3U−2

臨床症例データベースシステムにおけるセキュリティの強化
— 自己組織化マップを用いた打鍵リズム付き暗証番号による個人認証 —

山口 俊光† 納富 一宏† 石井 博章†† 斎藤 恵一‡ 藤本 哲男‡‡

†神奈川工科大学情報工学科
††神奈川工科大学福祉システム工学科
‡東亜大学経営学部経営学科
‡‡芝浦工業大学工学部機械工学科

1 はじめに

臨床症例のような医療情報の中には病歴など, 患者の個人情報を含むものがあるので, ネットワークを介し情報を共有するためには, 不特定多数の人間がアクセスできないよう個人認証が必要となる.

簡易な個人認証手法として数桁の暗証番号を用いた方法は広く普及している. しかしながら, 暗証番号による個人認証は桁数が少なく安全性が高いとは言い難い.

この暗証番号による個人認証を強化する手法として, 指紋や虹彩等を認証に用いるバイオメトリクス認証が広く知られている. しかしながら, バイオメトリクス認証では専用のハードウェアを用意しなければならない.

本稿では専用ハードウェアを用いずに, 自己組織化マップによるクラスタリングを行うことで, 暗証番号を入力する際の入力タイミング (打鍵リズム) から個人の癖に関する情報を取得し, これを個人認証に利用する手法について提案する.

2 システム構成

2.1 自己組織化マップを用いた個人認証

自己組織化マップ (Self-Organizing Maps) は,T.Kohonen により提案された教師なし競合学習型ニューラルネットワークであり, 入力層と出力層の 2 層からなる. データ間の特徴類似度による汎用的なクラスタリング能力を持つ. 入力タイミングの癖を分類するのに SOM のアルゴリズムを適用する.

暗証番号を入力する際のキー入力タイミングを SOM の入力ベクトルとして用いる. 入力ベクトルを用いて学習したマップ上に配置された同一 $userID$ の点の座標 s_i と, 新たに入力されてきたベクトルの座標 s の間のユークリッド距離 d をそれぞれ求め, その平均をとる. ユーザ ID $userID$ の学習により配置された点の個数が n 個である場合の距離関数 $d_{userID}(s)$ は次式で定義される.

$$d_{userID}(s) = \frac{1}{n}\sum_{i=1}^{n}\|s - s_i\| \qquad (1)$$

この距離関数により求められた値が閾値を越えなければ, 認証に成功したものとみなす.

2.2 打鍵リズム付き暗証番号

SOM 学習のための入力ベクトル $\boldsymbol{x}$ は 13 の属性からなる. 入力ベクトルの例を Fig.1 に示す.

0.187 0.181 0.166 0.181 0.063 0.156 0.222 0.207	0.07 0.077 0.075 0.084 0.089 0.096 0.185 0.116 0.083 0.116	0.117 0.104 0.091 0.097 -0.033 -0.029 0.106 0.124
Press-Press Time	*Press Time*	*Release Time*

Fig. 1: Input Vector

Press-Press Time はあるキーが押されてから次のキーが押されるまでの時間を示している. Press Time はキーが押されている時間を示している. Release Time はキーが離されてから次のキーが押されるまでの何も押されていない時間を示している.

入力ベクトルに負の属性値が含まれているものがある. これは,Fig.2 のような打鍵の違いがあるからである. α_p,β_p はキーを押したタイミング,α_r,β_r はキーを離したタイミングである.

Duplex Stroke は α_r でキーを離す前に β_p でキーを押している. そのため, ベクトルに負の属性値が含まれる.

2.3 実装システム概要

本システムの構成を Fig.3 に示す. 大まかな構成はサーバ/クライアントで構成される 2 層モデルをとっている. クライアントは, 認証に必要な ID と暗証番号, そしてキー入力のリズム情報をサーバに送信する. サーバでは,ID と暗証番号による通常の認証をおこな

Strengthening of the security in DBMS for Clinical Cases : Personal Authentication by 4 figure PIN with keystroke rhythm on Self-Organizing Maps

Toshimitsu YAMAGUCHI† Kazuhiro NOTOMI† Hiroaki ISHII†† Keiichi SAITO‡ Tetsuo FUJIMOTO‡‡
†Department of Information and Computer Science, Kanagawa Institute of Technology
††Department of Welfare Systems Engineering, Kanagawa Institute of Technology
‡Department of Business Management, Faculty of Business Management, University of East Asia
‡‡Department of Mechanical Engineering, Shibaura Institute of Technology
e-mail: mit@ish.ic.kanagawa-it.ac.jp

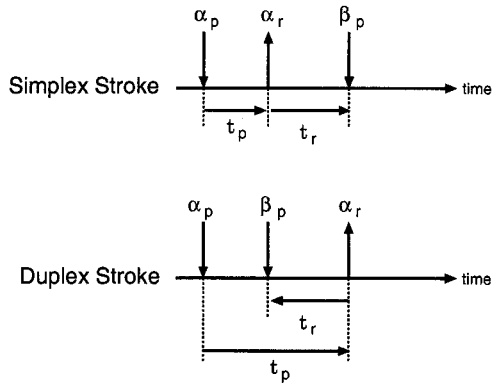

Fig. 2: Keystroke Timing Pattern

う．その後,ID とキー入力のリズムを用いた自己組織化マップによる認証を行う．この 2 つの認証に成功すると, 認証成功となる．

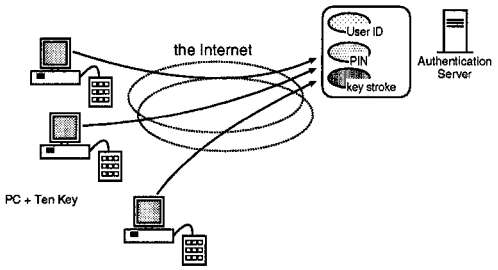

Fig. 3: System Structure

3 評価

3.1 評価方法

被験者 7 人を対象に認証実験をおこなった．同じ暗証番号の打鍵タイミングをマップ作成用に 8 回, 試行用に 40 回計測し, 打鍵リズム付き暗証番号を用意した．計測には SunMicrosystems 社製ワークステーションに付属する Type6 キーボードのテンキーを使用した．

マップ作成用入力を 2000 回学習させてマップを作る．生成するマップサイズは 50×50 ノードである．そのマップに対して, 試行用入力をマッピングし, マップ作成用入力 8 点からのユークリッド距離を計算し, その平均を求める．この値が, 閾値より小さければ「受容」とし, 閾値以上であれば「拒否」として閾値ごとの FRR(False Reject Rate:本人拒否率) および FAR(False Accept Rate:他人受容率) を計算した．FAR, FRR の定義式を以下に示す．

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}} \quad (2)$$

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}} \quad (3)$$

3.2 評価結果

評価結果を Fig.4 に示す．値は試行用リズム付き暗証番号 40 回分の FAR,FRR を 7 人分求め, それを平均したものである．

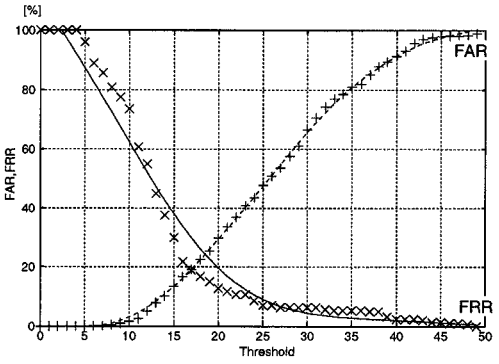

Fig. 4: FAR and FRR

暗証番号が他人に盗まれた場合, 通常の暗証番号のみで行う認証方式では FRR は 0%に近いが,FAR は 100%になってしまう．本システムを用い閾値を 15〜20 を設定することで,FAR,FRR をともに,25%以下に抑えることが可能になった．

4 まとめ

自己組織化マップを用いた打鍵リズム付き暗証番号による個人認証について述べた．今後は FAR,FRR の低下をはかり, 信頼性の向上を目指す．

参考文献

[1] 山口, 納富, 他：WWW による臨床症例検索システムの開発 — 自己組織化マップを用いた打鍵タイミングによる個人認証 (2000), 情報処理学会第 61 回全国大会講演論文集、4R-4.

[2] 山口, 納富, 他：臨床症例検索データベースの構築 — 自己組織化マップを用いた打鍵タイミングによる個人認証の改良 (2001), 情報処理学会第 62 回全国大会講演論文集、6Q-2.

[3] T.Kohonen, : 自己組織化マップ, シュプリンガー・フェアクラーク東京 (1996), 徳高平蔵 他 訳.