合成ウルフを用いた安全性評価に関する一考察

米澤 祥子 †‡　　姜 玄浩 ‡　　大塚 玲 †　　今井秀樹 †‡

† 産業技術総合研究所
101-0021 東京都千代田区外神田 1-8-13
{s-yonezawa, a-otsuka, h-imai}@aist.go.jp

‡ 中央大学
112-8551 東京都文京区春日 1-13-27
kang@imailab.jp

あらまし　バイオメトリクス認証システムに対し、合成ウルフを用いたセキュリティ評価手法を提案する。本手法では、テスト物体アプローチの生体特徴に関するパラメータを変化させながらウルフを探索し、ウルフ攻撃確率を評価する。本手法を用いると、従来アルゴリズムが公開されたシステムに対して適用されていたウルフ攻撃確率によるセキュリティ評価を、実際の製品に対しても適用できると期待される。

A Study on Security Evaluation Using Synthesized Wolf Samples

Shoko Yonezawa†‡　　Hyunho Kang‡　　Akira Otsuka†　　Hideki Imai†‡

†National Institute of Advanced Industrial Science and Technology (AIST)
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021
{s-yonezawa, a-otsuka, h-imai}@aist.go.jp
‡Chuo University
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551
kang@imailab.jp

Abstract　We show a new approach to the security evaluation for biometric authentication systems named “synthesized wolf” approach, which focuses on the parameters representing biometric characteristics. The goal of our appoach is to find “wolf” of the target system by changing these parameters, and to estimate Wolf Attack Probability (WAP) of the system. This approach comes from “test object” approach, which creates a dummy sample from acquired biometric samples of target person and checks whether the dummy sample is accepted by the system or not. Our approach is expected to be applied for the evaluation of black-box biometric products.

1　はじめに

近年、セキュリティの確保は社会的に重要な問題であり、本人を確認するための個人認証は特に注目を集めている。バイオメトリクス認証も個人認証技術のひとつであり、人間の身体的特徴や行動的特徴を用いて個人を認証する。これはパスワード認証や IC カード認証と違い生体情報のみを認証に用いるため、手軽な認証方式として注目されており、実際に銀行の ATM や入国審査等で用いられている。このようにバイオメトリクス認証が広く利用されるようになると、システムのセキュリティはバイオメトリクス認証のセキュリティに依存することになる。

つまり、バイオメトリクス認証に対するセキュリティ評価が必要になる。

バイオメトリクス認証のセキュリティ評価手法には、テスト物体アプローチとウルフ攻撃アプローチがある。テスト物体アプローチでは、実際の生体情報を取得して模造物をテスト物体として提示し、システムの評価を行う手法である。この手法では実際の認証システム製品等をブラックボックス評価できるが、生体情報を手に入れる必要がある。これに対しウルフ攻撃アプローチは、攻撃者が生体情報を知らないがウルフの存在を知っているとき、そのウルフをバイオメトリクス認証システムに提示してシステムの評価を行う手法である。この手法では生体情報の模造物を必要とせず、FAR (False Accept Rate: 他人受入率) より強い意味での安全性を言うことができる。しかし、このようなウルフを見つけるためには個々のアルゴリズムに関する知識が必要であるため、必然的にホワイトボックス評価となる。そのため、メーカー自身による製品評価には利用できるが、第二者認証や第三者認証での利用には技術仕様の詳細を評価機関等に公開する必要がある。

そこで本稿では、合成ウルフによるセキュリティ評価手法を提案する。本評価手法は、ブラックボックスシステムに対してウルフを探索し、合成ウルフを作製してウルフ攻撃確率を測定する。本稿ではまた、テスト物体アプローチの生体特徴パラメータに着目し、システムに受理されたテスト物体から合成ウルフを作製する方法を提案する。我々のアプローチは、システムに受理されたテスト物体の生体特徴パラメータを変化させ、システムの挙動を観察することによりシステムの内部アルゴリズムを推定し、その情報を基に合成ウルフを作製するものである。さらに、アルゴリズムの推定に利用できると考えられる生体特徴パラメータを具体的に挙げ、その推定方法について述べる。この方法で合成ウルフを作成することができれば、アルゴリズムの仕様を知らずにウルフを作製できたことになり、生体認証システム製品の新たなセキュリティ評価手法として期待される。

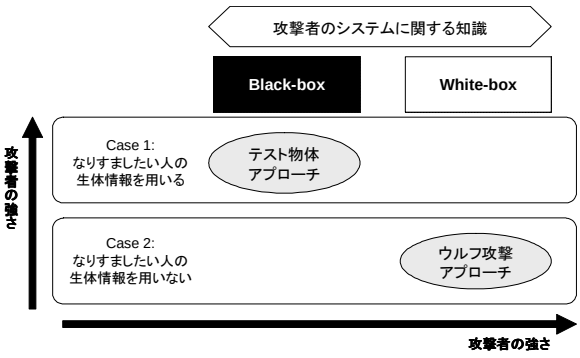

図 1: セキュリティ評価手法の分類

2 バイオメトリクス認証システムのセキュリティ評価手法

本章では、バイオメトリクス認証システムのセキュリティ評価技術について詳しく説明する。

2.1 テスト物体アプローチ

テスト物体アプローチは、実際の生体情報を利用してテスト物体を作製し、このテスト物体をバイオメトリクス認証システムに提示したときの挙動を観察することによってセキュリティ評価を行うものである。

テスト物体を用いたセキュリティ評価の手順は、以下の通り分類できる。

第 1 段階

(A) テスト物体の登録が可能か

(A-A) テスト物体の登録に対し、テスト物体による照合が可能か

第 2 段階

(A-L) テスト物体の登録に対し、身体部分による照合が可能か

(L-A) 身体部分の登録に対し、テスト物体による照合が可能か

これらの試行を多様なテスト物体を用いて複数のシステムに対して行い、結果を比較することによって、システムのセキュリティを評価することができる。

また、テスト物体の作製手順は、

(1) 生体情報の取得

(2) テスト物体の作製

に分けることができる。ここで、生体情報の取得時には、生体情報の取得コストや取得される生体情報の特性がパラメータとして関係する。同様に、テスト物体の作製時には人工物の作製コストや作製される人工物の特性がパラメータとして関係する。また、評価対象の認証システムで用いられる身体部分についても、人間の持つ特性がパラメータとして関係する [5]。つまり、これらの処理は以下のように関数で表すことができる。

- $\mathcal{C}(c_1, \cdots, c_u)$：生体情報取得関数
- $\mathcal{L}(l_1, \cdots, l_v)$：身体部分関数
- $\mathcal{M}(m_1, \cdots, m_w)$：テスト物体作製関数

例えば、文献 [5] で示された生体情報取得関数は、$\mathcal{C}(\rho, \lambda, \alpha)$ と表すことができる。ここで、ρ は撮像解像度、λ は光源波長、α は光源照射角度を表す。また文献 [7] のテスト物体作製関数は、$\mathcal{M}(str, s, p, d)$ と表すことができる。ここで、str はテスト物体の形状、s は表面層の素材、p は印刷物の枚数、d はテスト物体の透過率を表す。

また、身体部分関数 $\mathcal{L}$ を生体情報取得関数 $\mathcal{C}$ で取得した生体情報を $B(\mathcal{L}(l_1, \cdots, l_v), \mathcal{C}(c_1, \cdots, c_u))$, この生体情報に基づきテスト物体作製関数 $\mathcal{M}$ で作製されたテスト物体を $A(B(\mathcal{L}(l_1, \cdots, l_v), \mathcal{C}(c_1, \cdots, c_u)), \mathcal{M}(m_1, \cdots, m_w))$ と表すことができる。これは、各関数のパラメータにより多様なテスト物体を作製できることを意味する。

テスト物体アプローチでは、テスト物体による評価結果の校正用のバイオメトリクス認証システムを準備し、それらを評価対象のひとつとして他の評価対象システムと横並びでテストを実施するという研究が行われている。また、テスト物体の種類やテスト結果の分類方法の提案もされている [5]。

2.2 ウルフ攻撃アプローチ

ウルフ攻撃アプローチは2007年に宇根, 大塚, 今井によって提案された新しいセキュリティ評価手法である [6]。本アプローチでは、複数のテンプレートと高い類似度を有するサンプルをウルフ (wolf) 、ウルフを認証システムに提示したときなりすましに成功する確率をウルフ攻撃と定義し、ウルフ攻撃の成功確率がどこまで高まるかを評価する。

$\mathcal{U}$ をユーザの集合、$\mathcal{A}$ をあらゆる物体の集合、$\mathcal{M}$ を生体特徴の集合とする。このとき、$u \in \mathcal{U}$ から取得した生体特徴 $t_{u_k} \in \mathcal{M}$ $(k = 1, \ldots, m)$ と $w \in \mathcal{A}$ が一致する確率の平均値が受入確率より大きいとき、w をウルフと呼ぶ。ウルフ攻撃とは、攻撃者がユーザ $u \in \mathcal{U}$ の生体特徴を知らないが認証システムのアルゴリズムを完全に知っているという条件の下で、ウルフ w を利用して行うなりすまし攻撃のことである。また、認証システムに対してウルフ攻撃が成功する確率の最大値をウルフ攻撃確率 (WAP) と呼ぶ。ウルフおよび WAP の厳密な定義は [8] を参照されたい。

ウルフ攻撃ではなりすまし対象の生体特徴を必要としないが、認証システムに対するウルフの存在を知っていると仮定する。実際に、あるタイプの指紋マニューシャ照合アルゴリズムとあるタイプの指静脈パターン照合アルゴリズムに対して、ウルフが存在し、WAP が FAR より高くなることが示されている [6]。また、それぞれのアルゴリズムに関し、ウルフ攻撃に対して安全なアルゴリズムも提案されている [8]。

ただし、一般的にウルフを見つけるためには、認証システムの内部アルゴリズムを解析する必要がある。そのため、一般のブラックボックス認証システムに対してウルフが見つけられるかどうかは分かっていない。

3 合成ウルフによるセキュリティ評価

本章では、合成ウルフを用いたセキュリティ評価手法を提案し、テスト物体アプローチの結

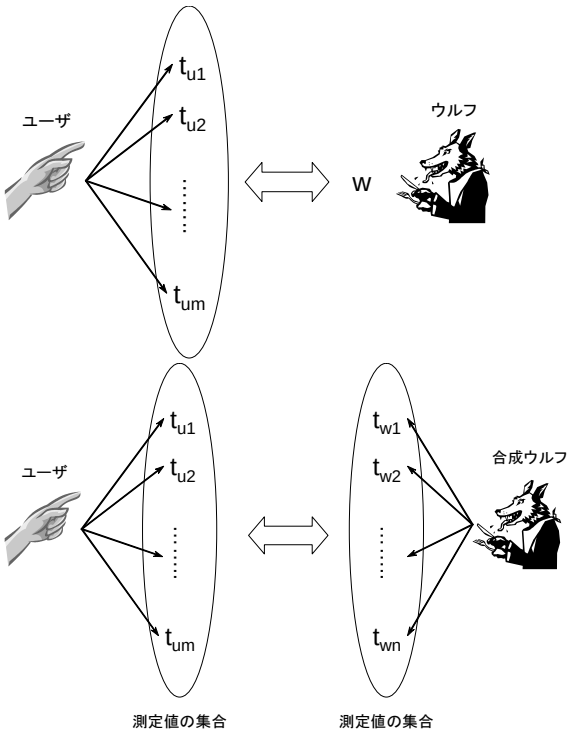

図 2: 合成ウルフの測定誤差

果を利用して合成ウルフを作製する方法について考察する。本アプローチは、テスト物体アプローチの生体特徴に関するパラメータを変化させる部分に焦点を当てたものである。

3.1 測定誤差を考慮したウルフ攻撃確率

従来のウルフ攻撃確率では、生体特徴は観測によってばらつきがあるが、ウルフは誤差がないものとして考えていた。これに対し合成ウルフを用いた攻撃では、合成ウルフの測定にも誤差が生じる可能性が考えられる。これを踏まえて、双方の測定誤差を考慮してウルフ攻撃確率を定義する。

$\mathcal{U}$ をユーザの集合、$\mathcal{A}$ をあらゆる物体の集合、$\mathcal{M}$ を生体特徴の集合とする。$u \in \mathcal{U}$, $w \in \mathcal{A}$ に対し、X_u および X_w を $\mathcal{M}$ の上の確率変数とする。また、$d : \mathcal{M} \times \mathcal{M} \to \mathrm{R}$ を $\mathcal{M}$ 上の距離関数とする。このとき、閾値を τ として、u と w が双方の測定誤差を含めて一致する平均確率 $P_{(u,w)}$ は

$$P_{(u,w)} = \sum_{\substack{s \in X_u, t \in X_w \\ d(s,t) < \tau}} P(X_u = s) P(X_w = t)$$

と表される。従って、ウルフ攻撃確率 WAP は

$$\begin{aligned} WAP &= \max_{w \in \mathcal{A}} \operatorname*{Ave}_{u \in \mathcal{U}} P_{(u,w)} \\ &= \max_{w \in \mathcal{A}} \operatorname*{Ave}_{u \in \mathcal{U}} \sum_{\substack{s \in X_u, t \in X_w \\ d(s,t) < \tau}} P(X_u = s) P(X_w = t) \end{aligned}$$

と定義できる。

理論的にはこの式でウルフ攻撃確率の上限が与えられるが、実験でこの上限値を推定するのは一般に困難であり、本論文では認証システム製品等にウルフ攻撃に対する既知の脆弱性、すなわち確率が大きくなるような合成ウルフ $w \in \mathcal{A}$ が存在しないことを実験的に調べるアプローチを検討する。

3.2 合成ウルフの作製方法

本節では、認証システム製品等に対して確率の大きい合成ウルフを実験的に見つける方法を考察する。

2.1 節で示したように、テスト物体の作製には生体情報や認証に使われる身体部分の特性、および人工物の材料となる素材の特性がパラメータとして影響する。ここで、身体部分と素材に関するパラメータを固定すれば、変化するパラメータは生体情報のみとなる。

そこで、既に認証システムに受理されることが分かっているテスト物体に対し、その生体特徴パラメータを変化させたものを認証システムに提示し、その挙動を観察することにより内部アルゴリズムを推定することを考える。

以降、認証システムに受理されるテスト物体を**コピー生体**と呼び、コピー生体の生体特徴パラメータを変化させて新しく作製したテスト物体を**合成サンプル**と呼ぶ。

バイオメトリクス認証システムでは、あらかじめ登録されたテンプレートに対して、測定し

た生体情報から生体特徴を抽出し、テンプレートと比較することによって一致／不一致を判定する。これは一般に照合アルゴリズムと呼ばれる。照合アルゴリズムは利用する生体特徴によっていくつかの種類に分類できる。

このように、テスト物体に含まれるある生体特徴を変化させた合成サンプルを作製し、認証システムに提示したときの挙動を測定することにより、どの生体特徴が認証システムの判定に影響を与えているのか推定することができると考えられる。

例えば、指紋認証システムでマニューシャ照合と画像比較による照合を分類するようなテストを考える。取得した指紋画像から、画像的にはほとんど変化のないようにマニューシャの一部を除くとする。このような画像を用いて合成サンプルを作製すると、マニューシャ照合を用いているシステムでは挙動が変化するだろう。逆に、画像の一部のコントラストを変化させて指紋の一部を変化させたとする。このような画像を用いた合成サンプルでは、画像比較による照合を用いているシステムで挙動が変化すると推測できる。

このように、各種照合アルゴリズムを分類できるようなテストを構成できれば、認証システムの内部アルゴリズムを推定できると考えられる。ここから解析的手法を用いてウルフを見つけ、合成ウルフを作製することができる。

3.3 パラメータの例

指紋の太さ 相関関数を用いたマッチング等、画像比較を用いたマッチングアルゴリズムでは、画像中のどの部分を指紋として認識するかによって出力が変化する。コピー生体の指紋の太さを変化させたとき、認証システムの出力に影響が出る場合、認証システムが画像比較によるマッチングアルゴリズムを使っている可能性が高いと推定される。

静脈の太さ 三浦らによる指静脈認証 [2] では、画像から指静脈パターンを抽出し、静脈の部分と静脈でない部分を塗り分けた 2 値画像を作る。このとき、静脈かどうかの判断が難しい箇所はあいまい領域として取り扱う。コピー生体の静脈の太さを変化させたとき、認証システムに影響が出る場合、認証システムが静脈のあいまい領域判定アルゴリズムを使っている可能性が高いと推定される。

マニューシャの数 Ratha らによる指紋マニューシャマッチングアルゴリズム [1] では、マニューシャの数が影響する。コピー生体のマニューシャの数を増やしたとき、認証システムの出力に影響が出る場合、認証システムが Ratha らの指紋マニューシャマッチングアルゴリズムを使っている可能性が高いと推定される。

4 まとめと今後の課題

本稿では、合成ウルフを用いたセキュリティ評価手法を提案し、テスト物体アプローチを踏まえた合成ウルフの作製方法を提案した。今後の課題として、合成ウルフを見つけるための内部アルゴリズム推定方法を詳細に検討するとともに、実際のバイオメトリクス認証システムを使って本評価手法を実証実験することが挙げられる。

参考文献

[1] N.K.Ratha, J.H.Cornell, and R.M.Bolle, “Enhancing Security and Privacy in Biometric-Based Authentication Systems,” IBM Systems Journal, Vol.40, No.3, pp.614-634, 2001.

[2] 三浦直人, 長坂晃朗, 宮武孝文, “線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用,” 電子情報通信学会論文誌, D-II, Vol,J86-D-II, No.5, pp.687-687, 2003.

[3] 松本勉, “生体認証システムのセキュリティ設計とセキュリティ測定,” ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会, pp.57-64, 2006.

[4] 松本勉, 田中瑛一, “指血管パタン認証システムのテスト物体によるセキュリティ測定法,” コンピュータセキュリティシンポジウム 2006 (CSS2006), pp.639-644, 2006.

[5] 松本勉, 田中瑛一, “指静脈認証システムのテスト物体によるセキュリティ測定法の研究,” 2007 年暗号と情報セキュリティシンポジウム (SCIS2007).

[6] M. Une, A. Otsuka and H. Imai, “Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems,” in Proc. of ICB 2007, LNCS 4642, pp.396-406, 2007.

[7] 松本勉, 田中瑛一, “透過光利用バイオメトリック認証システムのためのテスト物体作製方法,” 2008 年暗号と情報セキュリティシンポジウム (SCIS2008).

[8] M. Inuma, A. Otsuka and H. Imai, “Theoretical Framework for Construction Matching Algorithms in Biometric Authentication Systems,” in Proc. of ICB 2009, LNCS 5558, pp.806-815, 2009.