Wolf及びLambに対する安全性の高い生体認証の提案

村上　隆夫†　　高橋　健太†

†（株）日立製作所システム開発研究所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地

{takao.murakami.nr, kenta.takahashi.bw}@hitachi.com

あらまし　生体認証において，あらゆるユーザに対して高いスコア (類似度) を実現するユーザ (Wolf/Lamb) の存在が示されている．このようなユーザはあらゆる他人に対して認証誤りを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生体認証技術の研究は，筆者らの知る限り行なわれていない．本稿では，個人毎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，あらゆる種類の生体情報に適用可能な，Wolf 及び Lamb に対する安全性の高い手法を提案する．NIST BSSR1 を用いた評価実験を通して，提案手法が Wolf 及び Lamb に対して高い安全性を持つことを定量的に示す．

Biometric Authentication Secure against Wolf and Lamb

Takao Murakami†　　Kenta Takahashi†

†Hitachi, Ltd., Systems Development Laboratory
292, Yochida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-2423, Japan

{takao.murakami.nr, kenta.takahashi.bw}@hitachi.com

Abstract　The existence of Wolves/Lambs that have high similarity scores against any other users is shown in biometric authentication. These users can cause false accepts against any others, making the biometric system insecure. Although many techniques have been proposed to improve biometric accuracy, no techniques, to our knowledge, have been proposed to have security against both Wolves and Lambs. In this paper, we propose such a technique by normalizing scores to the posterior probabilities using user-specific imposter distribution. This technique can be applied to any kind of modality since it only uses scores obtained by the matcher. We quantitatively show that the proposed method has security against both Wolves and Lambs through the experinmental evaluation using the NIST BSSR1 database.

1　はじめに

ユーザの身体的特徴，或いは行動的特徴を用いて本人確認を行なう生体認証の普及が進んでいる．生体認証では，認証を試みるユーザ (以後，認証ユーザ) が自分の生体情報を提示し，システムがこの生体情報をあらかじめ登録されているユーザ (以後，登録ユーザ) の生体情報と照合してスコア (類似度或いは距離) を算出することで認証を行なう．この際，あらゆるユーザに対して高いスコア (以後，類似度) を実現するユーザ (Wolf/Lamb) の存在が示されている [1]．あらゆる登録ユーザに対して高いスコアを実現する認証ユーザは Wolf と呼ばれており，あらゆる認証ユーザに対して高いスコアを与える登録ユーザは Lamb と呼ばれている[1]．このようなユーザは，あらゆる他人に対して認証誤り (他人受入) を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 や Lamb に対して高い安全性を持つ生体認証技術の研究例は少ないのが現状であ

[1] このような認証ユーザ／登録ユーザの生体情報が Wolf/Lamb と呼ばれることもある．

る．Wolf に対しては文献 [2, 3] が，安全性の高い手法について理論的な考察を行なっているが，Lamb への対策については考慮されていない．筆者らの知る限りでは，Wolf と Lamb の両方に対して安全性が高い手法は今までに提案されていない．

筆者らは，システムが DB 内の N 人の登録ユーザの生体情報と順次照合を行なって認証ユーザが誰なのかを識別する 1:N 認証において，複数の生体情報を融合して判定を行なうマルチモーダル認証技術を提案している [4, 5]．本手法は，得られたスコアを事後確率に正規化して，これをユーザの判定基準としているが，文献 [5] では，この際に個人毎の他人分布 (他人同士のスコアが従う分布) を用いることで認証精度を向上し，さらに Wolf や Lamb 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 [5] の考察を基に，より一般的な生体認証，即ちシステムがある登録ユーザ (1 人) の生体情報と照合を行なって認証ユーザが本人か否かを判定する 1:1 認証において，Wolf 及び Lamb 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，あらゆる種類の生体情報に適用可能な，汎用性の高い手法である．また本稿では，提案手法の Wolf 及び Lamb に対する安全性評価を行なう．安全性評価はユーザが人工物を提示する場合も本来考慮すべきである [6] が，人工物の作成も含めた評価実験は困難であることや，生体検知技術 [7] などの様々な対策が施されている現状を考慮し，本稿では (人工物でない) 生体情報を用いた評価実験を行なう．具体的には，NIST BSSR1 (Biometric Scores Set - Release 1) Set2[8] を評価用データとした評価実験を行ない，提案手法が Wolf 及び Lamb に対して高い安全性を持つことを定量的に示す．

2 Wolf 及び Lamb に対する安全性の評価指標

2.1 Wolf と Lamb

文献 [1] では声紋認証において，あらゆる登録ユーザに対して高いスコアを実現する認証ユーザ (Wolf)，あらゆる認証ユーザに対して高いスコアを与える登録ユーザ (Lamb) が存在することを示している．1:1 認証では従来，得られたスコアが認証閾値を上回れば本人，そうでなければ他人と判定することで認証が行なわれるが，このとき Wolf はあらゆる他人に対してなりすましが可能となり，Lamb はあらゆる他人から容易になりすましが行なわれる恐れがある．

1:N 認証でも同様に，Wolf は常に (あらゆる DB に対して) 他人として認証成功となる恐れがあり，また Lamb は常に他の認証ユーザを自分として受理してしまう恐れがある．特に Lamb が登録されている場合は，どのユーザが認証を試みても識別結果がその Lamb となってしまい，認証システムとしての機能が完全に損なわれる危険性もある．

従って，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と言える．

2.2 WAP と LAP

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．FAR は認証ユーザの集合を V，登録ユーザの集合を E とし，認証ユーザ v と登録ユーザ e の認証結果を $match(v, e) \in \{\text{accept, reject}\}$ とすると，

$$FAR = \underset{v \in V}{Ave} \underset{e \in E, e \neq v}{Ave} P(match(v, e) = \text{accept}) \quad (1)$$

と表せる．但し，$P(match(v, e) = \text{accept})$ 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．即ち，FAR は全認証ユーザ及び全登録ユーザ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．この場合，あらゆる他人に対して認証成功となる Wolf，或いは Lamb が存在していたとしても，全ユーザの中で Wolf や Lamb が占める割合がごく僅かであれば，それによって FAR はほとんど上昇しない．従って，FAR は Wolf や Lamb に対する安全性の評価指標としては不十分であると言える．

文献 [6] では Wolf に対する安全性の評価指標として，以下の式で表される WAP (Wolf Attack Probability) を定義している．

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

但し，$\underset{v \in V}{max}\, X$ は $v \in V$ に関して X の最大値をとったものである．WAP は最も他人受入を引き起こし

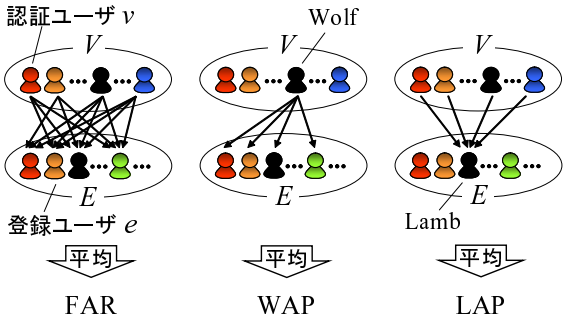

図 1: Wolf と Lamb に対する安全性の評価指標 (WAP/LAP)

やすい生体情報を持つ認証ユーザがなりすましを試みたときに，それが成功する確率値である．

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．

$$LAP = \max_{e \in E} \operatorname*{Ave}_{v \in V, v \neq e} P(match(v, e) = \text{accept}) \quad (3)$$

これは，最も他人受入を引き起こしやすい生体情報を持つ登録ユーザが，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，及び LAP を図 1 に示す．

1:N 認証における精度の評価指標としては，筆者らが文献 [4] において EFRR/EFAR/NFAR の 3 つを定義している．1:N 認証における Wolf 及び Lamb に対する安全性の評価尺度も定義することは可能と考えるが，それは複雑なものとなるため本稿では扱わない．

3 Wolf 及び 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ている [4, 5]．文献 [5] では，登録ユーザ毎に学習した他人分布を用いて，得られたスコアから認証ユーザが各登録ユーザ，或いは非登録ユーザであるという事後確率を求めることで Wolf 及び Lamb に対する高い安全性を実現できることを考察した．

本章では文献 [5] を基に，まず 1:1 認証において，Wolf 及び Lamb に対する安全性の高い手法を提案する．これは，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，また安全性評価も容易に行なえるためである．次に，提案手法が Wolf 及び Lamb に対して高い安全性を持つと考えられる理由を述べる．

3.1 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，登録ユーザ e_1 の他に認証ユーザ v との照合を行なうユーザ (以後，ダミーユーザ)$e_2, \cdots, e_N$ ($N-1$ 人) を，数多く用意しておく．ダミーユーザは登録ユーザ e_1 以外の人であれば良く，DB に登録されている他のユーザを用いても良いし，システムがあらかじめ用意した人であっても良い．数多くのダミーユーザを用意する理由は，第 3.2 節で詳述する．本稿では，登録ユーザとダミーユーザを合わせて被照合ユーザと呼ぶことにする．被照合ユーザ $e_1, \cdots, e_N$ 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，

$$S = \{s_i | 1 \leq i \leq N\} \quad (4)$$

とおく．提案手法では，

仮説 H_i:「認証ユーザ v は被照合ユーザ e_i である」 $(1 \leq i \leq N)$

仮説 H_0:「認証ユーザ v はどの被照合ユーザでもない」

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，登録ユーザ e_1 に対する事後確率 $P(H_1|S)$ を閾値 A と比較し，$P(H_1|S) > A$ 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 $P(H_i|S)$ $(i = 0,\ 2 \leq i \leq N)$ は求めなくても良いが，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．

$$P(H_i|S) = \frac{P(H_i)Z_i}{\sum_{n=0}^{N} P(H_n)Z_n} \quad (5)$$

但し，$P(H_i)$ はスコア集合 S が得られる前段階 (即ち，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，

$$Z_i = \frac{P(S|H_i)}{P(S|H_0)} \quad (6)$$

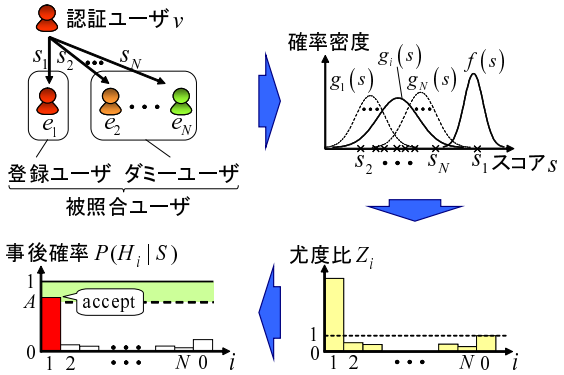

図 2: Wolf/Lamb に対する安全性の高い 1:1 認証

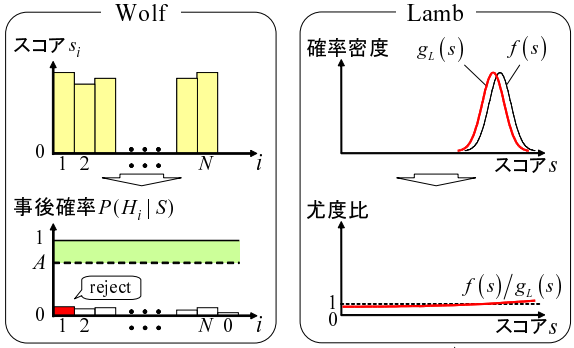

図 3: 提案手法の Wolf/Lamb に対する安全性

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，

$$P(s_i|H_j) = f(s_i) \quad (\text{if } i = j) \tag{7}$$
$$P(s_i|H_j) = g_i(s_i) \quad (\text{if } i \neq j) \tag{8}$$

と表せると仮定する．$f()$，$g_i()$ はそれぞれ全被照合ユーザ共通の本人分布 (本人同士のスコアが従う分布)，i 番目の被照合ユーザ e_i の他人分布である $(1 \leq i \leq N)$．このとき，全スコアが独立であると仮定すれば，式 (6) の尤度比 Z_i は，

$$\begin{aligned} Z_i &= \frac{P(s_i|H_i)\prod_{n\neq i} P(s_n|H_i)}{P(s_i|H_0)\prod_{n\neq i} P(s_n|H_0)} \\ &= \begin{cases} f(s_i)/g_i(s_i) & (\text{if } i \neq 0) \\ 1 & (\text{if } i = 0) \end{cases} \end{aligned} \tag{9}$$

と求めることができる．$f()$ 及び $g_i()$ は，正規分布などのモデルを仮定した上で，そのパラメータを被照合ユーザの生体情報や，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．或いは，式 (9) より尤度比 Z_i は，本人分布と他人分布の比 $f()/g_i()$ で表されるので，$f()/g_i()$ をロジスティック回帰 [9] 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 [9] に示されている．

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，照合を行なってスコア集合 $S = \{s_i|1 \leq i \leq N\}$ を求める．
2. 式 (9) により尤度比 Z_i $(0 \leq i \leq N)$ を算出する．($f()$ と $g_i()$ $(1 \leq i \leq N)$ は学習しておく)．
3. 式 (5) 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 A と比較し，$P(H_1|S) > A$ 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 1:1 認証を行なう様子を図 2 に示す．これは文献 [5] の手法において，生体情報の入力回数の上限値 T を $T = 1$ とし，事後確率 $P(H_i|S)$ $(i = 0,\ 2 \leq i \leq N)$ に対する閾値を 1 とした (即ち，識別しない) ものに相当する．

3.2 提案手法の Wolf 及び Lamb に対する安全性に関する考察

提案手法が Wolf 及び 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 $P(H_i)$ $(0 \leq i \leq N)$ は全て等しいとする．

提案手法では，各被照合ユーザに対するスコアを基に尤度比を求め，これを事後確率に正規化する．このとき，あらゆる被照合ユーザに対して高いスコア (及び尤度比) を実現する認証ユーザ (Wolf) が認証を試みたとしても，全仮説の事後確率の総和は常に 1 であるため，事後確率は低い値として算出される (図 3)．

例えば，全ての被照合ユーザに対して高いスコアが得られ，その結果として等しく高い尤度比 Z_i $(1 \leq i \leq N)$ が得られた場合，式 (5) より各被照合ユーザの事後確率 $P(H_i|S)$ は凡そ $1/N$ となる．従って，閾値をより高く設定すれば，このような Wolf は認証失敗となる．また，高いスコア (及び尤度比) が数多くのダミーユーザ e_i $(2 \leq i \leq N)$ に対して得られるほど，登録ユーザ e_1 に対する事後確率 $P(H_1|S)$ は小さい値となるので，ダミーユーザの増加に伴い，Wolf に対する安全性は向上すると考えられる．これが，提案手法において数多くのダミーユーザを用意

する理由である．

さらに，提案手法では個人毎に他人分布を学習する．このとき，あらゆる認証ユーザに対して高いスコアを実現する登録ユーザ (Lamb) の他人分布 $g_L(s)$ 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)．提案手法では，認証時に得られたスコアを基に，本人／他人分布の比として尤度比を求める (式 (9))．従って，認証時にこの登録ユーザ (Lamb) に対して高いスコア s が得られたとしても，尤度比 $f(s)/g_L(s)$ 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．これは，ロジスティック回帰を用いて $f()/g_L()$ を直接学習した場合も同じである．従って，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．

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個人毎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．

4 提案手法の Wolf 及び Lamb に対する安全性評価

4.1 実験条件

提案手法の Wolf 及び Lamb に対する安全性を定量的に評価するために，NIST BSSR1 (Biometric Scores Set - Release 1) Set2[8] を用いた評価実験を行なった．このデータは，6,000 人の被験者からそれぞれ左手及び右手の指紋（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 $6,000 \times 6,000$ 個）である．本実験では，左手の指紋のスコアセットを用いた．

6,000 人の被験者のうち，4,501 人を認証ユーザ，或いは登録ユーザとして，999 人をダミーユーザとして，残りの 500 人を分布学習用のユーザとして用いることにした．そして，任意の認証ユーザが任意の登録ユーザに対して 1:1 認証を試みる実験を行なった (本人／他人同士による認証試行は，それぞれ $4,501$ 回，$4,501 \times 4,500 = 20,254,500$ 回)．

分布の学習は，ロジスティック回帰によって尤度比を直接学習することで行なった．被照合ユーザ e_i $(1 \leq i \leq N)$ の尤度比 $f()/g_i()$ は，全学習用ユーザから得られた本人スコア (500 個) と，全学習用ユーザを被照合ユーザ e_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．全被照合ユーザ共通の尤度比 $f()/g()$ は，全学習用ユーザ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 ($500 \times 499 = 249,500$ 個) を用いて学習した．また，事前確率は，全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 FRR-WAP 曲線，及び FRR-LAP 曲線を求めた．また，ダミーユーザ数を増加させたときの WAP の変化を調べるため，ダミーユーザ数を 9，99，999 人 (即ち N=10，100，1,000) と変化させたときの FRR-WAP 曲線も求めた．さらに本実験では比較のため，登録ユーザ e_1 に対するスコア s_1 を閾値と比較する従来手法を用いた場合についても評価も行なった．

4.2 実験結果

ダミーユーザ数を 999 人としたときの，従来手法及び提案手法の FRR-WAP 曲線及び FRR-LAP 曲線を図 4 に示す．ここでは，参考のため FRR-FAR 曲線 (DET カーブ) も同時に示している．図 4 より，提案手法は従来手法と比較して WAP 及び LAP が大幅に低減できていることが分かる．これは，第 3.2 節の考察が実験結果に表れたものと考えられる．提案手法では FAR も低減できているが，これは Wolf や Lamb のように，複数のユーザに対して高いスコアを実現するユーザによる他人受入を大幅に削減できたためと考えられる．

具体的な性能を述べると，例えば FRR<7.5% という要件を設けたとき，スコアを閾値と比較する従来手法では FAR=8.3%，WAP=45%，LAP=32% と WAP や LAP が非常に高い値となっていた．これに対し，個人毎の他人分布を用いて事後確率を算出する提案手法では FAR=3.1%，WAP=6.9%，LAP=8.6% と大幅な性能向上が実現できている．以上により，提案手法の有効性が示された．

また，ダミーユーザ数を 9，99，999 人 (N=10，100，1,000) と増加させたときの FRR-WAP 曲線を図 5 に示す．ダミーユーザ数を増加させるほど WAP を低減できていることが分かる．但し，ダミーユーザ数を増加させるほど照合回数が増えるため，認証時間が大きくなる．即ち，認証時間と WAP はトレー

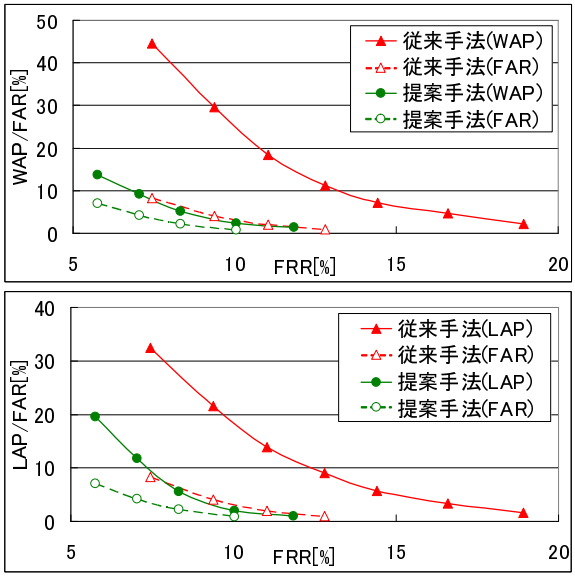

図 4: FRR-WAP 曲線と FRR-LAP 曲線 (点線は FRR-FAR 曲線)

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，数多くのダミーユーザを用意するのが望ましいと考える．

5 まとめ

本稿では，1:1 認証において Wolf 及び Lamb に対して高い安全性を持つ認証方式を提案した．そして，Lamb に対する安全性の評価指標として LAP を新たに定義した上で，提案手法の Wolf 及び Lamb に対する安全性の評価実験を行なった．その結果，個人毎の他人分布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 及び LAP を大幅に低減できることを示した．提案手法はスコアのみを用いており，あらゆる種類の生体情報に適用可能な汎用性の高い手法である．また文献 [5] も提案手法と同様に，個人毎の他人分布を用いて事後確率を求めているため，Wolf 及び Lamb に対する高い安全性を持っている，と考えられる．

今後は，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なうことを検討している．

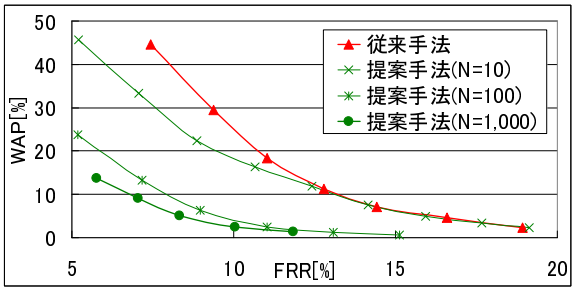

図 5: FRR-WAP 曲線とダミーユーザ数との関係

参考文献

[1] G.Doddington et al., ”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)

[2] M. Inuma et al., “ Theoretical Framework for Constructing Matching Algorithms in Biometric Authentication Systems, ” Proc.ICB, pp.806-815 (2009)

[3] 小島由大他，“ウルフ攻撃確率を考慮したマッチングアルゴリズムのフレームワークにおける安全で可用性の高い認証プロトコル”，SCIS2009 (2009)

[4] 村上隆夫他，“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”，CSS2008 (2008)

[5] 村上隆夫他，“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”，SCIS2009 (2009)

[6] M.Une et al., “Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems,” Proc.ICB, pp.396-406 (2007)

[7] 宇根正志他，“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 47 巻 6 号，pp.605-608 (2006)

[8] National Institute of Standards and Technology: NIST Biometric Scores Set (online), available from http://www.itl.nist.gov/iad/894.03/biometricscores/index.html

[9] P. Verlinde et al., “A Contribution to Multi-Modal Identity Verification Using Decision Fusion,” Proc.PROMOPTICA (2000)