im2017-02　暗号プロトコルに利用できる筆跡データの抽出

佐々木　萌(16RMD13)

セキュリティシステム設計研究室 ［指導：稲村　勝樹　助教］

1. **はじめに**

近年、急速にスマートフォンやタブレットの普及が進み、インターネット上のサービスを利用する際は、個人認証を行うことが増えている。個人認証方式で用いられている要素は大きく分けて3つある。まずパスワードなどの本人の記憶によるもの、次に本人のみが所持している物を用いるもの、そして本人の生体に基づくデータを用いるものがある。その中でも企業Webサイトのおよそ8割がIDとパスワードを用いる認証方式(以下パスワード認証)を用いている。パスワード認証は比較的導入が容易である。しかし、従来のパスワード認証には課題がある。パスワードを設定するのはユーザ自身であるため、ユーザごとのセキュリティ意識に依存しやすく、安易なパスワード設定が起こりやすい。その結果、攻撃者が容易にパスワードを推測することができ、不正ログインに繋がるという課題がある。

こうした課題への対策として、パスワードとパスワード以外の認証情報を併用する二要素認証が提案されている。既存の二要素認証を提案する方式では、パスワードと併用する2つ目の認証情報に生体情報である指紋や静脈,虹彩を用いている。しかし、これらは専用のデバイスが必要であるため、全ての端末で認証に利用することができない。一方、タッチパネルはスマートフォンやタブレット端末などに埋め込まれている。そこで今回はタッチパネルを利用し、筆跡情報を二要素目の認証情報とする。

従来の筆跡情報を用いる認証方式２)は事前に登録済みの筆跡データと認証時に入力する筆跡データの類似度を測ることによって認証を行うものであった。この場合、筆跡データから固定値を抽出することは出来ず、認証で用いる鍵のような他の認証方式には適用しにくい。

したがって本研究では、文字から固定値に変換することができる筆跡特徴点を提案し、固定値への変換の有用性を評価する。筆跡を採取するアプリを作成し、その採取した筆跡データから得られる特徴点の提案およびその特徴点から生成される固定値の有用性を評価する。

1. **既存研究**

本研究では、稲村氏が提案しているCHAPを拡張せず多要素認証を実現するプロトコルへの導入を前提としており、それを以下に示す。

まず、CHAPとはパスワードを用いたチャレンジ・レスポンス型認証方式の一つである。低負担かつ安全に行うことができるという特徴から、PPP(Point-to-Point Protocol) [2] のユーザ認証用など幅広く使われている。この通信パケットを拡張することなく2種類以上の認証情報を送ることが可能となるプロトコルへ導入することとした。

1. **研究目的**
2. **提案内容**

生体認証情報による認証は、ユーザ自身が認証情報になるため、何かを持ち運ぶ等の負担がない。その中でも行動的特徴による認証は、日常生活上の行動に近いため、認証に対する抵抗感が少ないと考えられる。また、万が一認証情報が漏洩した場合、認証情報を簡単に変更する事が出来る。以上の利点から、パスワードと併用する認証情報として筆跡情報を用いる。

これまでの筆跡情報を用いた認証2)は、事前に登録してある筆跡データと採取した筆跡データの類似度による認証であった。しかし、本研究では、固定値の認証情報としてパスワードと併用することを目指す。したがって、ユーザがタッチパネル上に指で書いた文字の特徴差から固定値への変換の可能性を評価した。

1. **対象とする筆跡データ**

筆跡に個人差が生まれるのは、個人毎の習得している書写技能に差があるためであると考えられる。3)ゆえに、書写技能3)に基づいて特徴点を抽出する必要がある。

本研究では、タッチパネルに書いた文字のデータから読み取る事が出来る特徴点により評価を行うため、書写技能のうち造形法を利用した。造形法とは、点画がどのように組み合わされて文字が構成されているのかというものである。また、造形法の中でも特徴差をビット情報に変換しやすいと考えられる、「画の交わり方」を筆跡特徴点の基準に利用した。

画の交わり方を基準に、以下3つの筆跡特徴点を定めた。1)画が交差しない部分で交差するか2)本来2つの画が接している部分で片方の画が突出しているか3) 本来2つの画が接している部分で画が離れているか

基準1)を図1、基準2)を図2、基準3)を図3に示す。

図 2.画の突出

図 1.画の交差

1. **実験と評価**

今回の実験は、Androidで筆跡を画像で保存するアプリを作成し、直線的な画が多いという理由から、大文字のアルファベットおよび片仮名のデータを22人の被験者から採取した。そのアプリから文字入力により得られた文字に対して、3つの評価基準により固定値への変換の可能性を評価した。

評価結果として、2通り以上のビット列を生成することが出来るアルファベットを表1に、片仮名を表2に示す。表における合計とは、特徴点の数から、1文字あたりに表現出来るビット列の場合の数である。「A」を例に挙げると、特徴点の合計が6つであるため、26=64通りとなる。

また、背景が黄緑色の文字は、文字の形の個人差が顕著であった文字である。また、場合の数の平均を比較したところ、片仮名よりアルファベットの方がより多くの筆跡特徴を抽出することが出来ると分かった。さらに、片仮名およびアルファベットともに、評価基準の合計の平均値を比較したところ、画の交差＜画の突出＜画の離れ　となった。

評価基準を比較した際、評価基準3の画の離れが突出して平均値が高かった。その一因として、文字を書く線の太さや指で書くということが挙げられる。

表 1.アルファベット評価結果

表 2.片仮名評価結果

1. **まとめ**

本研究では、タブレット上に指で書いた文字から筆跡特徴点を提案し、そこから固定値への変換の可能性を評価した。結果として、今後改良の余地はあるが、筆跡の特徴差から変換したビット情報が認証情報として有効であることが分かった。

今後の課題として、描く線の太さの違いを考慮すること、文字の形の個人差の固定値への変換の可能性を検討すること等が挙げられる。

**参考文献**

1. 独立行政法人情報処理推進機構:情報セキュリティ10大脅威 2017, 2017
2. ウィッツェル株式会社:セキュリティ/サイン認証/サイバーサイン,

http://www.witswell.co.jp/cybersign/ (参照 2015-8-8)

1. 情報処理振興事業協会セキュリティセンター:本人認証技術の現状に関する調査報告書,2002