情報処理学会論文誌　Vol. 51　No. 12　2319–2329 (Dec. 2010)

推薦論文

生体認証におけるWolfとLambに対する安全性の高い判定アルゴリズムの提案

村上隆夫[†1]　高橋健太[†1,†2]

生体認証において，複数の他人の生体情報に対して高いスコア（類似度）を実現する生体情報（Wolf/Lamb）の存在が示されている．このような生体情報は，他人の生体情報に対して認証誤りを容易に引き起こす恐れがあるため，生体認証の安全性を大きく低下させる要因となる．しかしながら，Wolf と Lamb の両方に対して高い安全性を持つ手法を提案し，その有効性を実験的に示した研究例は，筆者らの知る限りまだ存在していない．本稿では，テンプレートごとの他人分布を用いて得られたスコアを事後確率に正規化することで，スコアを出力するあらゆる生体認証に適用可能な，Wolf および Lamb に対する安全性の高い手法を提案する．NIST BSSR1 を用いた従来手法との比較実験を通して，提案手法が Wolf および Lamb に対して高い安全性を持つことを定量的に示す．

A Decision Algorithm for Biometric Authentication with Security against Wolves and Lambs

Takao Murakami[†1] and Kenta Takahashi[†1,†2]

The existence of Wolves/Lambs that have high similarity scores against biometric data of others is shown in biometric authentication. These biometric data can easily cause false accepts against others, making the biometric system insecure. No techniques, however, have been experimentally shown to have security against both Wolves and Lambs, to our knowledge. In this paper, we propose such a technique by normalizing the scores to the posterior probabilities using the impostor distributions specific to the template. This technique can be applied to any biometric systems that output the scores. We quantitatively show that the proposed method has security against both Wolves and Lambs through the comparison experiment using the NIST BSSR1 database.

1. はじめに

ユーザの身体的特徴，あるいは行動的特徴を用いて本人確認を行う生体認証が，利便性と安全性の両面において優れた認証手段として注目を集めている[1)]．生体認証では，システムが認証を試みるユーザから生体情報（以後，認証サンプル）を取得し，これをあらかじめ登録されている生体情報（以後，テンプレート）と照合してスコア（類似度あるいは距離）を算出することで本人確認を行う．このとき，複数の他人の生体情報に対して高いスコア（以後，類似度として定義）を実現する生体情報の存在が指摘されている[2)]．複数の他人の生体情報に対して高いスコアを実現する認証サンプルは Wolf と呼ばれており，複数の他人の生体情報に対して高いスコアを与えるテンプレートは Lamb と呼ばれている[3)]．このような生体情報は，他人の生体情報に対して認証誤り（他人受入）を容易に引き起こす恐れがあるため，生体認証の安全性を大きく低下させる要因となる．

これに対して，Wolf や Lamb に対する高い安全性を実現することを目的とした研究例がいくつか存在する[4)–7)]．しかしながら，Wolf と Lamb の両方に対して高い安全性を持つ手法を提案し，その有効性を実験的に示した研究例は，筆者らの知る限りまだ存在していない．

このようななか，筆者らは，システムが DB 内の N 個のテンプレートと順次照合を行ってユーザが誰なのかを識別する $1:N$ 認証において，複数の認証サンプル（指紋，顔，静脈など）を融合して判定を行うマルチモーダル認証技術を提案した[8),9)]．本手法は，本人/他人の生体情報どうしのスコアが従う分布（以後，本人/他人分布）を用いて，得られたスコアを事後確率に正規化し，これを判定基準としているが，文献 9) では，この際に用いる他人分布をテンプレートごとに学習することで認証精度を向上させ，さらに Wolf と Lamb の両方に対しても高い安全性を実現できることを考察した．

本稿では文献 9) の考察をもとに，より一般的な生体認証，すなわち，ユーザが 1 つの認証サンプルのみを入力し（ユニモーダル），システムが 1 つのテンプレートと照合を行って本人か他人を判定する認証（1 : 1 認証）において，Wolf と Lamb の両方に対して高い安全性を持つ手法を提案する．本手法はスコアのみを用いているため，スコアを出力するあらゆ

†1 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†2 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
本稿の内容は 2009 年 10 月のコンピュータセキュリティシンポジウム 2009（CSS2009）にて報告され，CSEC 研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

る生体認証に適用可能な，汎用性の高い手法である．また本稿では，提案手法の Wolf および Lamb に対する安全性評価を行う．具体的には，NIST BSSR1（Biometric Scores Set - Release 1）Set2 [10] を評価用データとした評価実験を行い，提案手法が Wolf と Lamb の両方に対して高い安全性を持つことを定量的に示す．

2. Wolf と Lamb

2.1 生体認証における Wolf と Lamb の問題

文献 2) では声紋認証において，複数の他人の生体情報に対して高いスコアを実現する認証サンプル（Wolf），およびテンプレート（Lamb）が存在することを示している．また，文献 11) ではあらゆる生体情報に対して，非常に高いスコアを実現する認証サンプル（Universal Wolf）の存在を指摘している⋆1．本稿では，同様にあらゆる生体情報に対して，非常に高いスコアを実現するテンプレートを Universal Lamb と呼ぶ．その一方で，ある生体情報に対しては高いスコアを，別の生体情報に対しては低いスコアを実現するような Wolf, Lamb を，それぞれ曖昧な Wolf，曖昧な Lamb と呼ぶことにする．

このようなユーザが生体認証に与える影響を考える．1 : 1 認証では，一般的には得られたスコアが認証閾値以上であれば本人，そうでなければ他人と判定することで認証を行う（以後，スコア判定法）．このとき，ユーザは Wolf を提示することで複数の他人に対してなりすましが可能となり，Lamb を登録したユーザは複数の他人から容易になりすましが行われる恐れがある．1 : N 認証でも同様のことがいえるが，特に 1 : N 認証において Lamb が登録されている場合は，なりすましを試みる意図の有無に関係なく，複数のユーザがその Lamb を登録したユーザとして識別されてしまい，認証システムとしての機能が大きく損なわれる危険性もある．したがって，Wolf と Lamb は 1 : 1 認証，1 : N 認証のいずれにおいても安全性を大きく低下させる要因である．

2.2 Wolf と Lamb に対する安全性の評価指標

1 : 1 認証における精度の評価指標として，FRR（False Reject Rate：本人拒否率）と FAR（False Accept Rate：他人受入率）の 2 つが従来より定義されている．FRR はシステムが本人を誤って他人として判定してしまう誤り率であり，FAR はシステムが他人を誤って本人として判定してしまう誤り率である．人工物 [12] を除いた認証サンプル，テンプレートの集合をそれぞれ V，E とし，認証サンプル $v \in V$ とテンプレート $e \in E$ を照合することで得られた認証結果を $match(v, e) \in \{\text{accept, reject}\}$ とすると，FAR は，

$$\mathrm{FAR} = \underset{v \in V}{Ave} \ \underset{e \in E, e \not\sim v}{Ave} \ P(match(v, e) = \text{accept}) \tag{1}$$

と表せる．ただし，$P(match(v, e) = \text{accept})$ は認証結果 $match(v, e)$ が accept となる確率値を表し，$\underset{v \in V}{Ave}\ X$ は $v \in V$ に関して X の平均値をとったものである．また，$e \not\sim v$ はテンプレート e と認証サンプル v がそれぞれ別々のユーザから提示されたことを表すものとする．すなわち，FAR は全認証サンプルおよび全テンプレートに対して他人受入が発生する確率の平均値をとったものである．

Wolf に対する安全性の評価指標としては，文献 11) が WAP（Wolf Attack Probability）を定義している．これは，以下の式で表される⋆2．

$$\mathrm{WAP}' = \underset{v' \in V'}{max} \ \underset{e \in E}{Ave} \ P(match(v', e) = \text{accept}) \tag{2}$$

ただし，v' は人工物 [12] までも含めた認証サンプル，V' はその集合であり，$\underset{v' \in V'}{max}\ X$ は $v' \in V'$ に関して X の最大値をとったものである．すなわち，WAP′ はユーザが人工物も含めて，最も数多くのテンプレートに対して認証成功となる認証サンプルを提示したときに，その認証が成功となる確率値である．

しかしながら，人工物に対しては現在，様々な生体検知技術 [13] が提案されている．その一方で，人間の生体情報を用いた攻撃は，たとえ生体検知技術を用いても防ぐことができないため，人工物を用いた攻撃とは切り離して考える必要がある．本稿では人工物を用いた攻撃は生体検知技術で対応するものとし，人工物以外の Wolf に対する安全性の評価指標として，文献 6) と同様に，以下の式で定義される WAP を用いる⋆3．

$$\mathrm{WAP} = \underset{v \in V}{max} \ \underset{e \in E, e \not\sim v}{Ave} \ P(match(v, e) = \text{accept}) \tag{3}$$

これは，最も他人受入を引き起こしやすい認証サンプルを持つユーザがなりすましを試みたときに，それが成功となる確率値である．

本稿では，Lamb に対する安全性の評価指標についても上記と同様に考え，以下の式で表される LAP（Lamb Accept Probability）を新たに定義する．

⋆1 文献 11) ではスコアを距離として定義しているが，本稿では類似度として定義したうえで大小関係を逆にしている．

⋆2 本稿で評価に用いる WAP と区別するため，文献 11) で定義されている WAP を WAP′ と表記する．

⋆3 文献 11) の WAP′ では，テンプレートと認証サンプルが同一人物によって提示された場合も含まれているが，本稿で用いる WAP では，そのような場合を除外する（すなわち，他人受入が起こる場合のみを考慮する）．

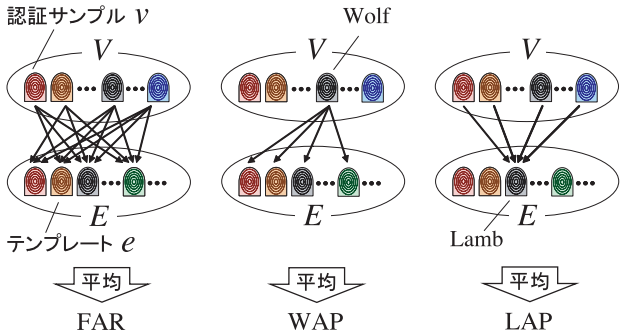

図 1　他人受入に関する安全性の評価指標（FAR/WAP/LAP）
Fig. 1　Security measures related to false accepts (FAR/WAP/LAP).

$$\mathrm{LAP} = \max_{e \in E} \operatorname*{Ave}_{v \in V, v \not\sim e} P(match(v, e) = \mathrm{accept}) \tag{4}$$

これは，最も他人受入を引き起こしやすいテンプレートを登録したユーザが，他人によるなりすまし攻撃を受けたときに，それが成功となる確率値である．

他人受入に関する評価指標である FAR，WAP，および LAP を**図 1** に示す．FAR はあらゆる他人同士の生体情報を照合して誤り率の平均値をとったものであり，WAP，LAP はそれぞれ最も他人受入を引き起こしやすい認証サンプル（Wolf），テンプレート（Lamb）を他人の生体情報と照合して誤り率の平均値をとったものである．WAP，LAP を実験的に評価する際には，なるべく多くの他人受入を引き起こす Wolf，Lamb が評価用データの中に含まれるよう，十分多くの評価用データを用意すべきである．

なお，1 : N 認証に関しては，精度の評価指標（EFRR/EFAR/NFAR）が筆者らによって定義されており[8]，Wolf に対する安全性の評価指標（1 : N 認証における WAP）が文献 11) で議論されている．ただし，本稿では 1 : 1 認証において Wolf/Lamb に対して安全性の高い手法を提案し，安全性評価を行う．1 : N 認証における安全性評価は，本稿では扱わない．

3. 従 来 手 法

Wolf あるいは Lamb に対して高い安全性を実現することを目的とした研究例がいくつか存在する[4)–7)]．これらはいずれも，認証時において認証サンプルが Wolf，あるいはテンプレートが Lamb であっても，なりすましが起きにくくなるよう対策を施すものとして提案されている．

文献 4) では，認証時にテンプレートのほかに，あらかじめ用意しておいた $N-1$ 個のテンプレート（以後，ダミーテンプレート）とも照合を行って（計 N 個と照合），テンプレートに対する認証結果が accept であった場合でも，計 T（$\leq N$）個以上の生体情報に対して認証結果が accept であったときは他人と判定する手法（以後，人数閾値法）を提案している．この手法は，認証結果（accept/reject）を出力するあらゆる生体認証に適用可能なため汎用性が非常に高いが，Wolf に対する高い安全性を実現することのみを目的としている．テンプレートが Lamb であったとしても，ダミーテンプレートに対する認証結果（accept/reject）には影響を与えないため，この手法は認証時における Lamb への対策にはなっていないと考えられる（これについては，5 章で実験的に検証する）．

文献 5) では，ユーザが（人工物も含めた）認証サンプル $v' \in V'$ を提示した後，システムがテンプレートの集合 E から任意のテンプレートを選択したときに，そのテンプレートとの距離が x より小さくなる確率値 $P(v', x)$ を求め，これが δ 未満となるような x の最大値を距離に対する閾値としたうえで，テンプレート e との照合を行う手法を提案している．文献 5) は，この手法を用いることで WAP′ が δ まで抑えられることを理論的に示している．確率値 $P(v', x)$ の具体的な算出方法として，文献 5) では各ユーザ $u \in U$（U は全人類の集合）から十分多くのテンプレートを取得して各ユーザの特徴量分布 $P(X_u = t)$ を学習しておき（X_u はユーザ u のテンプレートを表す確率変数であり，$t \in E$ はその実現値），認証時にそれらを用いて，

$$P(v', x) = \frac{1}{|U|} \sum_{u \in U} \sum_{\substack{t \in E \\ d(v', t) < x}} P(X_u = t) \tag{5}$$

と求める方法を提案している（$|U|$ は全人類の数，$d(v', t)$ は認証サンプル v' とテンプレート t との距離）．

しかしながら，特徴量の次元数が高い場合や，生体情報を取得するたびに特徴量の次元数が変化する場合には，特徴量分布の学習は非常に困難である（たとえば，虹彩認証における特徴量（アイリスコード）は数千次元であり，指紋におけるマニューシャの数は，指紋を取得するたびに変化する恐れがある[14)]）．また，この手法は特徴量抽出や照合アルゴリズムの内部仕様が不明な場合には適用できない．したがって，文献 5) は汎用性に欠けるという問題がある．また，$P(v', x)$ はテンプレート e との照合を行う前に求める値であり，テンプレート e に依存せずに決まる．したがって，それが Lamb であったとしても $P(v', x)$ は変

わらず，閾値も変わらない．すなわち，この手法も Lamb への対策になっているとはいえない．

文献 6) では，認証サンプル $v \in V$ とテンプレート $e \in E$ とのスコア $s(v,e)$ を求めた後，テンプレートの集合 E から任意のテンプレート $t \in E$ を選択した場合のスコア $s(v,t)$ が $s(v,e)$ より大きくなるような確率値（偶然一致確率）ACP(v,e) を求め，これが閾値 A_{th} よりも小さければ本人，大きければ他人とする手法を提案している．ACP(v,e) は，以下の式で定義される．

$$\mathrm{ACP}(v,e) = \frac{1}{|E|}\sum_{t \in E} P(s(v,t) > s(v,e)) \tag{6}$$

文献 6) も，この手法を用いることで WAP が A_{th} まで抑えられることを理論的に示しており，また，ユーザが人工物を含めた認証サンプル $v' \in V'$ を提示した場合においても，WAP′ が A_{th} まで抑えられることを示している．ACP(v,e) の算出方法の具体例として，文献 6) では指紋のマニューシャマッチングにおいて，特徴点（マニューシャ）が指紋領域において一様に分布するという仮定をおいたうえで ACP(v,e) を計算する手法を提案している．

しかしながら，特徴量が一様に分布するという仮定は一般的に成立せず，また文献 5) 同様，これも特徴量抽出や照合アルゴリズムの内部仕様が不明な場合には適用できない．したがって，この手法も汎用性の観点で課題がある．また，e が Lamb の生体情報であったとしても，$s(v,t)$ には影響がなく（t と e が他人同士の生体情報の場合），一方で $s(v,e)$ は高くなるため ACP(v,e) は小さくなる．したがって，この手法も Lamb への対策になっていないと考えられる．文献 6) では，アルゴリズムレベルでは認証サンプルの集合 V とテンプレートの集合 E に差はなく，これらを交換することで Lamb に対する高い安全性を実現できることを述べている．しかしながら，この場合は Wolf に対する安全性と Lamb に対する安全性の関係が逆転するため，Wolf への対策が考慮されないことになると考えられる．

文献 7) は，Lamb の存在を考慮したうえでのマルチモーダル認証技術を提案している．ここでは，登録時にテンプレートを提示したユーザに対して，そのユーザの生体情報どうしのスコアが従う分布（本人分布）と，他人の生体情報とそのユーザの生体情報とのスコアが従う分布（他人分布）との分離度合いを表す d-prime を，モダリティ（生体情報の種類）ごとにあらかじめ求めておく（これを lambness metric と定義）．認証時には，これを全モダリティに対する総和が 1 となるように正規化したものを重み係数として，各モダリティに対するスコアの重み付け和を求め，閾値と比較する．まず，この手法はユニモーダル認証には適用できず（重み係数が 1 となり，スコアを閾値と比較するスコア判定法と等価になるため），汎用性が低い．また，この手法は Lamb に対しては高い安全性を持つ可能性があるが，理論的，あるいは実験的な検証がなされておらず，その有効性は不明である．さらに，全認証サンプルの中に Wolf が存在していたとしても，その割合がごくわずかであれば他人分布，および d-prime に与える影響は小さいため，この手法は Wolf への対策になっていないと考えられる．

以上のとおり，認証時に Wolf と Lamb の両方に対する安全性を同時に向上させる手法は筆者らの知る限り，提案されていないのが現状である．ただし，Wolf は認証時に提示されるのに対して Lamb は登録時に提示されるため，Lamb に対しては登録時にテンプレートが Lamb か否かの判定を行い，Lamb と判定した場合は別の生体情報を再登録させるなどの対策を事前に施すことができる．たとえば，人数閾値法[4] と同様の考えを用いて，登録時に提示されたテンプレートを N 個のダミーテンプレートと照合してスコアを求め，計 T 個以上のダミーテンプレートに対してスコアが閾値 s_{th} 以上であれば（すなわち，認証結果が accept であれば）Lamb と判定する方法が考えられる．

しかしながら，ある生体情報に対しては高いスコアを，別の生体情報に対しては低いスコアを実現するような曖昧な Lamb に対しては，登録時に検出が困難な場合がある．このような Lamb が誤って登録されると，それ以降の生体認証の安全性が低下する恐れがある．閾値 s_{th} やパラメータ T を小さくすれば，曖昧な Lamb も検出できるようになるが，その場合は逆に，Lamb でない生体情報を Lamb と判定する判定誤りの件数が増加し，そもそも登録ができないユーザの数が増えてしまう恐れがある．以上のことを考慮し，認証時における（曖昧な Lamb も含めた）Lamb への対策を，Wolf への対策とともに講じておくことが重要であると考える．

4. Wolf および Lamb に対する安全性の高い生体認証

筆者らは，$1:N$ 認証において生体情報の入力回数を最小限に抑えつつ認証精度を高めるマルチモーダル認証技術を提案した[8),9)]．本手法は，本人/他人の生体情報どうしのスコアが従う分布（本人/他人分布）を用いて，スコアを事後確率に正規化しているが，文献 9) では，他人分布をテンプレートごとに学習することで認証精度を向上させ，さらに Wolf と Lamb の両方に対しても高い安全性が得られることを考察した．

本章では文献 9) の考察をもとに，ユニモーダルの $1:1$ 認証において，Wolf と Lamb の両方に対して高い安全性を実現する手法を提案する．これは，ユニモーダルの $1:1$ 認証の方がより一般的に用いられている生体認証であり，安全性評価も容易に行えるためである．

また，提案手法は認証時において Wolf と Lamb への対策を施すものであるが，この手法が（曖昧な Wolf と曖昧な Lamb を含めた）Wolf と Lamb の両方に対して高い安全性を持つと考えられる理由を述べる．

4.1　提案手法のアルゴリズム

以下，本稿で提案する手法について説明する．まず，テンプレートのほかに認証サンプル v との照合を行うダミーテンプレート（$N-1$ 個）を用意しておく．ダミーテンプレートとしては，DB に登録されている他のテンプレートを用いてもよいし，システムがあらかじめ用意しておいた生体情報を用いてもよい．本稿では，認証サンプルとの照合を行うテンプレートおよびダミーテンプレートを合わせて被照合テンプレート $r_1, \cdots, r_N$ と呼ぶことにする（r_1 はテンプレート，$r_2, \cdots, r_N$ はダミーテンプレート）．被照合テンプレート $r_1, \cdots, r_N$ に対して得られたスコアをそれぞれ $s_1, \cdots, s_N$ とし，全スコアの集合を，

$$S = \{s_i | 1 \leq i \leq N\} \tag{7}$$

とおく．提案手法では，

仮説 H_i：「認証サンプル v は被照合テンプレート r_i と同一人物のものである」（$1 \leq i \leq N$）

仮説 H_0：「認証サンプル v はどの被照合テンプレートとも異なるユーザのものである」

という仮説を定義し，スコア集合 S が得られたときに各仮説 H_i（$0 \leq i \leq N$）が真である事後確率 $P(H_i|S)$（$0 \leq i \leq N$）を求める．その後，仮説 H_1（すなわち，認証サンプル v がテンプレート r_1 と同一人物のものであるという仮説）に対する事後確率 $P(H_1|S)$ を閾値 P_{th} と比較し，$P(H_1|S) > P_{th}$ であれば本人，そうでなければ他人と判定する．$P(H_1|S)$ 以外の事後確率 $P(H_i|S)$（$i = 0,\ 2 \leq i \leq N$）は求めなくてもよいが，本稿では説明の都合上，これらも求めるものとする．

以下，事後確率 $P(H_i|S)$ の算出方法を説明する．これは，ベイズの定理より以下のように変形できる．

$$P(H_i|S) = \frac{P(H_i)Z_i}{\sum_{n=0}^{N} P(H_n)Z_n} \tag{8}$$

ただし，$P(H_i)$ はスコア集合 S が得られる前段階（すなわち，生体情報の入力前）において，仮説 H_i が真である事前確率であり，システム側であらかじめ設定しておく．また，Z_i は，

$$Z_i = \frac{P(S|H_i)}{P(S|H_0)} \tag{9}$$

で表される尤度比である（$0 \leq i \leq N$）．

尤度比 Z_i は以下のように算出する．まず，確率密度 $P(s_i|H_j)$ が任意の i，j に対し，

$$P(s_i|H_j) = f(s_i) \ (\text{if } i = j) \tag{10}$$

$$P(s_i|H_j) = g_i(s_i) \ (\text{if } i \neq j) \tag{11}$$

と表せると仮定する．$f()$，$g_i()$ はそれぞれ本人同士のスコアが従う分布（本人分布），他人の生体情報と被照合テンプレート r_i とのスコアが従う分布（他人分布）である（$1 \leq i \leq N$）．すなわち，本人分布は全被照合テンプレート共通のものを 1 つ用意し，他人分布は被照合テンプレート r_i（$1 \leq i \leq N$）ごとに用意する．このとき，全スコアが独立であると仮定すれば，式 (9) の尤度比 Z_i は，

$$\begin{aligned} Z_i &= \frac{P(s_i|H_i)\prod_{n\neq i} P(s_n|H_i)}{P(s_i|H_0)\prod_{n\neq i} P(s_n|H_0)} \\ &= \begin{cases} f(s_i)/g_i(s_i) & (\text{if } i \neq 0) \\ 1 & (\text{if } i = 0) \end{cases} \end{aligned} \tag{12}$$

と求めることができる．$f()$ および $g_i()$ は，正規分布などのモデルを仮定したうえで，そのパラメータを被照合テンプレートや，分布学習用に収集しておいた生体情報を用いてあらかじめ学習しておく．あるいは，式 (12) より尤度比 Z_i は，確率密度 $f(s_i)$ と確率密度 $g_i(s_i)$ の比 $f(s_i)/g_i(s_i)$ で表されるので，尤度比 $f(s)/g_i(s)$ のスコア s に対する特性をロジスティック回帰[8),15)] を用いて学習してもよい．ロジスティック回帰を用いることの有効性は文献 8)，15) に記されている．

以下，提案手法のアルゴリズムをまとめる．

1. 生体情報が入力された後，照合を行ってスコア集合 $S = \{s_i | 1 \leq i \leq N\}$ を求める．
2. 式 (12) により尤度比 Z_i（$0 \leq i \leq N$）を算出する（あらかじめ本人分布 $f()$ と他人分布 $g_i()$，あるいは尤度比 $f()/g_i()$（$1 \leq i \leq N$）を学習しておく）．
3. 式 (8) により事後確率 $P(H_i|S)$（$0 \leq i \leq N$）を算出する．
4. $P(H_1|S)$ を閾値 P_{th} と比較し，$P(H_1|S) > P_{th}$ であれば本人，そうでなければ他人と判定する．

提案手法に基づいてユニモーダルの 1 : 1 認証を行う様子を**図 2** に示す．これは文献 9) の手法において，生体情報の入力回数の上限値を 1 とし（ユニモーダル），事後確率 $P(H_i|S)$（$i = 0,\ 2 \leq i \leq N$）に対する閾値を 1 にして識別しないようにしたもの（1 : 1 認証）に相当する．

4.2　提案手法の Wolf および Lamb に対する安全性に関する考察

提案手法が Wolf および Lamb に対して持つ安全性について考察する．以下，各仮説の事前確率 $P(H_i)$（$0 \leq i \leq N$）はすべて等しいとする．

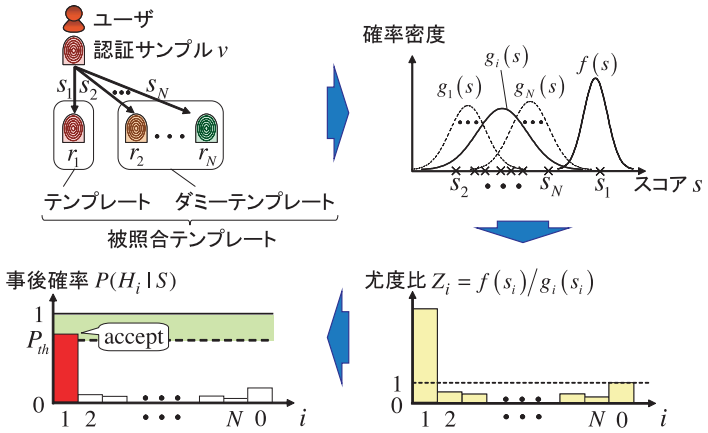

図 2　提案手法に基づくユニモーダルの 1 : 1 認証
Fig. 2　Unimodal biometric verification using the proposed method.

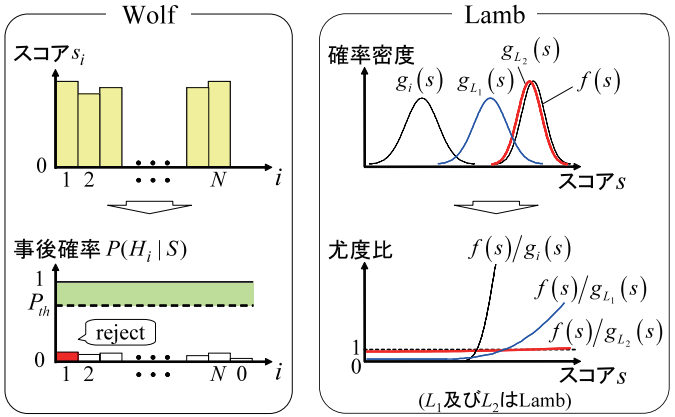

図 3　提案手法が持つ Wolf および Lamb に対する安全性
Fig. 3　Security of the proposed technique against Wolf and Lamb.

まず，提案手法の Wolf に対する安全性について考察する．提案手法では，各被照合テンプレートに対するスコアをもとに尤度比を求め，これを事後確率に正規化する．このとき，複数の被照合テンプレートに対して高いスコア（および尤度比）を実現する認証サンプル（Wolf）を持つユーザが認証を試みたとしても，全仮説の事後確率の総和はつねに 1 であるため，事後確率 $P(H_1|S)$ は低い値として算出される（**図 3**）．たとえば，ユーザが Universal Wolf を提示した結果，すべての被照合テンプレートに対して非常に高い尤度比 Z_i（$1 \leq i \leq N$）が等しく得られた場合，式 (8) より事後確率 $P(H_1|S)$ はおよそ $1/N$ となる．したがって，閾値をより高く設定すれば，その Universal Wolf を提示したユーザは認証失敗となる．また，高いスコア（および尤度比）が得られるダミーテンプレートの数が多ければ多いほど，事後確率 $P(H_1|S)$ は小さい値となるので，ダミーテンプレートの増加にともない，曖昧な Wolf も含めた Wolf に対する安全性が向上すると考えられる．ダミーテンプレート数と WAP との関係は，次章で実験的に検証する．

次に，提案手法の Lamb に対する安全性について考察する．提案手法では被照合テンプレートごとに他人分布 $g_i()$（あるいは尤度比 $f()/g_i()$）を学習する．このとき，複数の他人の生体情報に対して高いスコアを実現するテンプレート（Lamb）の他人分布 $g_{L_1}(s)$（あるいは $g_{L_2}(s)$）は，スコアの高い領域に位置するものとして学習される（図 3）．したがって，認証時にこのテンプレート（Lamb）に対して高いスコア s が得られたとしても，尤度比 $f(s)/g_{L_1}(s)$（あるいは $f(s)/g_{L_2}(s)$）は小さくなり（図 3），これを全仮説に対する総和が 1 となるよう正規化した事後確率も同様に小さい値となる．したがって，提案手法は Lamb に対しても高い安全性を持つと考えられる．たとえば，Lamb の他人分布 $g_{L_2}(s)$ が本人分布 $f(s)$ とほぼ一致するものとして学習された場合，そのテンプレートに対する尤度比 Z_1 はつねにほぼ 1 となる（図 3）．これは尤度比 Z_0 と等しく（式 (12) 参照），事後確率 $P(H_1|S)$ が 0.5 を超えることはない（式 (8) 参照）．したがって，閾値をより高く設定すれば，その Lamb を登録したユーザとして認証成功となることはない．

また，図 3 から分かるように，提案手法では他人分布がスコアの高い領域に位置するほど（テンプレートの Lamb 度合いが大きいほど），同じ尤度比の値を得るために必要なスコアの値が高くなる．したがって，テンプレートの Lamb 度合いが大きいほど，より高いスコアが認証成功となるために必要となる．3 章において，登録時の Lamb 対策では曖昧な Lamb に関する検出誤りが問題となることを述べたが，提案手法ではこのようにテンプレートの Lamb 度合いに応じて，認証成功となるために必要なスコア値を制御することで，曖昧な Lamb から Universal Lamb に至るまでの Lamb 対策を柔軟に施すことが可能となる．

以上をまとめると，提案手法はスコアから尤度比を求める際に，被照合テンプレートごとの他人分布を用いることで Lamb に対する安全性を実現し，求めた尤度比を事後確率に正規化することで Wolf に対する安全性を実現するものと考えられる．

5. 提案手法の Wolf および Lamb に対する安全性評価

5.1 実 験 条 件

提案手法の Wolf および Lamb に対する安全性を定量的に評価するための実験を行った．本実験で用いたデータは，NIST BSSR1（Biometric Scores Set - Release 1）Set2[10] である．このデータは，6,000 人の被験者からそれぞれ左手および右手の指紋（登録用，認証用に 1 つずつ）を収集し，その各々の生体情報を総当りに照合することで得られたスコアのセット（左手，右手それぞれスコアの数は 6,000 × 6,000 個）である．また本実験では，左手の指紋のスコアセットを用いた．

6,000 個の指紋のうち，4,501 個を認証サンプル，あるいはテンプレートとして，999 個をダミーテンプレートとして，残りの 500 個を分布学習用として用いることにした．そして，任意の認証サンプルを提示し，任意のテンプレートに対して 1 : 1 認証を試みる実験を行った（本人/他人同士による認証試行は，それぞれ 4,501 回，4,501 × 4,500 = 20,254,500 回）．

分布の学習は，ロジスティック回帰によって尤度比（$f()/g_i()$ あるいは $f()/g()$）を直接学習することで行った．このときの他人分布は被照合テンプレート r_i（$1 \leq i \leq N$）ごとに用意する場合と，全被照合テンプレート共通のものを用いる場合の両方を試みた．被照合テンプレート r_i（$1 \leq i \leq N$）の尤度比 $f()/g_i()$ は，分布学習用の全指紋から得られた本人スコア（500 個）と，分布学習用の全指紋を被照合テンプレート r_i と照合して得られた他人スコア（500 個）を用いて学習した．全被照合テンプレート共通の尤度比 $f()/g()$ は，分布学習用の全指紋を総当り照合して得られた本人スコア（500 個）と，他人スコア（500 × 499 = 249,500 個）を用いて学習した．また，事前確率はすべて等しくなるように $P(H_i) = 1/(N+1)$（$0 \leq i \leq N$）とした．

以上の実験条件で閾値を様々な値に変化させたときの，提案手法の FRR-WAP 曲線，FRR-LAP 曲線，および FRR-FAR 曲線を求めた．この際，比較のため，従来手法としてスコア判定法と人数閾値法[4] を用いた場合の評価も行った．本実験で評価を行った手法は，以下のとおりである．

- **スコア判定法：**
  テンプレートに対して得られたスコアを閾値 s_{th} と比較する手法
- **人数閾値法：**
  各被照合テンプレートに対して，得られたスコアを閾値 s_{th} と比較することで認証結果（accept/reject）を求め，テンプレートに対する認証結果が accept であった場合でも，計 T（$\leq N$）個以上の被照合テンプレートに対して認証結果が accept であったときは他人と判定する手法
- **提案手法（事後確率/共通）：**
  全被照合テンプレート共通の他人分布を用いて事後確率 $P(H_1|S)$ を算出後，閾値 P_{th} と比較する手法
- **提案手法（尤度比/被照合テンプレートごと）：**
  被照合テンプレートごとの他人分布を用いて尤度比 Z_1 を算出後，閾値 P_{th} と比較する手法
- **提案手法（事後確率/被照合テンプレートごと）：**
  被照合テンプレートごとの他人分布を用いて事後確率 $P(H_1|S)$ を算出後，閾値 P_{th} と比較する手法

人数閾値法に関しては，人数に対する閾値 T として $T = 4$，40，400 の 3 通りを試みた．また，提案手法に関しては「提案手法（事後確率/共通）」，「提案手法（尤度比/被照合テンプレートごと）」，「提案手法（事後確率/被照合テンプレートごと）」の 3 つを評価したが，これはスコアから尤度比を求めてそれを事後確率に正規化する効果（Wolf に対する安全性向上）と，被照合テンプレートごとの他人分布を用いて尤度比を求める効果（Lamb に対する安全性向上）とがそれぞれ明確になるようにするためである（評価 1）．

また，上記の評価実験におけるダミーテンプレート数は 999 個であるが，提案手法におけるダミーテンプレート数と WAP との関係を調べるため，「提案手法（事後確率/被照合テンプレートごと）」においてダミーテンプレート数を 9，99，999 個（すなわち $N = 10$，100，1,000）と変化させたときの FRR-WAP 曲線も求めた（評価 2）．

5.2 実 験 結 果

5.2.1 評価 1：従来手法との比較

スコア判定法，人数閾値法，および提案手法の FRR-WAP 曲線，FRR-LAP 曲線，および FRR-FAR 曲線を**図 4** に示す．ただし，人数閾値法ではスコアに対する閾値を小さくしすぎると，ある時点から FAR と FRR がともに上昇してしまう[4] ため，その部分は省略している．また，人数閾値法において，人数に対する閾値 T を小さくすると FRR が上昇し，$T = 4$ のときは FRR > 24%と FRR が非常に大きくなってしまったため，図 4 には表示していない（代わりに，**表 1** に人数閾値法（$T = 4$）の FRR < 25%における性能を表示）．

図 4 から，人数閾値法ではスコア判定法と比べて FRR が 6%付近（$T = 400$ のとき），および 15%付近（$T = 40$）のときに WAP を少し低減させることができているが，LAP は

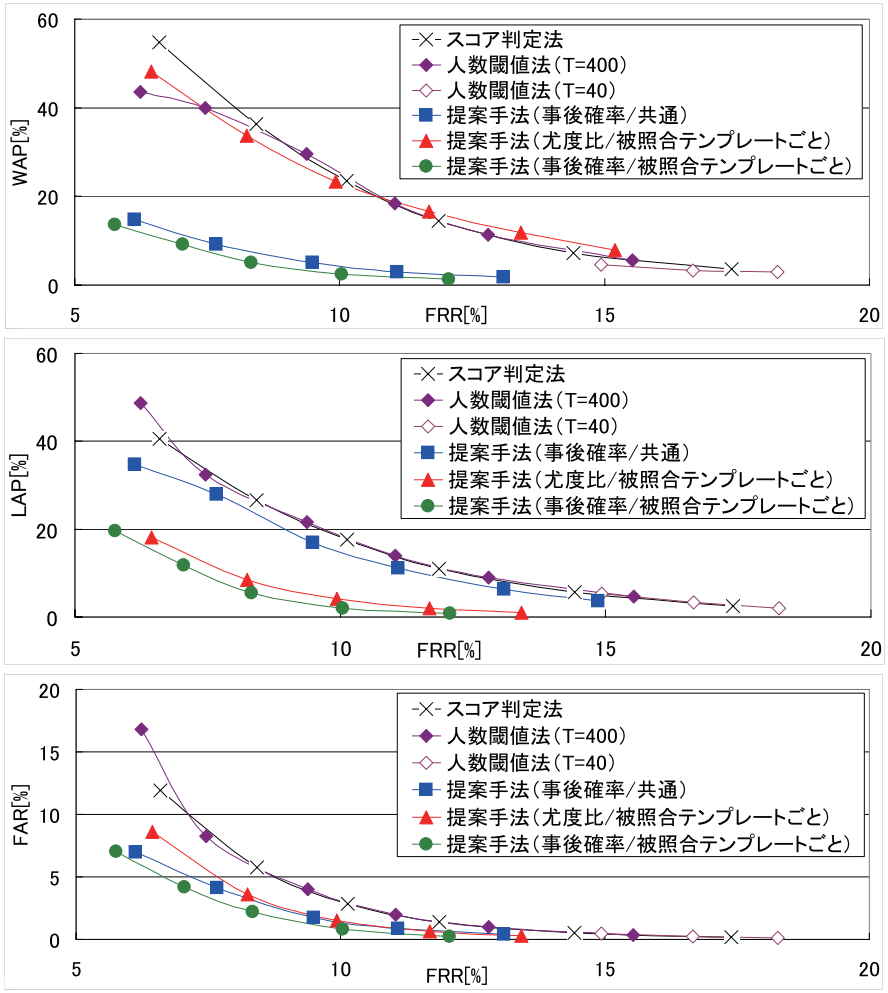

図 4　従来手法と提案手法の性能（FRR-WAP 曲線/FRR-LAP 曲線/FRR-FAR 曲線）
Fig. 4　The performance of the conventional techniques and the proposed technique (FRR-WAP curve/FRR-LAP curve/FRR-FAR curve).

表 1　従来手法と提案手法の WAP/LAP/FAR（上：FRR < 7.5%，下：FRR < 25%）
Table 1　WAP/LAP/FAR in the conventional techniques and the proposed technique (top: FRR < 7.5%, bottom: FRR < 25%).

FRR < 7.5%のときの性能

	WAP	LAP	FAR
スコア判定法	45%	32%	8.3%
人数閾値法（$T = 400$）	40%	32%	8.2%
提案手法（事後確率/被照合テンプレートごと）	6.9%	8.6%	3.1%

FRR < 25%のときの性能

	WAP	LAP	FAR
スコア判定法	0.53%	0.33%	0.010%
人数閾値法（$T = 4$）	0.42%	0.31%	0.0094%
提案手法（事後確率/被照合テンプレートごと）	0.044%	0.044%	0.0005%

まったく低減させることができていないことが分かる．WAP の低減度合いが小さかったのは，ある生体情報に対しては高いスコアを，別の生体情報に対しては低いスコアを実現するような曖昧な Wolf に対する安全性を向上させることができなかったためと考える．たとえば，テンプレートを含む計 $T-1$ 個の被照合テンプレートに対しては閾値 s_{th} 以上，その他の被照合テンプレートに対してはすべて閾値 s_{th} 未満のスコアを実現するような Wolf が提示された場合，人数閾値法では認証成功となる．LAP をまったく低減させることができなかったのは，3 章での考察が実験結果にも現れたものといえる（すなわち，人数閾値法は認証時における Lamb 対策になっていない）．

一方，提案手法ではスコア判定法と比べて，スコアから尤度比を求めてそれを事後確率に正規化することで WAP を大幅に低減させ（事後確率/共通），被照合テンプレートごとの他人分布を用いて尤度比を求めることで LAP を大幅に低減させることができている（尤度比/被照合テンプレートごと）ことが分かる．また，この 2 つを組み合わせることで，WAP および LAP の大幅な低減が実現できている（事後確率/被照合テンプレートごと）．これは，4.2 節での考察どおり，事後確率に正規化することで Wolf に対する安全性を，被照合テンプレートごとの他人分布を用いることで Lamb に対する安全性を向上させることができたことを意味する．

提案手法が人数閾値法と比較しても，WAP を大幅に低減させることができているのは，提案手法では各被照合テンプレートに対するスコアを，人数閾値法のように 2 値の離散的な情報（accept/reject）にまでそぎ落とすのではなく，その連続的な大小関係を保ったまま事後確率に正規化するためと考える．たとえば，人数閾値法では閾値 s_{th} 未満のスコアに対

しては，すべて reject という判定結果まで情報をそぎ落とすが，提案手法ではそのようなスコアの中でも s_{th} に近い値のものが多ければ，テンプレートの事後確率は小さく算出され，他人受入が起こりにくくなる．このように提案手法では曖昧な Wolf に対してより柔軟に，安全性の高い認証を行うことができ，それが実験結果に現れたものと考える．

また，「提案手法（事後確率/被照合テンプレートごと）」が WAP，LAP ともに最も良い性能を実現しているが，これはユーザが Wolf を提示して，Lamb を登録したユーザに対してなりすましを試みるような場合に対しても安全性が向上したためと考えている．また，提案手法では FAR も低減させることができているが，これは Wolf や Lamb のように，複数の生体情報に対して高いスコアを実現する生体情報による他人受入を大幅に削減できたためと考える．

具体的な性能として，FRR $<$ 7.5%，あるいは FRR $<$ 25%という要求値を設けたときの各手法の性能（WAP/LAP/FAR）を表 1 に示す．ただし，人数閾値法については FRR $<$ 7.5%のときは $T = 400$，FRR $<$ 25%のときは $T = 4$ の性能を示している．いずれの FRR の要求値においても，提案手法では従来手法と比べて大幅な性能向上が実現できていることが分かる．以上により，提案手法の有効性が示された．

5.2.2　評価 2：ダミーテンプレート数と WAP との関係

「提案手法（事後確率/被照合テンプレートごと）」において，ダミーテンプレート数を 9，99，999 個（$N = 10$，100，1,000）と変化させたときの FRR-WAP 曲線を，スコア判定法の FRR-WAP 曲線とともに**図 5** に示す．ダミーテンプレート数を増加させるほど WAP を低減させることができていることが分かる．ただし，ダミーテンプレート数を増加させるほど照合回数が増えるため，認証時間はダミーテンプレート数にほぼ比例する形で増加する．すなわち，WAP と認証時間はトレードオフの関係にある．実際の適用先では，認証時間が要求値を満たす範囲内で，数多くのダミーテンプレートを用意するのが望ましいと考える．

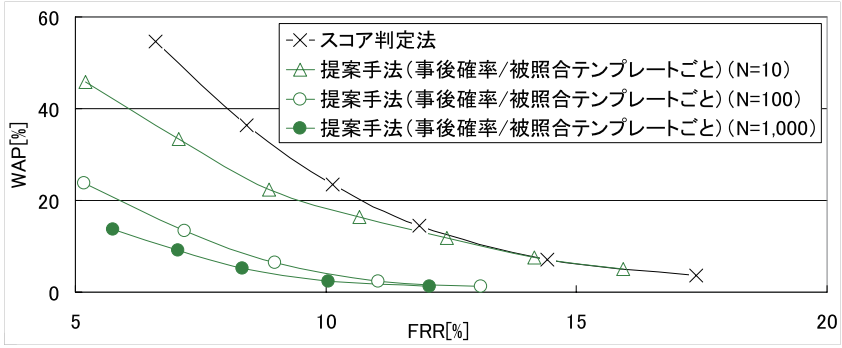

図 5　FRR-WAP 曲線とダミーテンプレート数との関係
Fig. 5　Relationship between FRR-WAP curve and the number of the dummy users.

6. ま と め

本稿では，ユニモーダルの 1 : 1 認証において Wolf と Lamb の両方に対して高い安全性を持つ手法を提案した．そして，Lamb に対する安全性の評価指標として LAP を新たに定義したうえで，提案手法の Wolf および Lamb に対する安全性の評価実験を行った．その結果，ダミーテンプレートを用いてスコアから尤度比を求め，これを事後確率に正規化することで WAP が大幅に低減され，被照合テンプレートごとの他人分布を用いて尤度比を算出することで LAP を大幅に低減させることができることを示した．提案手法はスコアのみを用いているため，スコアを出力するあらゆる生体認証に適用可能な汎用性の高い手法である．また文献 9) も提案手法と同様に，テンプレートごとの他人分布を用いて事後確率を求めているため，Wolf と Lamb の両方に対する高い安全性を持っていると考えられる．

今後は，登録時の Lamb 対策と認証時の Lamb 対策を組み合わせることを検討している．登録時に Lamb を検出して排除する方法では，曖昧な Lamb に関する検出誤りが問題となることを，3 章で述べた．提案手法も登録時の Lamb 検出に利用できる可能性があるが，この場合においても，Lamb か否かの二者択一を行う必要があるため，検出誤りが発生しうるという問題が依然として残る．その一方で，提案手法を用いた認証時における Lamb 対策では，Lamb を検出して排除することはせず，4.2 節で述べたように，テンプレートの Lamb 度合いが大きいほど，認証成功となるためにより高いスコア値を要求することで，曖昧な Lamb から Universal Lamb に至るまでの Lamb 対策を柔軟に施すことができる．しかしながら，この方法では Lamb（特に Universal Lamb）を持つユーザは本人としても認証しにくくなるという問題が別途生じる恐れがある．したがって，登録時には Universal Lamb を検出して排除し，認証時には曖昧な Lamb も含めた Lamb 対策を施すのが望ましいと考えている．

また，提案手法では，ダミーテンプレートの数だけでなく，その選定方法が Wolf に対する安全性に影響を与えると考えられる．今後は，より少ないダミーテンプレート数で Wolf に対する安全性を向上させるための，ダミーテンプレートの選定方法を検討する予定である．その際，本稿で評価用データに用いた NIST BSSR1 Set2[10] は（照合後の）スコアの

セットであったため，認証時間の測定実験を行うことができなかったが，適当な生体情報と照合アルゴリズムを用いて，認証時間に関する測定実験を行うことも検討している．

さらには，文献 9) の 1 : N 認証における Wolf/Lamb に対する安全性評価を行うことや，提案手法が（人工物も含めた）Wolf/Lamb に対して高い安全性を持つことの理論的な証明を行うことも，今後の課題である．

参 考 文 献

1) Jain, A.K., Ross, A. and Prabhakar, S.: An Introduction to Biometric Recognition, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.14, No.1, pp.4–20 (2004).
2) Doddington, G., Liggett, W., Martin, A., Przybocki, M. and Reynolds, D.: SHEEP, GOATS, LAMBS and WOLVES A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation, *Proc. ICSLP 98*, pp.1351–1354 (1998).
3) ISO/IEC 19792, Information technology — Security techniques — Security evaluation of biometrics (2009).
4) 小島由大，繁富利恵，井沼　学，大塚　玲，今井秀樹：ウルフ攻撃に対して安全な照合アルゴリズム—しきい値の最適化と虹彩認証を用いた実験，2010 年暗号と情報セキュリティシンポジウム，2F3-4 (2010).
5) Inuma, M., Otsuka, A. and Imai, H.: Theoretical Framework for Constructing Matching Algorithms in Biometric Authentication Systems, *Proc. ICB*, pp.806–815 (2009).
6) 門田　啓：偶然一致確率法によるウルフ攻撃に安全な生体認証，2010 年暗号と情報セキュリティシンポジウム，2F3-1 (2010).
7) Snelick, R., Uludag, U., Mink, A., Indovina, M. and Jain, A.: Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.27, No.3, pp.450–455 (2005).
8) 村上隆夫，高橋健太：多重仮説における逐次確率比検定を用いた ID レス生体認証の高精度化，情報処理学会論文誌，Vol.50, No.12, pp.3186–3195 (2009).
9) 村上隆夫，高橋健太：個人毎のスコア分布を用いた逐次的融合判定による ID レス生体認証の高精度化，2009 年暗号と情報セキュリティシンポジウム，2F4-4 (2009).
10) National Institute of Standards and Technology: NIST Biometric Scores Set (online). http://www.itl.nist.gov/iad/894.03/biometricscores/index.html
11) Une, M., Otsuka, A. and Imai, H.: Wolf Attack Probability: A Theoretical Security Measure in Biometric Authentication Systems, *IEICE Trans. Information and Systems*, Vol.E91-D, No.5, pp.1380–1389 (2008).
12) Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems, *Proc. SPIE*, Vol.4677, pp.275–289 (2002).
13) 宇根正志，田村裕子：バイオメトリック認証システム：4. 脆弱性の解消に向けた最新対策技術の動向 2. 生体検知技術，情報処理，Vol.47, No.6, pp.605–608 (2006).
14) Jain, A., Bolle, R. and Pankanti, S.: *BIOMETRICS Personal Identification in Networked Society*, Kluwer Academic Publishers (1999).
15) Verlinde, P. and Acheroy, M.: A Contribution to Multi-Modal Identity Verification Using Decision Fusion, *Proc. PROMOPTICA* (2000).

(平成 22 年 4 月 27 日受付)
(平成 22 年 9 月 17 日採録)

推　薦　文

生体認証における Wolf とは，あらゆる登録ユーザに対して高いスコアを得る不正認証者が存在してしまうという脆弱性であり，逆に，Lamb は，複数の他人の生体情報から高いスコアで認証を許してしまう登録者が存在してしまうというものである．多くの研究では，Wolf の考慮はされているが，Lamb を考慮したものはほとんどない．本研究では，Wolf と Lamb の両方の存在を考慮した認証方法を提案している点で新規性が高い．データベースを用いた評価実験も提案方式の有効性を立証している．論文の完成度も高く，推薦するに十分な優れた研究である．　（コンピュータセキュリティ研究会主査　菊池浩明）

村上　隆夫（正会員）

平成 16 年東京大学工学部電子情報工学科卒業．平成 18 年同大学院修士課程修了．同年（株）日立製作所入社．以来，同システム開発研究所にて生体認証技術の研究開発に従事．平成 20 年 CSS2008 優秀論文賞受賞．平成 21 年 CSS2009 優秀論文賞受賞．平成 22 年度山下記念研究賞受賞．

高橋　健太（正会員）

平成 10 年東京大学理学部情報科学科卒業．平成 12 年同大学院修士課程修了．同年（株）日立製作所入社．以来，同システム開発研究所にて生体認証技術の研究開発に従事．現在，東京大学大学院情報理工学系研究科社会人博士課程に在籍中．平成 13 年情報処理学会高度交通システム研究会優秀論文賞受賞．平成 20 年度情報処理学会論文賞受賞．