バイオメトリクス認証における ウルフ攻撃に対して安全な照合アルゴリズム

小島 由大† 繁富 利恵†‡ 井沼 学‡ 大塚 玲†‡ 今井 秀樹†‡

† 中央大学大学院理工学研究科電気電子情報通信工学専攻
112-8551 東京都文京区春日 1-13-27

yoshihiro-kojima@imailab.jp

‡ 産業技術総合研究所 情報セキュリティ研究センター
101-0021 東京都千代田区外神田 1-18-13 秋葉原ダイビル 1102 号室

{rie-shigetomi, inuma.manabu, a-otsuka, h-imai}@aist.go.jp

あらまし バイオメトリクスの 1 対 1 認証において，ウルフ攻撃に対して安全な照合アルゴリズムを提案する．提案アルゴリズムは，通常の 1 対 1 照合に加え，さらに他の登録テンプレートとの誤一致人数を尺度としてウルフ判定を行う．本研究では，提案アルゴリズムにおけるウルフ攻撃確率，他人受入率，本人拒否率の上界を示す．さらに，ウルフ攻撃確率と本人拒否率の上界のトレードオフを示し，認証精度の高いモダリティにおいては，その両方を同時に小さくすることが可能なことを証明する．

A Matching Algorithm Secure against the Wolf Attack in Biometric Authentication Systems

Yoshihiro Kojima† Rie Shigetomi†‡ Manabu Inuma ‡ Akira Otsuka†‡
Hideki Imai†‡

†Major of Electrical, Electronic, and Information-communication Engineering,
graduate course of Science and Engineering, Chuo University grad school
1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551, Japan

‡Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology
1-18-13 Sotokanda Chiyoda-ku Tokyo 101-0021,Japan

{rie-shigetomi, inuma.manabu, a-otsuka, h-imai}@aist.go.jp

Abstract We propose a matching algorithm secure against the wolf attack in one-to-one biometric authentications. Our proposal algorithm first executes a one-to-all comparison using a conventional measure such as the Hamming distance and then decides whether the prover is truly an authorized user by the number of unauthorized users who are incorrectly accepted. We calculate upper bounds of FAR, FRR and WAP (the wolf attack probability) in the proposal authentication algorithm and show the trade-off between an upper bound of WAP and that of FRR. We also show that our proposal algorithm can achieve lower FAR, FRR and WAP simultaneously.

1 はじめに

近年，バイオメトリクス認証システムが広く利用され，バイオメトリクス認証の研究も盛んに行われている．バイオメトリクス認証システムを安全に使うためには，セキュリティの評価が重要になってくる．現在，バイオメトリクス認証システムのセキュ

リティを評価する場合，主に他人受入率（FAR）や本人拒否率（FRR）で評価されている．

バイオメトリクス認証には，アルゴリズムによっては複数の登録テンプレートと誤一致を引き起こすウルフという入力情報が存在する．ウルフを用いて攻撃をしたとき，その最大の攻撃成功確率をウルフ攻撃確率（WAP) と呼び，WAP を用いてウルフ攻撃の耐性を評価する．これらのことより，バイオメトリクス認証のセキュリティの評価には，FAR，FRR に加えて WAP の評価が必要である．

今回提案するアルゴリズムは通常の 1 対 1 照合に加え，さらに他の登録テンプレートとの誤一致ユーザ数を尺度として，ウルフ判定を行うアルゴリズムである．このアルゴリズムを用いることにより，FAR と WAP は減少することがわかり，さらに WAP は，照合するテンプレート数を n，誤一致ユーザ数を $T-1$ （T は自分を含めた一致ユーザ数）としたとき，WAP $\leq T/(n-1)$ となることを証明する（定理 2)．

また，提案するアルゴリズムにおいて，WAP と FRR はトレードオフの関係にあり，照合するテンプレート数 n と一致許容数 T によって，それぞれは増減する．照合するテンプレート数 n のシステムが存在するとき，最適な一致許容数 T を選ぶことによって，FRR と WAP を同時に小さくすることができることを証明する（定理 3)．

2　バイオメトリクス認証のモデル

2.1　バイオメトリクス認証のモデル

U を正規ユーザ全体とする．M は有限集合で, システムは個人のバイオメトリクスを読み込み, 特徴抽出アルゴリズムを経て, ある有限集合 M の元として出力し, 登録や照合に用いるものとする．つまり, 登録テンプレートや照合時の入力サンプルは M の元として表される (例えば, Daugman [1] の虹彩認証では $M=\{0,1\}^{2048}$)．読み込み時のノイズ, システム環境などによりそれぞれのユーザ $u\in U$ のサンプルは M の元として一意に出力されるわけではない．よって，$u\in U$ に対して X_u を u の出力の分布を表す確率変数とする．つまり，$\mathrm{P}(X_u=s)$ は，ユーザ $u\in U$ の出力が $s\in M$ となる確率である．照合アルゴリズムは，match : $M\times M\to\{$”accept”,”reject”$\}$ で表され，入力サンプルの出力 $s\in M$ と登録テンプレート $t\in M$ に対して類似度を計算して accept か reject のいずれかを返す．

このときユーザ $u\in U$ の入力サンプルがユーザ $v\in U$ (u と同じでもよい) の登録テンプレートと一致する確率を Prob[v accepts u] と書く．このとき

$$\begin{aligned}\mathrm{Prob}[v\text{ accepts }u] &= \sum_{\substack{(s,t)\in M\times M\\ \mathrm{match}(s,t)=\text{” accept ”}}}\mathrm{P}(X_u=s)\,\mathrm{P}(X_v=t)\\ &= \sum_{s\in M}\mathrm{P}(X_u=s)\sum_{\substack{t\in M\\ \mathrm{match}(s,t)=\text{” accept ”}}}\mathrm{P}(X_v=t)\\ &= \sum_{s\in M}\mathrm{P}(X_u=s)\,\mathrm{P}_s(v) \qquad (1)\end{aligned}$$

である．ここで，$\mathrm{P}_s(v)=\sum_{\substack{t\in M\\ \mathrm{match}(s,t)=\text{” accept ”}}}\mathrm{P}(X_v=t)$ は $s\in M$ が $v\in U$ の登録テンプレートとの照合で accept となる確率である．

通常の 1 対 1 バイオメトリクス認証における登録アルゴリズムと照合アルゴリズムのモデルを以下のように定める．

登録アルゴリズム

$v\in U$: 登録を行うユーザ
$t\leftarrow X_v$ をテンプレートとして登録する．

照合アルゴリズム

$u\in U$: 認証を行うユーザ
u はユーザ $v\in U$ を名乗る．
u は $s\leftarrow X_u$ を提示する．
v のテンプレート $t\in M$ に対して

$$\mathrm{match}(s,t)=\begin{cases}\text{”accept” ならば照合成功}\\ \text{”reject” ならば照合失敗}\end{cases}$$

(注意): 正規ユーザ $u\in U$ は照合時に本人 u を名乗るが，なりすましを行うユーザは他のユーザを名乗る．

3　安全性評価と精度評価

3.1　なりすまし攻撃に対する安全性評価尺度

1 対 1 認証における 2 種類のなりすまし攻撃とそれぞれの攻撃成功確率 (=それぞれの攻撃に対する安全性の評価尺度) について述べる．

3.1.1 ゼロエフォート攻撃

攻撃者は，自分以外の任意のユーザ $v \in U$ を名乗る．そして，自分の正規のバイオメトリクスサンプルを提示して v になりすまそうとする．このとき，攻撃成功確率は他人受入率 (FAR) に一致する．

$$\begin{aligned}\mathrm{FAR} &= \\ &\underset{(u,v)\in(U\times U)^{diff}}{\mathrm{Ave}} \mathrm{Prob}[v \text{ accepts } u] \\ &= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \mathrm{Prob}[v \text{ accepts } u] \\ &= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(v)\end{aligned} \tag{2}$$

ここで, $(U\times U)^{diff} = \{(u,v) \in U \times U \mid u \neq v\}$.

3.1.2 ウルフ攻撃

攻撃者は, 自分以外の任意のユーザ $v \in U$ を名乗るが，v のサンプルの出力分布 X_v を知らない．攻撃者は，ウルフ ((自分以外の) 全ユーザに対する誤認識の確率の期待値が大きいサンプルであり，人工物も含む) を提示して,v になりすまそうとする．このとき，攻撃成功確率の最大値 (攻撃者が最も期待値の高いサンプルを提示したときの成功確率) をウルフ攻撃確率 (WAP) と呼ぶ [2] ．よって

$$\mathrm{WAP} = \max_{a\in A} \underset{v\in U\,:\,v\neq a}{\mathrm{Ave}} \mathrm{Prob}[v \text{ accepts } a] \tag{3}$$

である．ここで，A は，人工物提示などを行う不正ユーザを含めた全ユーザの集合である．

特定のユーザのバイオメトリクス情報を持たずに，故意のなりすましを行う攻撃者に対する安全性を評価するためには FAR だけでは不十分であり，WAP を用いて評価しなければならない．

3.2 精度評価

ここで，バイオメトリクス認証の精度評価にも触れる．精度評価には，おもに FAR と 本人拒否率 (FRR) が用いられる．FRR は正規ユーザが自分を名乗り，自分の正規サンプルを提示して照合失敗となる確率である．よって，

$$\begin{aligned}\mathrm{FRR} &= 1 - \underset{u\in U}{\mathrm{Ave}}\,\mathrm{Prob}[u \text{ accepts } u] \\ &= 1 - \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(u) \\ &= \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)(1 - \mathrm{P}_s(u))\end{aligned} \tag{4}$$

既存のバイオメトリクス認証においては，FAR と FRR を十分小さな値に抑えることが目標とされ，そのような認証アルゴリズムが用いられている．しかし WAP を評価尺度として考慮していない既存のアルゴリズムの中には，WAP の理論値が無視できないほど高い値を示すものもある [2][3][4] .

4 提案する照合アルゴリズム

4.1 本研究の目的

本論文の目標は，既存の認証アルゴリズムと比較して，認証精度を低下させることなく (つまり FAR や FRR をほとんど増加させることなく)，かつ WAP も十分に小さな値で抑えることができる照合アルゴリズムを提案し，その安全性を証明することである．

4.2 提案する照合アルゴリズム

提案するウルフ攻撃に対して安全な照合アルゴリズムでは，一般的なバイオメトリクスの 1 対 1 照合アルゴリズムに加え，さらに他の登録テンプレートとも照合を行い，その誤一致人数を尺度としてウルフ判定を行うアルゴリズムである．

照合アルゴリズム

$u \in U$: 認証を行うユーザ
u はユーザ $v \in U$ を名乗る．
u は $s \leftarrow X_u$ を提示する．
v のテンプレート $t \in M$ に対して

$$\mathrm{match}(s,t) = \begin{cases} \text{”accept” ならば次へ} \\ \text{”reject” ならば照合失敗} \end{cases}$$

すべての $v' \in U\backslash v$ に対して，$\mathrm{match}(s,v') =$ ”accept” となる v' の個数が

$$\begin{cases} T-1 \text{ 以下ならば照合成功} \\ T \text{ 以上ならば照合失敗} \end{cases}$$

提案アルゴリズムにおける他人受入率，ウルフ攻撃確率，本人拒否率をそれぞれ $\mathrm{FAR}^{\mathrm{prop}}$, $\mathrm{WAP}^{\mathrm{prop}}$, $\mathrm{FRR}^{\mathrm{prop}}$ と書く．それぞれは次のようの示される．

$$
\begin{aligned}
&\mathrm{FAR}^{\mathrm{prop}} \\
&= \operatorname*{Ave}_{(u,v)\in(U\times U)^{diff}} \mathrm{Prob}[v \text{ accepts } u] \\
&= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \sum_{s\in M} \mathrm{P}(X_u = s) \\
&\quad \mathrm{Prob}[v \text{ accepts } s] \\
&= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(v) \\
&\quad \sum_{k=0}^{T-1} \sum_{\substack{I\subset U\setminus\{v\} \\ \sharp I=k}} \prod_{v'\in I} \mathrm{P}_s(v') \prod_{v''\in(U\setminus\{v\})\setminus I} (1-\mathrm{P}_s(v''))
\end{aligned}
\tag{5}
$$

$$
\begin{aligned}
&\mathrm{WAP}^{\mathrm{prop}} \\
&= \max\left\{ \max_{a\in A\setminus U} \operatorname*{Ave}_{v\in U} \mathrm{Prob}[v \text{ accepts } a]\,, \right. \\
&\qquad \left. \max_{a\in U} \operatorname*{Ave}_{v\in U\,:\,v\neq a} \mathrm{Prob}[v \text{ accepts } a] \right\} \\
&= \max\left\{ \max_{a\in A\setminus U} \frac{1}{|U|} \sum_{v\in U} \mathrm{Prob}[v \text{ accepts } a]\,, \right. \\
&\qquad \left. \max_{a\in U} \frac{1}{|U|-1} \sum_{v\in U\,:\,v\neq a} \mathrm{Prob}[v \text{ accepts } a] \right\}
\end{aligned}
\tag{6}
$$

である．

$$
\begin{aligned}
&\mathrm{FRR}^{\mathrm{prop}} \\
&= \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{Prob}[u \text{ rejects } s] \\
&= \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s) \\
&\times \left(\{1-\mathrm{P}_s(u)\} + \mathrm{P}_s(u) \sum_{k=T}^{|U|-1} \sum_{\substack{I\subset U\setminus\{u\} \\ \sharp I=k}} \prod_{v'\in I} \mathrm{P}_s(v') \right. \\
&\qquad \left. \prod_{v''\in(U\setminus\{u\})\setminus I} \{1-\mathrm{P}_s(v'')\} \right)
\end{aligned}
$$

$$
\begin{aligned}
&= \mathrm{FRR} \\
&+ \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(u) \sum_{k=T}^{|U|-1} \sum_{\substack{I\subset U\setminus\{u\} \\ \sharp I=k}} \\
&\quad \prod_{v'\in I} \mathrm{P}_s(v') \prod_{v''\in(U\setminus\{u\})\setminus I} (1-\mathrm{P}_s(v''))
\end{aligned}
\tag{7}
$$

である．ここで $\mathrm{Prob}[u \text{ rejects } s]$ は $s\in M$ が $u\in U$ の登録テンプレートとの照合で reject となる確率である

5 安全性と認証精度の評価

定理 1.

$$
\mathrm{FAR}^{\mathrm{prop}} \leq \mathrm{FAR} \tag{8}
$$

証明．(5) 式より，

$$
\sum_{k=0}^{T-1} \sum_{\substack{I\subset U\setminus\{v\} \\ \sharp I=k}} \prod_{v'\in I} \mathrm{P}_s(v') \prod_{v''\in(U\setminus\{v\})\setminus I} (1-\mathrm{P}_s(v'')) \leq 1
$$

であるため，(2) 式と比較すると，明らかに

$$
\mathrm{FAR}^{\mathrm{prop}} \leq \mathrm{FAR}
$$

となる． □

定理 2.

$$
\mathrm{WAP}^{\mathrm{prop}} \leq \frac{T}{|U|-1} \tag{9}
$$

証明．(6) 式より，それぞれ

$$
\begin{aligned}
&\max_{a\in A\setminus U} \frac{1}{|U|} \sum_{v\in U} \mathrm{Prob}[v \text{ accepts } a] \\
&= \max_{a\in A\setminus U} \frac{1}{|U|} \sum_{v\in U} \sum_{s\in M} \mathrm{P}(X_a = s)\,\mathrm{P}_s(v) \\
&\sum_{k=0}^{T-1} \sum_{\substack{I\subset U\setminus\{v\} \\ \sharp I=k}} \prod_{v'\in I} \mathrm{P}_s(v') \prod_{v''\in(U\setminus\{v\})\setminus I} (1-\mathrm{P}_s(v''))
\end{aligned}
\tag{10}
$$

$$
\begin{aligned}
&\max_{a\in U} \frac{1}{|U|-1} \sum_{v\in U\,:\,v\neq a} \mathrm{Prob}[v \text{ accepts } a] \\
&= \max_{a\in U} \frac{1}{|U|-1} \sum_{v\in U\,:\,v\neq a} \sum_{s\in M} \mathrm{Prob}(X_a = s) \\
&\quad \mathrm{P}_s(v) \sum_{k=0}^{T-1} \sum_{\substack{I\subset U\setminus\{v\} \\ \sharp I=k}} \prod_{v'\in I} \mathrm{P}_s(v') \prod_{v''\in(U\setminus\{v\})\setminus I} (1-\mathrm{P}_s(v''))
\end{aligned}
\tag{11}
$$

である．ここで，(10) 式について，各 $a \in A \backslash U$ に対して，

$$\begin{aligned}
&\frac{1}{|U|}\sum_{v\in U}\sum_{s\in M}\mathrm{P}(X_a=s)\,\mathrm{P}_s(v)\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\backslash\{v\}\\ \sharp I=k}}\\
&\quad\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in(U\backslash\{v\})\backslash I}(1-\mathrm{P}_s(v''))\\
=&\frac{1}{|U|}\sum_{s\in M}\mathrm{P}(X_a=s)\sum_{k=0}^{T-1}\sum_{v\in U}\sum_{\substack{I\subset U\backslash\{v\}\\ \sharp I=k}}\mathrm{P}_s(v)\\
&\quad\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in(U\backslash\{v\})\backslash I}(1-\mathrm{P}_s(v''))\\
=&\frac{1}{|U|}\sum_{s\in M}\mathrm{P}(X_a=s)\sum_{k=0}^{T-1}(k+1)\sum_{\substack{I\subset U\\ \sharp I=k+1}}\prod_{v'\in I}\mathrm{P}_s(v')\\
&\quad\prod_{v''\in U\backslash I}(1-\mathrm{P}_s(v''))\\
\le&\frac{1}{|U|}\sum_{s\in M}\mathrm{P}(X_a=s)\,T\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\\ \sharp I=k+1}}\prod_{v'\in I}\mathrm{P}_s(v')\\
&\quad\prod_{v''\in U\backslash I}(1-\mathrm{P}_s(v'')) \qquad (12)
\end{aligned}$$

である．

ここで $\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\\ \sharp I=k+1}}\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in U\backslash I}(1-P_s(v''))$ は，$s\in M$ が U の中の 1 人以上 T 人以下のユーザとの照合で accept となる確率であるから

$$\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\\ \sharp I=k+1}}\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in U\backslash I}(1-\mathrm{P}_s(v''))\le 1$$

である．よって

$$\begin{aligned}
&\frac{1}{|U|}\sum_{s\in M}\mathrm{P}(X_a=s)\,T\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\\ \sharp I=k+1}}\prod_{v'\in I}\mathrm{P}_s(v')\\
&\quad\prod_{v''\in U\backslash I}(1-\mathrm{P}_s(v''))\\
\le&\frac{1}{|U|}\sum_{s\in M}\mathrm{P}(X_a=s)\,T\le\frac{T}{|U|} \qquad (13)
\end{aligned}$$

である．よって

$$\begin{aligned}
&\max_{a\in A\backslash U}\frac{1}{|U|}\sum_{v\in U}\sum_{s\in M}\mathrm{P}(X_a=s)\,\mathrm{P}_s(v)\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\backslash\{v\}\\ \sharp I=k}}\\
&\quad\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in(U\backslash\{v\})\backslash I}(1-\mathrm{P}_s(v''))\\
\le&\frac{T}{|U|} \qquad (14)
\end{aligned}$$

である．(11) 式についても同様に，各 $a\in U$ に対して，

$$\begin{aligned}
&\max_{a\in U}\frac{1}{|U|-1}\sum_{v\in U\,:\,v\neq a}\sum_{s\in M}\mathrm{P}(X_a=s)\,\mathrm{P}_s(v)\\
&\quad\sum_{k=0}^{T-1}\sum_{\substack{I\subset U\backslash\{v\}\\ \sharp I=k}}\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in(U\backslash\{v\})\backslash I}(1-\mathrm{P}_s(v''))\\
\le&\frac{T}{|U|-1} \qquad (15)
\end{aligned}$$

である．ゆえに，

$$\mathrm{WAP}^{\mathrm{prop}}\le\frac{T}{|U|-1}$$

である． □

本人拒否率 $\mathrm{FRR}^{\mathrm{prop}}$ の計算を行う．1 人の正規ユーザが 1 回のサンプルの提示により，自分との照合に成功した上で，さらに照合に成功する他の正規ユーザの人数の分布を表す確率変数を Y とする．つまり

$$\begin{aligned}
&\mathrm{P}(Y=k)=\frac{1}{|U|}\sum_{u\in U}\sum_{s\in M}\mathrm{P}(Y_u=s)\,\mathrm{P}_s(u)\\
&\quad\sum_{\substack{I\subset U\backslash\{u\}\\ \sharp I=k}}\prod_{v'\in I}\mathrm{P}_s(v')\prod_{v''\in(U\backslash\{u\})\backslash I}(1-\mathrm{P}_s(v''))
\end{aligned} \qquad (16)$$

である．このとき，

$$\begin{aligned}
&\mathrm{FRR}^{\mathrm{prop}}\\
&=\mathrm{FRR}+\sum_{k=T}^{|U|-1}\mathrm{P}(Y=k)=\mathrm{FRR}+\mathrm{P}(Y\ge T)
\end{aligned} \qquad (17)$$

定理 3. 確率変数 X の表す確率分布の平均を μ, 標準偏差を σ とする．$T=\mu+a\sigma$ のとき次が成立する．

$$\mathrm{FRR}^{\mathrm{prop}}\le\mathrm{FRR}+\frac{1}{a^2} \qquad (18)$$

証明. チェビシェフ不等式から，誤一致人数 Y の表す確率分布の平均を μ, 標準偏差を σ として，任意の実数 a を選ぶとき，

$$\mathrm{P}(|Y-\mu|\ge a\sigma)\le\frac{1}{a^2} \qquad (19)$$

が成り立つ．ここで，$Y\ge T$ ならば，$|Y-\mu|\ge a\sigma$ であるから，

$$\mathrm{P}(Y\ge T)\le\mathrm{P}(|Y-\mu|\ge a\sigma) \qquad (20)$$

となり，

$$\mathrm{P}(Y \geq T) \leq \frac{1}{a^2} \tag{21}$$

が成り立つ．ゆえに，(17),(21) 式より

$$\mathrm{FRR}^{\mathrm{prop}} \leq \mathrm{FRR} + \frac{1}{a^2}$$

となることがわかる． □

6 $\mathrm{WAP}^{\mathrm{prop}}$ と $\mathrm{FRR}^{\mathrm{prop}}$ のトレードオフ

$\mathrm{WAP}^{\mathrm{prop}}$ と $\mathrm{FRR}^{\mathrm{prop}}$ がそれぞれ定理 2，3 で示した上界 $\mathrm{WAP}^{\mathrm{prop}}_{\mathrm{ub}} = \frac{T}{|U|-1}$, $\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}} = \mathrm{FRR} + \frac{1}{a^2}$ $(T = \mu + \sigma)$ をとるとき，2 つのトレードオフを考える．(18) 式より，

$$\frac{1}{\sqrt{\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FRR}}} = a \tag{22}$$

となる．ここで，$T = \mu + a\sigma$ より，$a = (T - \mu)/\sigma$ なので，これを (22) に代入して，

$$\frac{1}{\sqrt{\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FRR}}} = \frac{T - \mu}{\sigma} \tag{23}$$

とできる．さらに，(9) 式より，ユーザ数を n とすれば，$T = (n-1)\,\mathrm{WAP}^{\mathrm{prop}}_{\mathrm{ub}}$ となり，また，誤一致人数の平均 $\mu = (n-1)\,\mathrm{FAR}$ で表されることから，(23) 式は，

$$\frac{1}{\sqrt{\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FRR}}} = (n-1)\frac{\mathrm{WAP}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FAR}}{\sigma} \tag{24}$$

となる．これを整理して，

$$\frac{\sigma}{(n-1)} = (\mathrm{WAP}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FAR})\sqrt{\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}} - \mathrm{FRR}} \tag{25}$$

となり，$\mathrm{WAP}^{\mathrm{prop}}_{\mathrm{ub}}$ と $\mathrm{FRR}^{\mathrm{prop}}_{\mathrm{ub}}$ のトレードオフの関係が導かれた．(25) 式より，十分小さい σ（例えば，認証精度が高く，本人分布の分散が小さいようなモダリティにおいて，σ は十分小さい）であれば，今回の提案アルゴリズムは，認証精度を低下させることなく，ウルフ攻撃確率を小さく抑えることができると考えられる．

7 まとめと今後の課題

バイオメトリクス認証のモデルを定義し，通常の 1 対 1 認証の照合アルゴリズムにおける安全性評価尺度である FAR と認証精度評価尺度である FRR を導出した．また，ウルフを用いたなりすまし攻撃に対する評価尺度である WAP を導出した．

本論文では，ウルフ攻撃に対して安全な新しい照合アルゴリズムを提案し，安全性と認証精度を証明した．本提案アルゴリズムにおいて，ウルフ攻撃確率（$\mathrm{WAP}^{\mathrm{prop}}$）他人受入率（$\mathrm{FAR}^{\mathrm{prop}}$）本人拒否率（$\mathrm{FRR}^{\mathrm{prop}}$) の上界を示した．さらに，$\mathrm{WAP}^{\mathrm{prop}}$ と $\mathrm{FRR}^{\mathrm{prop}}$ の上界のトレードオフを示し，認証精度の高いモダリティにおいては，その両方を同時に小さくすることが可能なことを証明した．

今後の課題として，具体的なモダリティ（例えば，Daugman の虹彩認証など）に対して，σ や μ を計算し，実際に有効かどうかを検討するということが考えられる．

参考文献

[1] J.Daugman,“How Iris Recognition Works, IEEE Transactions on Circuits and Systems for Video Technology,” vol. 14, No. 1, pp. 21-30, January 2004

[2] M. Une, A. Otsuka, H. Imai, “Wolf Attack Probability : A New Security Measure in Biometric Authentication Systems, ” International Conference on Biometrics ICB2007, LNCS 4642, pp. 396-406.

[3] 渡邉直彦，繁富利恵，宇根正志，大塚 玲，今井秀樹，“指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ，” Proc of CSS2006, pp.621-626,2006.

[4] 河上梨恵，繁富利恵，美添一樹，宇根正志，大塚玲，今井秀樹，“マニューシャ・マッチングのウルフに関する理論的考察，” Proc of SCIS2007, 2007.