サーバに事前に登録しておく（モデルはサーバの公開鍵等で暗号化して送付する）．

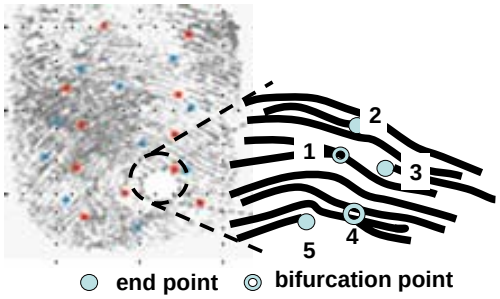

図 2 訓練データ用マイニューシャ

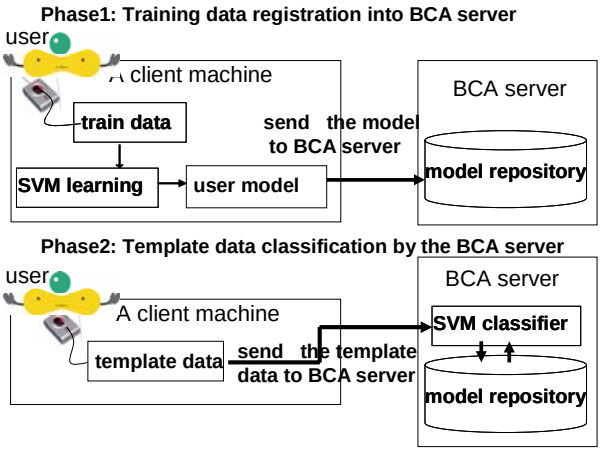

図 1 モバイルエージェント認証の流れ

3.3 モバイルエージェント認証

エージェントの動作開始時に，暗号化した証明者のテストデータ$\boldsymbol{x}_i$ をエージェント内部に格納して認証サーバに移動して認証を受ける．

4　実験結果

異なる 2 人の証明者の特定指のテンプレートによる実験結果を以下に示す．

4.1 特定指のみによる認証

判定結果を図 3a, 3b に示す．学習に用いたカーネル関数は線形とし，両図とも他人の訓練データ数を１名，２名，４名の３ケースについての分類結果を示している．学習に用いた本人データと読み取り誤差を考慮して本人のリレーション数を若干修正したテストデータはすべてほぼ+1 の判定となる．一方，非本人のテストデータによる他人判定結果は，訓練時の非本人データが１名の場合を除き，他人の判定は良好と考えられる．本人と認証する閾値を+0.8 以上とすると，図 3a, 3b の証明者が A と B の２ケースでは,FAR，FRR ともゼロである．

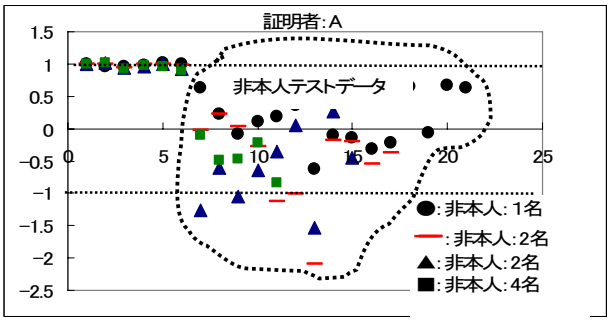

図 3.a 証明者 A の特定指での実験結果

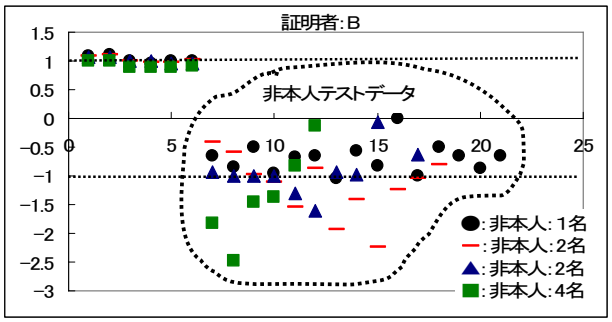

図 3b 証明者 B の特定指での実験結果

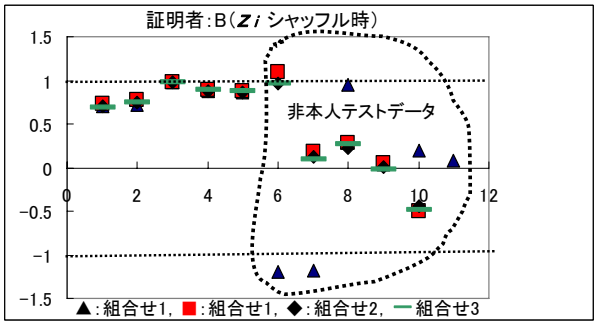

図 5 証明者 B の 2 本の指のサブテンプレートをシャッフルした時の実験結果

4.2 ２本の指による認証

２本の指による訓練データを生成し，その判定能力を実験した結果を図 4a と 4b に示す．本人と認証する閾値を+0.8 以上とすると，図 4a のテストデータが■では他人受理ケースはゼロだが，本人拒否ケースが 1/6 である一方，テストデータが▲では他人受理ケースが 1/7 存在する．ただし，本人拒否ケースのテストデータは，訓練データとのリレーション数の隔たりが他の 5 ケースに比較して大きくしたテストデータである．また，図 4b のケースでは，２種類の非本人テストデータ各 6 ケース中，他人受容ケースが各 1 ずつ存在する．

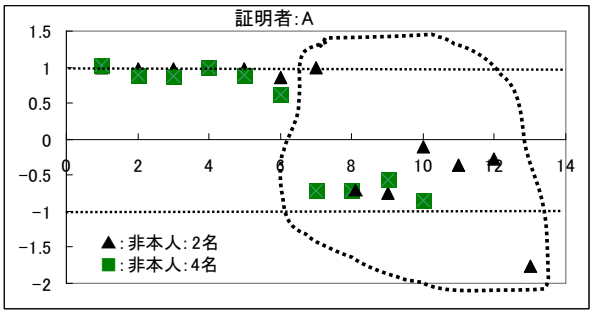

図 4a 証明者 A の 2 本の指での実験結果

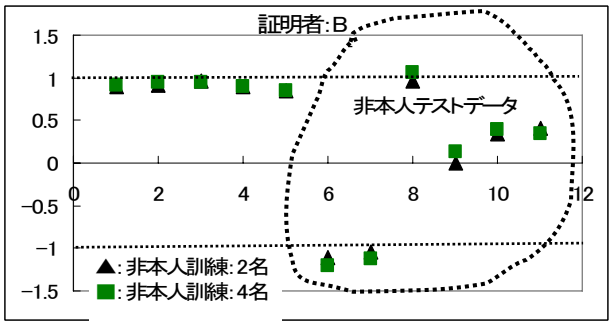

図 4b 証明 B の 2 本の指での実験結果

4.3 入力ベクトル $x_i = {}^t(z^i_1, z^i_2, .., z^i_k)$の変形処理

証明者本人の指iテンプレートであるベクトル $x_i = {}^t(z^i_1, z^i_2, .., z^i_k)$は，暗号化されて認証サーバに送付されるとはいえ，生体の特徴情報そのものであるため一旦，漏洩するとその代替は困難となる．そこで，２本の指で抽出できるマイニューシャ数は 15 個程度は可能であるため，サブベクトル$z^i_1, z^i_2, .., z^i_k$ (k≧15)をランダムにシャフリングした擬似テンプレートx'_iを本人訓練データとして使用できれば，15!の組合せから任意のテンプレートを選択できるので，取消し可能な生体認証(cancelable biometrics authentication)の可能性が開ける．図 5 は，図 4b と同一証明者の訓練データを 3 通りの並べ替えで生成したx'_iにより学習・生成したモデルを元に，同様に並べ替えた本人のテストデータおよび図.4b と同一の非本人テストデータで判定した結果である．図からわかることは，本人と推定する割合が+0.7 近傍に下がるケースもあるが，複数の認証テストにより本人との判定は可能と考えられる．一方，特定の非本人データについては，組合せを変更した学習モデルでも他人を受容する場合が存在することがわかる．

5 考察

以上の実験結果を踏まえて，本認証方式の有効性の有無を以下で考察する．

5.1 学習モデル生成には何本の指を用いるべきか

入力ベクトルx_i の次元は抽出するマイニューシャ数に比例するが，今回の実験では 1 本の指あたりで 5～8 で，ベクトル次元は 20～32 である．高次元になるほど一般に特徴空間の線形分離は難しくなるが，今回の実験でも非線形カーネルによる学習も行ったところ，線形学習以上の判定能力は得られなかった．図 3 と図 4 を比較してわかるように，1 本の指によるほうが他人受理率(FAR)は低い結果が得られている．悪意ある攻撃を想定すると，学習モデル生成はユーザ側で簡単に実行できるので，特定指による判定では異なる複数本による総合的な判定が望ましい．

5.2 取消し可能なバイオメトリクスの実現可能性

入力ベクトルx_i を構成するマイニューシャ点のサブベクトルを並べ替えて生成するx'_i を本人の擬似テンプレートとして利用するためには，安全性の点から 2 本によるテンプレートのほうが好ましい．その一方，FARの危険度は大きくなる傾向があるよ

うに思われる．

図 5 の横軸が 6, 7, 8 の非本人テストデータは, 同一人の 2 本の指の組合せで作成した入力ベクトル（例；[右中指 ‖ 左人差指], [左人差指 ‖ 右中指], [左中指 ‖ 左人差指]など）による判定結果である．同図からわかるように, 1 つの学習モデルにおいて異なる複数個のテストデータによる判定を実施することで FAR の危険を減ずることができるとともに, 異なる複数個の学習モデルも併用することで FAR，FRR とも低下できることが可能と考えられる．また, 悪意ある攻撃者はランダムに生成したテストデータによる攻撃を仕掛けるが, 複数判定による認証を行うことにより, 攻撃を回避できる可能性を高めることができる．

5.3 モバイルエージェントへの適用について

ユーザ本人の認証のみならず，当該ユーザが生成したエージェントにテストデータを格納してサーバでの認証を受けることで，その保持者を確認できるため，エージェントの真正性が保証される．エージェントが複数のサーバで作業を実行する場合は，移動前にサーバに学習モデルを送付しておけばよく，サーバがモデルを長期間管理する必要もないので，その管理負担は軽い．

5.4 双方向認証システムへの適用について

証明者サイドから発信されるエージェントの真正性保証だけでなく，ピッキングなどの詐欺行為を防止するためにも，認証サーバの真正性を保証することが必要である．サーバからも証明者サイドにサーバの真正性を示す学習モデルを送付して双方向に認証するプロトコルの導入が必要となる．

6　今後の課題

本提案手法の有効性をさらに検証し，分散システム環境下での適用を考える上で，以下の課題を検討する必要がある．

(1) 複数指のテンプレートによる学習精度の検証；多くの実験データによる SVM による学習モデルの判定能力の検証の実施．特に，他人を模擬した多数のテストデータによる検証が必要である．

(2) シャフリングによる擬似テンプレートの性能検証；多くの実験データによる FAR, FRR の定量的な推定検討が必要である．すなわち，複数の擬似テンプレートによる複数の学習モデルによる FAR, FRR の定量的評価を行う．

(3) 実装・評価；モバイルエージェントのプラットフォーム[6]への実装と実験による機能・性能評価の実施．

本論文では，バイオメトリクス情報として指紋のリレーション情報を用いたが，指紋パターンの周波数変換した情報による学習モデルやその他の特徴データによる SVM 学習モデルの有効性も検討に値すると考えられる．

謝辞

本研究の一部は, 平成 18 年度の国立情報学研究所「提案型共同研究」の支援を受けて実施したもので, ここに記して謝意を表す．また，データの収集整理にあたって，情報工学科 5 年の常国絵里子氏の協力に深く謝意を表します．

参考文献

1) 吉岡信和，田原康之，本位田真一，モバイルエージェントによる柔軟なコンテンツ流通を実現するアクティブコンテンツ，*情報処理学会論文誌：データベース*，Vol.44, No.SIG 1(TOD 20) pp 45-57 (2003 年 12 月号).

2) 大北剛（訳）, N. Cristianini and J. Shawe-Taylor，サポートベクターマシン入門．共立出版 (2005).

3) N. Ratha, J. Connel, and R. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, (2001)

4) 菊池浩明, 非対称バイオメトリクス認証プロトコルの安全性について，*SCIS 2006*, (2006).

5) T. Joachims, *SVM*^{light} *"Support Vector Machine"*, http://www.cs.cornell.edu/People/tj/svm_light/index.html, (2004).

6) 画像電子学会（編），星野幸夫（監），指紋認証技術, pp.48/49，電機大出版局

7) 石川 冬樹，吉岡 信和，田原 康之，本位田 真一，階層構造制御に注目したモバイルエージェントフレームワークとそのマルチメディア応用, *電子情報通信学会論文誌* 「ソフトウェアエージェントとその応用」特集号 Vol. J88-D-I No.9 pp 1402/1417 (2005)