SCIS 2009 The 2009 Symposium on Cryptography and Information Security
Otsu, Japan, Jan. 20-23, 2009
The Institute of Electronics, Information and Communication Engineers

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

An Efficient and Secure Protocol in a Framework of Matching Algorithms Based on Wolf Attack Probability

小島 由大* 繁富 利恵*† 井沼 学† 大塚 玲*†
Yoshihiro Kojima Rie Shigetomi Manabu Inuma Akira Otsuka
今井 秀樹*†
Hideki Imai

あらまし 近年，バイオメトリクス認証の普及とともにそのセキュリティの評価が重要となってきている．その要因として，ウルフを用いたなりすまし攻撃が挙げられる．現在，ウルフに関する研究が活発にされていて，いくつかのモダリティにおいては，ウルフが実際に発見されている．そこで，ウルフ攻撃に対して安全なマッチングアルゴリズムを構成するためのフレームワークが必要となる．本稿では，虹彩認証のマッチングアルゴリズムを例にとり，理想的に安全なマッチングアルゴリズムと従来のマッチングアルゴリズムを用いて安全性と可用性の両面から評価をし，ウルフ攻撃に対して安全なマッチングアルゴリズムを定義する．また，そのフレームワーク内において，ウルフ攻撃に対し安全で，かつ実現可能性の高いマッチングアルゴリズムの一つとして，CSS2008 で提案したマッチングアルゴリズムを紹介する．

キーワード バイオメトリクス認証，ウルフ，WAP，マッチングアルゴリズム，フレームワーク

1 はじめに

バイオメトリクス認証が広く利用されるにつれ，バイオメトリクス認証システムの安全性の評価がますます重要となってきている．

バイオメトリクス認証システムの脅威の 1 つとして，なりすましがある．田辺らは，指静脈認証の特徴抽出アルゴリズムにおいて，実際にウルフを発見する [1] など，特にウルフを用いたなりすましが注目されている．しかし，一般的なマッチングアルゴリズムは，なりすましに対する安全性の評価尺度として他人受入率（FAR）を参照することが多いため，ウルフ攻撃のような意図的なになりすましに対して必ずしも安全とは言えない．ウルフ攻撃に対する安全性の評価尺度として，ウルフ攻撃確率（WAP[2]）がある．既存のマッチングアルゴリズムは新しいセキュリティ評価尺度である WAP を考慮して設計されておらず，WAP が極端に高くなる例も示されている．指静脈パターンマッチングアルゴリズムにおいて，WAP = 1 となる（どのような登録情報に対しても一致と判定される）ウルフが発見された [3] という報告もある．そこで，ウルフ攻撃に対して安全なマッチングアルゴリズムを構成するためのフレームワークが必要となる．

本稿では，まずバイオメトリクス認証における精度評価と安全性評価尺度として，本人拒否率（FRR）・FAR・WAP を定義し，ウルフ攻撃に対して安全なマッチングアルゴリズムを定義する．その定義から，理想的に安全なマッチングアルゴリズムを示し，一般的なマッチングアルゴリズムについて考察を行う．

既存研究 [4] によれば，理想的に安全なマッチングアルゴリズムはウルフ攻撃に対して安全ではあるが実際に使うには時間がかかりすぎてしまい，一般的なマッチングアルゴリズムは，時間を考慮する必要はないが，ウルフに対して安全とは言えない．つまり，ウルフに対して安全かつ実用に耐えるようなマッチングアルゴリズムは存在しないとされている．

* 中央大学理工学研究科，〒 112-8551 東京都文京区春日 1-13-27, Graduate School of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan E-mail: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 10 階 1003 号室, Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Akihabara-Daibiru Room 1003, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan E-mail: {rie-shigetomi,inuma.manabu,a-otsuka,h-imai} @aist.go.jp

我々は CSS2008 において，通常の固定しきい値マッチングアルゴリズムと受け入れ人数による判定を連結させたマッチングアルゴリズム [5] を提案した．本稿では，この提案アルゴリズムを井沼ら [4] によるフレームワークの中で再評価する．その結果，我々の提案アルゴリズムは，ウルフ攻撃に対して安全でかつ実現可能な処理時間が期待できるものであることが明らかとなった．

本稿の構成は次の通りである．2 章において，バイオメトリクス認証のモデルを説明する．3 章において，バイオメトリクス認証の精度評価と安全性評価について説明する．4 章において，ウルフ攻撃に対して安全なマッチングアルゴリズムを定義する．5 章において，WAP 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ついて説明する．6 章において，安全で実現可能な処理時間のマッチングアルゴリズムについて説明する．7 章においてまとめ，8 章において，今後の課題について述べる．

2 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 はある集合で, 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 [6] 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．マッチングアルゴリズムは，$\mathrm{match} : M \times M \to \{\text{“accept”}, \text{“reject”}\}$ 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（ハミング）距離を計算して 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 $\mathrm{Prob}[v \text{ accepts } u]$ 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マッチング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．

マッチングアルゴリズム

$u \in U$: 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 精度評価と安全性評価

3.1 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 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，

$$\begin{aligned}\mathrm{FRR} &= 1 - \operatorname*{Ave}_{u\in U} \mathrm{Prob}[u \text{ accepts } u] \\ &= 1 - \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(u) \\ &= \frac{1}{|U|} \sum_{u\in U} \sum_{s\in M} \mathrm{P}(X_u = s)(1 - \mathrm{P}_s(u)) \qquad (2)\end{aligned}$$

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．

3.2 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．

3.2.1 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．

$$\begin{aligned}
&\mathrm{FAR} = \\
&\underset{(u,v)\in(U\times U)^{diff}}{\mathrm{Ave}} \mathrm{Prob}[v \text{ accepts } u] \\
&= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \mathrm{Prob}[v \text{ accepts } u] \\
&= \frac{1}{|U|\cdot(|U|-1)} \sum_{(u,v)\in(U\times U)^{diff}} \sum_{s\in M} \mathrm{P}(X_u = s)\,\mathrm{P}_s(v) \quad (3)
\end{aligned}$$

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

3.2.2 ウルフ攻撃

攻撃者は, 攻撃対象のバイオメトリクス認証システムのアルゴリズムを知っており，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（特定の個人のバイオメトリクス情報を知らない）．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，

$$\mathrm{WAP} = \max_{a\in A} \underset{v\in U}{\mathrm{Ave}}\, \mathrm{Prob}[v \text{ accepts } a] \quad (4)$$

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．

4 ウルフ攻撃に対して安全なマッチングアルゴリズムの定義

あるマッチングアルゴリズムが $\mathrm{WAP} < \delta$ $(0 < \delta)$ を満たすとき，このマッチングアルゴリズムをウルフ攻撃に対して δ-secure であると定義する．また，十分小さい δ に対して δ-secure であるマッチングアルゴリズムを単に，ウルフ攻撃に対して安全なマッチングアルゴリズムと呼ぶ.

今，入力するバイオメトリクス情報とそれに対応する登録テンプレートとの（ハミング）距離を計測し，その距離があるしきい値 τ より近いかどうかで認証を行う方式を考える．

多くのマッチングアルゴリズムでは，FRR と FAR からしきい値 τ を設定している．しかし，これではウルフ攻撃に対して安全なマッチングアルゴリズムは構成できない.

4.1 理想的なマッチングアルゴリズム

理想的なマッチングアルゴリズムは，入力ごとに入力に対してすべてのユーザから得られるサンプルとの照合結果を用いてしきい値 τ を決定するマッチングアルゴリズムである．

このマッチングアルゴリズムは，入力ごとにすべてのユーザと照合を行い，その後しきい値 τ を決定するため，ウルフ攻撃確率を常に他人受入率と（ほぼ）同じ確率に保つことが可能となる．ただし，すべてのユーザの中で，入力に対して一番距離が短いものを選ぶという方法は，今は考えない．そうしてしまうと，1 対 1 バイオメトリクス認証のモデルと矛盾が生じてしまう．このモデルにおいては，入力として提示されたバイオメトリクス情報が認証を行うユーザの名乗ったテンプレートであるかどうかのみを判定する．

理想的なマッチングアルゴリズムでは次の式が成り立つ.

$$\mathrm{WAP}^{\mathrm{ideal}} = \mathrm{FAR}^{\mathrm{ideal}} \quad (5)$$

しかし，このマッチングアルゴリズムは，ウルフに対する安全性はあるが，すべてのユーザとの照合を行ったあとに照合結果の分布に対して適切なしきい値 τ を決定しなければならないため，実現不可能な処理時間を要してしまう.

4.2 従来のマッチングアルゴリズム

虹彩認証の従来のマッチングアルゴリズムを例として，Daugman の 2 つのマッチングアルゴリズムについて検討を行う.

4.2.1 しきい値固定マッチングアルゴリズム [6]

しきい値固定マッチングアルゴリズムは，最も簡単なマッチングアルゴリズムで，入力によらず，常にしきい値 τ は一定である.

そのため，しきい値固定マッチングアルゴリズムでは，ウルフ攻撃を防ぐことができない.

4.2.2 ビット長可変マッチングアルゴリズム [7]

ビット長可変マッチングアルゴリズムは，しきい値固定マッチングアルゴリズムを改良したもので，入力サンプルの有効ビット長（[7] では，虹彩領域から，アイリス

コードと呼ばれる固定長ビット列を生成するが，虹彩領域と重なるまぶたやまつげ等の照合に用いない部分を取り除くため，入力によって有効ビット長が変化する）に比例して，しきい値 τ を変化させるマッチングアルゴリズムである．

論文 [8, 9] の結果から，入力するバイオメトリクス情報の持つエントロピーが消失ビット以外の有効ビット長に比例すると仮定すれば，エントロピーを減らすようなウルフ攻撃に対してのみ安全と言える．しかし，入力するバイオメトリクス情報の持つエントロピーは虹彩領域に均一に分布しているわけではないため，入力情報のエントロピーが有効ビット長に比例しない．

よって，より詳しいエントロピー情報をもつ攻撃者を仮定すると，ビット長可変マッチングアルゴリズムもウルフ攻撃に対して安全であるとは言えない．

5 WAP を考慮したマッチングアルゴリズムのフレームワーク

理想的なマッチングアルゴリズムとしきい値固定マッチングアルゴリズムから，WAP を考慮したマッチングアルゴリズムのフレームワークを検討する．理想的なマッチングアルゴリズムを考えると，ウルフ攻撃を考慮した安全性は非常に高いが，処理時間が実現不可能なほどかかってしまう．それに対して，しきい値固定マッチングアルゴリズムを考えると，ウルフ攻撃を考慮した安全性は非常に低いが，処理時間はほとんどかからない．

2 つのマッチングアルゴリズムを基にして，それぞれのマッチングアルゴリズムの位置づけを図 1 に示す．縦軸にウルフ攻撃に対する安全性をとり，また，横軸に処理時間をとり，上に行くほど安全性が高いことを表している．右に行くほど処理時間が早いことを表している．

論文 [4] によると，安全性（security）と可用性（efficiency）がトレードオフの関係にあり，ウルフ攻撃に対して安全かつ実現可能な処理時間のマッチングアルゴリズムが未だ発見されていないことが述べられている．つまり，ウルフ攻撃に対して安全かつ実現可能な処理時間のマッチングアルゴリズムがないということである．

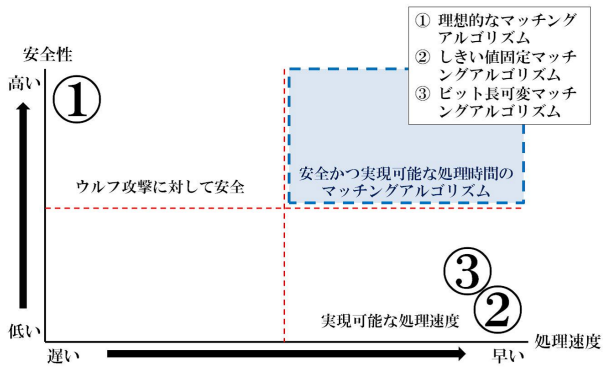

図 1: フレームワークにおける各マッチングアルゴリズムの位置づけ 1

6 安全で実現可能な処理時間のマッチングアルゴリズム

CSS2008 で提案したウルフ攻撃に対して安全なマッチングアルゴリズムは，一般的なバイオメトリクスの 1 対 1 マッチング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．詳細なアルゴリズムを次に示す．

マッチングアルゴリズム

$u \in U$: 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

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

この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 $\mathrm{FAR}^{\mathrm{prop}}$, $\mathrm{WAP}^{\mathrm{prop}}$, $\mathrm{FRR}^{\mathrm{prop}}$ とすると，それぞれ次のような結果が得られる．

定理 1.

$$\mathrm{FAR}^{\mathrm{prop}} \leq \mathrm{FAR} \tag{6}$$

定理 2.

$$\mathrm{WAP}^{\mathrm{prop}} \leq \frac{T}{|U|} \tag{7}$$

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．

$$\mathrm{FRR}^{\mathrm{prop}} \leq \mathrm{FRR} + \frac{1}{a^2} \tag{8}$$

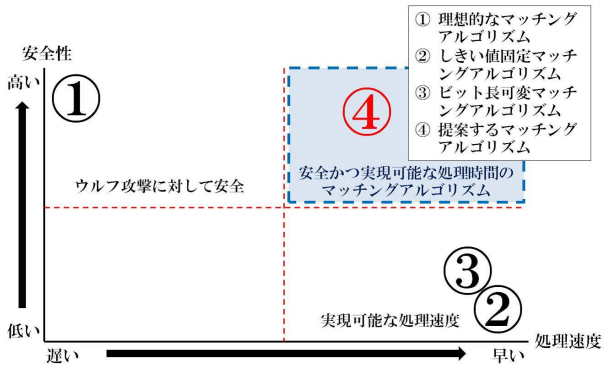

図 2: フレームワークにおける各マッチングアルゴリズムの位置づけ 2

ここで，FAR, FRR は基となるマッチングアルゴリズムの他人受入率，本人拒否率を表している．

ウルフ攻撃に対する安全性において，式 (7) より，このマッチングアルゴリズムが $(T/|U|)$-secure であるということがわかる．

処理速度においても，このマッチングアルゴリズムは，照合に用いる登録テンプレートを照合をし易くするような処理を行う（例えば，虹彩から抽出されるアイリスコードのようにビット列に変換して保存する等）ことで，高速化することが可能となる．また，登録テンプレートとの照合において，誤一致人数が人数しきい値 T を超えた時点でその入力はウルフと判定されるため，すべての登録テンプレートとの照合を完了するよりも早く，照合結果が得られる場合もある．つまり，このマッチングアルゴリズムが十分実用に耐える処理速度であるということがわかる．

以上のことから，このフレームワークにおいて，このマッチングアルゴリズムは，図 2 の位置づけになると考えられる．理想的なマッチングアルゴリズムほど安全性は高くはないが，ウルフ攻撃に対して十分な安全性があり，固定しきい値マッチングアルゴリズムやビット長可変マッチングアルゴリズムほど処理速度は早くはないが，十分実用に耐える速度を達成している．

7 まとめ

本稿では，ウルフ攻撃に対して安全なマッチングアルゴリズムを定義し，理想的なマッチングアルゴリズムと従来のマッチングアルゴリズムから，WAP を考慮したマッチングアルゴリズムのフレームワークを論文 [4] にならい定義した．また，そのフレームワークによれば，ウルフ攻撃に対して安全かつ処理時間の早いマッチングアルゴリズムは存在しない．

論文 [4] のフレームワークの中で，我々が CSS2008 で提案したマッチングアルゴリズムを再評価した．このマッチングアルゴリズムは，図 2 より，ウルフ攻撃に対して安全かつ処理時間の早いマッチングアルゴリズムであると言える．

8 今後の課題

今後の課題として，WAP を考慮したマッチングアルゴリズムのフレームワーク内において，今回紹介した CSS2008 で提案した我々のマッチングアルゴリズムとは異なった，より安全性の高いもの，もしくは，より処理速度の早いものを検討するということが考えられる．

参考文献

[1] 田辺康宏，美添一樹，今井秀樹，“指静脈認証システムにおけるセキュリティ評価手法の提案，” 暗号と情報セキュリティシンポジウム 2008 SCIS2008, 2008

[2] M. Une, A. Otsuka, and H. Imai, “Wolf Attack Probability : A New Security Measure in Biometric Authentication Systems, ” International Conference on Biometrics 2007 ICB2007, LNCS 4642, pp. 396-406, 2007

[3] 渡邉直彦，繁富利恵，美添一樹，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- 特徴抽出過程を含めた考察- ，” 暗号と情報セキュリティシンポジウム 2007 SCIS2007, 2007

[4] M. Inuma, A. Otsuka, and H. Imai, “Theoretical framework for constructing matching algorithms in biometric authentication systems, ” International Conference on Biometrics 2009 ICB2009, 2009（投稿中）

[5] 小島由大，繁富利恵，井沼学，大塚玲，今井秀樹，“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，” コンピュータセキュリティシンポジウム 2008 CSS2008, pp. 809-814, 2008

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

[7] J. Daugman,“Probing the Uniqueness and Randomness of IrisCodes : Results From 200 Billion Iris Pair Comparisons, ” Proceedings of the IEEE, vol. 94, No. 11, pp. 1927-1935, November 2006

[8] 小島由大，繁富利恵，美添 一樹，井沼学，大塚玲，今井秀樹，“虹彩認証におけるウルフ攻撃確率の理

論的考察, ” 暗号と情報セキュリティシンポジウム 2008 SCIS2008, 2008

[9] 小島由大, 繁富利恵, 井沼学, 大塚玲, 今井秀樹, “虹彩認証におけるウルフ攻撃確率の理論的考察その 2 , ” バイオメトリックセキュリティ研究会, 2008