4R-04

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 —

山口 俊光† 納富 一宏† 岡本 雅幸† 石井 博章† 斎藤 恵一‡ 藤本 哲男‡‡

†神奈川工科大学情報工学科
‡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

臨床症例文書を共有することは、新たな症例の病態を検討・類推する上で非常に重要である。医療情報の中には病歴などの患者の個人情報を含むものがあるので、情報共有にWWWを用いる場合、パスワードのみの認証では安全性が十分とは言い難い。

パスワードのみで行なう個人認証ではパスワードが盗まれた場合、正規ユーザ以外の人間に正規ユーザとしてシステムに侵入されてしまう危険性が非常に高くなる。

このパスワードのみで行なう認証の弱点を補うため提案がなされている。バイオメトリクス認証という生体測定学を認証に応用したものもその1つである。バイオメトリクス認証の方法としては、指紋や網膜によって個人認証を行なうものがよく知られている [1]。しかしながら、これらの個人認証手段を実際に利用するためには専用のハードウェアを各ユーザが用意しなくてはならない。

そこで、本稿ではパスワードを入力する際の打鍵タイミングを測定し、そのタイミングをもとに自己組織化マップを用いて個人認証を行う方法について述べる。

2 システムの構成

2.1 WWWの利用

インターネット上の代表的なサービスであるWWWを利用することは、臨床症例データベースの検索・登録において全国的な地域をカバーするのに非常に有利である。また、WWWブラウザをクライアントとして用いるため、ユーザはソフトウェアを新規にインストールする必要がない。本システム全体の構成図をFig.1に示す。

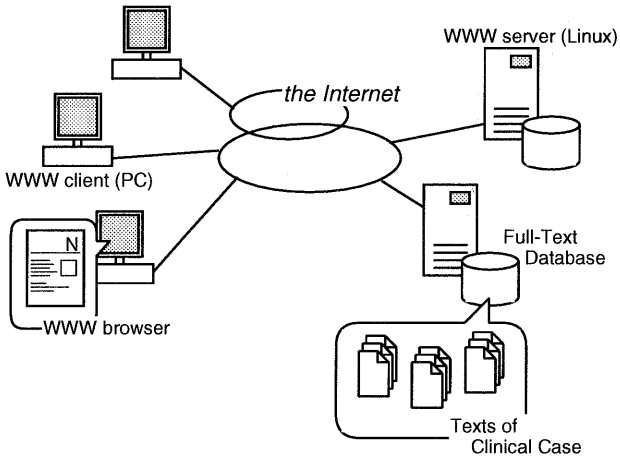

Fig. 1: System Structure

2.2 自己組織化マップを用いた個人認証

本認証システムはJavaアプレットとして実装した。まずユーザ登録の際にキータイプのタイミングを計測し、その値で自己組織化マップを作成する。タイミングの測定は1ミリ秒単位で行われる。システムにログインするときも同じようにキータイプのタイミングを測定する。入力された文字列が正しいかどうかを確認し、パスワードを入力した際のキータイプのタイミングを入力ベクトルとして、自己組織化マップ上にマッピングする (Fig.2)。マップ作成時に用いた入力の位置と新たな入力の位置のユークリッド距離をもとめ、閾値より小さければログインを許可し、閾値以上であればパスワードの文字列が正確に入力されていてもログインを拒否する。

Development of DBMS for Clinical Cases on WWW : Personal Authentication with Keystoroke Timing Pattern on Self-Organizing Maps

Toshimitsu YAMAGUCHI† Kazuhiro NOTOMI† Noriyuki OKAMOTO† Hiroaki ISHII† Keiichi SAITO‡ Tetsuo FUJIMOTO‡‡

†Department of Information and Computer Science, 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

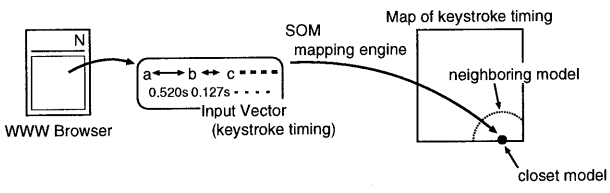

Fig. 2: SOM based Personal Authentication System

3 自己組織化マップ

自己組織化マップはコホーネン(Kohonen)によって提案された競合学習型ベクトル量子化ニューラルネットワークである。

ニューロンは層状をなし、入力データは各ニューロンに並列的に伝達される。入力データ $\boldsymbol{x}_i$ が投入されると各ニューロンは次式により内部ポテンシャル net_i^j を計算する [2]。

$$net_i^j = \frac{1}{D(\boldsymbol{w}_i, \boldsymbol{x}_j)} \tag{1}$$

ここで、$\boldsymbol{w}_i = (w_{i1}, w_{i2}, w_{i3}, ..., w_{in})$ は各ニューロンの結合重みベクトルである。D は入力と結合重みベクトルとの相違を示す距離関数であり、ユークリッド距離が一般的に用いられている。

$$D(\boldsymbol{w}_i, \boldsymbol{x}_j) = |\boldsymbol{w}_i - \boldsymbol{x}_j| \tag{2}$$

この式により最大の内部ポテンシャルを示す結合重みベクトルが競合に勝ち残ったニューロンとなる。そのニューロンの近傍のニューロンを巻き込みながら、次式に示すコホーネンの学習則にしたがって結合重みベクトルの修正を行なう。

$$\boldsymbol{w}_k^{new} = \boldsymbol{w}_k^{old} + \alpha(\boldsymbol{x}_j - \boldsymbol{w}_k^{old}) \tag{3}$$

α は学習係数と呼ばれる値で、学習回数 t の関数で表される。本システムは 2000 回の学習によって生成されたマップを用いて認証を行っている。

4 評価

4.1 評価方法

同じパスワードの打鍵タイミングをマップ作成用に 4 回、試行用に 30 回計測した。実験は、「5 分間タイプ練習」、「3 分間休憩」、「計測」の順で行った。マップ作成用の入力を 2000 回学習させマップを作る。そのマップに対し試行用の入力をマッピングしマップ作成用入力 4 点からのユークリッド距離をそれぞれ測定し平均値を求める。その平均が 0 から 60 まで 5 きざみの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。

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}} \tag{4}$$

$$FRR = \frac{\text{本人拒否回数}}{\text{試行回数}} \tag{5}$$

4.2 評価結果

実験結果を Fig.3 に示す。値は 30 試行分の FAR、FRR の平均を 10 人分求め、それを平均したものである。

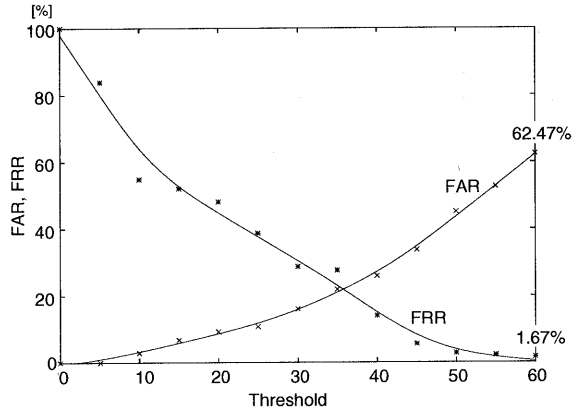

Fig. 3: FAR and FRR (Average)

パスワードが盗まれてしまった場合、通常のパスワードのみの認証方式では FRR は 0%に近いが、FAR は 100%になってしまう。本システムを用いることにより FRR が 0%近くになる閾値 60 の場合でも FAR を 60%程度に抑えることが可能になった。

5 まとめ

自己組織化マップを用いた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している。

参考文献

[1] Simson Garfinkel, G. S.: UNIX & インターネットセキュリティ, O'REILLY (1998), 山口 英 監訳、 谷口 功 訳.

[2] 臼井支郎, 他：基礎と実践 ニューラルネットワーク, 第 7 章, コロナ社 (1995).