

本人確認用の指紋の偽造対策についての検討

Counter Measures against Fake Fingerprints in Personal Identification

小林 哲二 *

Tetsuji KOBAYASHI

1. まえがき

パスワードや暗証番号は、漏洩や個人情報からの推定などによる危険が大きい。この対策の1つとして、多くのバイオメトリクス装置が開発されている。バイオメトリクスの情報が用いられる場合[1], [2], [3], バイオメトリクスの情報自体を偽造されるという危険がある。偽造した指紋パターンでも、市販の指紋照合装置（指紋認識装置）に受理される可能性が大きいということが報告されている[4]。著者は、攻撃者が偽造指紋を使用する可能性があることへの対策として、複数の指紋を連続入力することによって暗証番号を表現する新手法を提案し、誤り率などの評価を行ってきた[5], [6], [7], [8]。本稿では提案方法の安全性を評価する。

2. 指紋照合システムへの攻撃要素

指紋センサは、コンピュータまたは情報機器に指紋画像を入力する。入力された検査指紋と、登録指紋の一致性をチェックするために、指紋認識（指紋照合）アルゴリズムがある。指紋の偽造の要素は、指紋パターンの偽造と生体反応の偽造である。指紋パターンについては、合成樹脂などで偽造される可能性がある。指紋センサは、指紋の生体反応をチェックするために、電気伝導度、光の反射スペクトル、又は温度のような生体固有の特性を使用できる。しかし、偽造指紋を使用する攻撃者もこれらの生体特性を擬似する可能性がある。また、攻撃者生体指紋と本人偽造指紋を併用する（例えば偽造指紋の合成樹脂を生体指紋上に貼り付け、且つ部分的には生体指紋も露出しておく）攻撃の場合には、生体反応は攻撃者生体指紋でOKになり、且つ指紋パターンは本人偽造指紋でOKになることが発生し得る。

従って、ネットワーク環境における指紋照合装置の使用に際しては、偽造指紋が使用されることを前提とする必要がある。システムの管理者は、ユーザが所有する端末に接続されたバイオメトリクス機器をチェックできないので、偽造指紋の危険は、サービス窓口で使用される場合よりも、情報ネットワークシステムにおいて特に大きい。表1に、指紋の利用環境と偽造検出難易度の関係を示す。

表1 指紋の利用環境と偽造検出難易度の関係

指紋の利用環境	偽造検出	例
ネットワークのユーザ端末	極めて困難	ユーザのPC, 携帯電話機
システムの無人管理の専用端末	困難	金融機関のATM
システムの有人管理の専用端末	管理者の目視で可能	国際空港の入管審査

* 日本工業大学 〒345-8501 埼玉県宮代町学園台 4-1 情報棟, Nippon Institute of Technology, Dept. of Computer and Information Engineering, 4-1-1 Gakuendai, Miyashiro-machi, Saitama-ken, 345-8501 Japan

3. 複数の指紋による暗証番号の入力

3.1 提案方法の概要

提案方法は、ユーザが、左右の手の指から任意数の指を選択し、選択した指の指紋を用いて、数字・指紋シーケンス対応表に従って、指紋シーケンス（1つ以上の指紋が連続したものであり、同じ指紋の連続も可能）によって数字を表現し、更にそれを暗証番号の個々の数字について行って、指紋シーケンス連結（指紋シーケンスが複数個連結したもの）とする。これによって、指紋だけで暗証番号を入力することを可能とする。選択指、及び数字・指紋シーケンス対応表は、個々のユーザの秘密情報である。

提案方法は、指紋センサおよび指紋認識アルゴリズムに依存せずに実現できる。図1に、提案方法に基づく指紋シーケンスによる暗証番号入力、指紋センサ、及び指紋認識（指紋照合）の関係を示す。

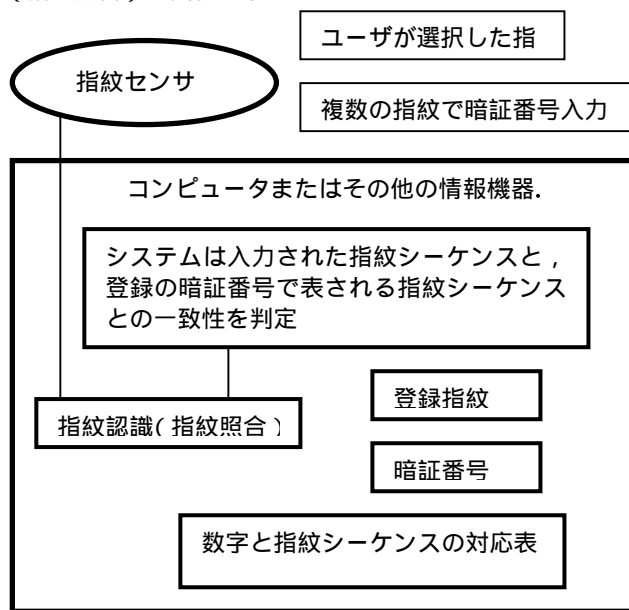


図1 提案方法による指紋による暗証番号入力の実現

3.2 複数の指紋の利用

複数の指紋を使用して、暗証番号を入力する方法では、ユーザが容易に指紋シーケンスを記憶できるように設定する。暗証番号は複数の数字から成る。選択された指の指紋を各々の数字に対応させる方法を以下に示す。

(1) セパレータ（区切り記号）

セパレータは、指紋シーケンスによる個々の数字を区分するものである。セパレータは、指紋センサからの指紋の入力、又はキーボードからのキー入力のどちらかで実現する。どちらが良いかはアプリケーションに依存する。セパレータは数字ごとに必要なので、暗証番号を入力するときのセパレータの入力回数を最小にするために、1つの数字について、1回の指紋入力、又は1回のキー入力になるように設定する。セパレータは、最後の数字の入力時には省略可能であるが、各数字に必ずセパレータを付加する。

ように定めておいた方がユーザに覚えやすいので、以下では、そのようにする場合を記述する。

(2) 数字と指紋シーケンスの対応付け方法

数字と指紋シーケンスの対応付けは、ユーザごとの秘密情報である。これは、1対1の方法と、1対多の方法に分類できる。1対1の方法では、個々の暗証番号と、それを表現する指紋シーケンス連結に1対1の対応がある。1対多の方法では、個々の暗証番号と、それを表現する指紋シーケンス連結の間に1対多の対応がある。提案方法は、システムが内部的に登録暗証番号に対する指紋シーケンス連結を登録されている指紋から生成できるので、1対1、及び、1対多の対応方法のどちらにも使用できる。実際に使用する場合には、1対1の対応方法が望ましい。

キーボードのキー入力をセパレータとして使用する場合、個々の数字を表す指紋シーケンスがそれぞれ異なるように設定すれば、必ず、1対1の対応方法になる。

指紋をセパレータとして使用する場合には、セパレータとして選択された指紋が数字を表すために使用されず、且つ個々の数字を表す指紋シーケンスが異なっていれば、1対1対応方法になる。そうでない場合（即ち、セパレータの指紋も数字を表すために兼用される場合）には、指紋シーケンス連結の区切りが不明確になるので1対1の対応方法にならないことがある。

以下において、指紋をセパレータとして使用する場合には、1対1の対応方法の例を示す。

【3個の指紋による数字・指紋対応方法（例）】

選択した3本の指の3個の指紋(A, B, S)を用いる場合には、次の方法で数字を指紋シーケンスにより表現できる。

1S（即ち、1回指紋Sを入力）は、各数字のためのセパレータを意味する。nA1S（即ち、n回指紋Aを連続して入力し、1S（セパレータ）を後続して入力する）は、数字n（n=0, 1, 2, 3, 4, 5）を意味する。nB1S（即ち、n回指紋Bを連続して入力し、1S（セパレータ）を後続して入力する）は、数字n+5、（n=1, 2, 3, 4）を意味する。

この場合、各数字(0, 1, ..., 9)ごとの指紋の入力数を合計して、平均を求める計算によって、1つのセパレータを含む1つの数字を表現するために平均して3.5回の指紋入力が必要である。例えば、暗証番号2570を入力する指紋シーケンス連結は次のようになる。

AASAAAAASBBSS

(3) 指紋による暗証番号の検査結果表示

システムが、指紋による暗証番号の検査結果を表示する場合、次の案がある。案T1：暗証番号を表す指紋シーケンスがすべて入力されてから、結果を表示する。この案では、攻撃者は個別の数字を判定できない。案T2：指紋シーケンスの途中で指紋照合NGとなった場合、システムはすぐに本人確認処理を打切って結果を表示する。この方式では、攻撃者は個別の数字を判定できるので、案T1よりも危険である。従って、案T1を用いるべきである。

4. 提案方法への攻撃に対する安全性

(1) 複数指紋の組合せの全探索攻撃

【攻撃方法】 攻撃者は、攻撃対象とする本人の暗証番号、及び本人の遺留指紋を不正入手し、更に偽造指紋を作成する。偽造指紋を指紋センサから入力することによって、指

紋シーケンスによる暗証番号のすべての組合せを調べる。

【対策】 対策は不要である。理由は、次のとおりである。指紋入力と照合を合わせた時間が1回の攻撃時間になり、すべての組合せについての膨大な回数、反復する必要がある。指紋は指紋センサから入力せねばならないが、人が指紋センサから指紋を連続入力するのは、数時間が限界であるので、提案方法は、十分に安全であると言える。

(2) 傍観者からの攻撃と対策

【攻撃方法】 ユーザが指紋センサから指紋を入力時に、傍観者が指の動作を見て暗証番号を読取る。

【対策】 ユーザは、指紋センサを使用時に指を隠す。又は、指紋センサに接触していないダミー入力を傍観者に分からないように含ませる。

(3) 指紋センサを擬似する攻撃と対策

【攻撃方法】 指紋センサと指紋照合モジュールが分離している場合、攻撃者が指紋センサからの指紋データ等の送信をコンピュータ等で擬似して攻撃する。

【対策】 指紋照合モジュールは、指紋センサの正当性を、暗号により認証する。又は、指紋センサからの同じユーザの指紋照合NGのときの再試行回数に上限を設定する。

5. むすび

本人確認用の指紋の偽造対策は、ネットワーク環境では必須であるが、従来は困難であった。そこで、指紋だけで暗証番号を表現する新しい方法を提案した。提案方法を指紋照合システムに適用すると、攻撃者が指紋を偽造しても、個々の指紋と数字の対応が未知なので偽造指紋を行使できないため、システムのセキュリティを顕著に向上できる。提案方法は、指紋認識アルゴリズムおよび指紋センサとは独立である。提案方法への攻撃と対策を考察し、十分に安全なことを示した。

参考文献

- [1] J. Chirillo and S. Blaul: Implementing Biometric Security, Wiley Publishing Inc., 2003.
- [2] 小林哲二: 細線化画像パターンマッチングによる指紋照合, 電子情報通信学会論文誌, D-2, Vol. J79-D-2, No.3, pp.330-340, 1996.
- [3] T. Kobayashi: A Fingerprint Matching Method for Personal Identification, Proceedings of the IASTED, International Conference on Computer Graphics and Imaging (CGIM2003), ACTA Press, pp.228-231, USA, Aug. 2003.
- [4] 青山奈保子, 遠藤由紀子, 平林昌志, 太田和夫, 松本 勉: 指紋画像からの人工指作製(その3) デジタルカメラを用いた場合, 電子情報通信学会, 2003年暗号と情報セキュリティシンポジウム(SCIS2003), 予稿集, pp.393-398, Jan. 2003.
- [5] 小林哲二: 個人認証用の指紋と暗証番号の入力方法についての検討, 電子情報通信学会, 2003年度総合大会講演論文集, A-7-25, p.198, March 2003.
- [6] 小林哲二: 複数の指紋で暗証番号を表現する個人認証, 情報処理学会, コンピュータセキュリティシンポジウム2003(CSS2003)論文集, pp.175-180, Oct. 2003.
- [7] T. Kobayashi: A Method to Input a Code Number using Fingerprints, Proceedings of the IASTED, International Conference on Communications, Internet, and Information Technology (CIIT2003), ACTA Press, pp.264-269, USA, Nov. 2003.
- [8] T. Kobayashi: A Code Number Input Method using Multiple Fingerprints for Improving the Cell-phone Security, Proceedings of the First International Conference on Mobile Computing and Ubiquitous Networking (ICMU2004), IPSJ, pp. 112-117, Yokosuka, Jan. 2004.