

ライフスタイル認証におけるゆらぎ吸収を目的とした テンプレート更新手法の提案

小林 良輔¹ 山口 利恵¹

概要: 近年、ライフスタイル認証といった技術が提案され、ライフスタイルには個人性を持つことがわかっている。ライフスタイル認証ではあらかじめライフログから個人性を抜き出したテンプレートが登録されるが、一般的に人間のライフスタイルは変化していくものである。そのため、このテンプレートはライフスタイルの変化にあわせて更新する必要があるが、ライフスタイル認証のテンプレート更新に関する既存研究は存在しない。本論文ではライフスタイルが変化するいくつかのケースに応じたテンプレート更新手法を提案し、その中でライフスタイルのゆらぎに対応したケースについて実験を行った。

キーワード: ライフスタイル認証, テンプレート更新, ゆらぎ, 行動認証, Wi-Fi

Template Update Technique Adapting to Lifestyle Fluctuation for Authentication and Its Application to Wi-Fi Authentication

RYOSUKE KOBAYASHI¹ RIE SHIGETOMI YAMAGUCHI¹

Abstract: Lifestyle authentication has been proposed, and it is known that lifestyle habits of people have their characteristics. In the authentication methods, a template is registered which is created by extracting user's characteristics from lifelogs in advance. However, lifestyle of people will generally change. The template is necessary to be updated with the change of lifestyle, and there have been no studies on template update techniques in lifestyle authentication. In this paper, we propose template update techniques on the variety cases in lifestyle authentication. We conduct an experiment of one case utilizing Wi-Fi information, and confirm the effectiveness of template updating.

Keywords: lifestyle authentication, template update, fluctuation, behavior authentication, Wi-Fi

1. はじめに

近年、ライフスタイル認証という新しい個人認証技術が提案されている。ライフスタイル認証は人間の行動パターンから得られる個人特性を利用する手法である。この行動パターンは生活習慣を記録したライフログから観察することができ、IoT時代となった昨今、ライフログはスマートフォンやウェアラブル端末により容易に収集することができる。実際に既存研究にはスマートフォンを利用したライフスタイル認証手法の提案がいくつか存在している。例え

ば、スマートフォンセンサーが取得したGPS情報を利用した研究 [1] や、Wi-Fi 情報を利用した研究 [2] などがある。これらの論文からGPS情報を利用した実験 [1] では95%程度の認証精度が出ており、Wi-Fi 情報を利用した実験 [2] では90%以上の認証精度が出ていることがわかる。このことから、人々のライフスタイルは個人特性を持つことがわかり、認証要素となりうるものである。

しかしながら、人間のライフスタイルは一般的に変化していくものである。引越しをすれば行動範囲は変わるであろうし、転職をすれば生活リズムも変わるかもしれない。そのため、ライフスタイル認証はいつまでも有効的に利用できるものとは言えない。ライフスタイル認証は人間の行

¹ 東京大学
The University of Tokyo

動パターンの特徴が、日々同じもしくは似ているという事柄を利用したのだからである。ライフスタイルが変化すると、ライフスタイル認証の精度は下がっていく。ライフスタイル認証を有用なものにするには、ライフスタイルの変化に対応していくことが求められる。

ライフスタイル認証システムでは、登録モードと検証モードの二つのモードが存在している。登録モードでは、テンプレートと呼ばれる、ライフスタイル情報からユーザーの個人特性を抜き出したデータがシステムに登録される。そして検証モードでは、入力されるライフスタイル情報と登録モードで登録されたテンプレートを比較し、入力された情報が登録されたテンプレート本人と同じかどうかを照合する、といった仕組みである。検証モードで入力されるライフスタイル情報は日々の生活行動の結果であり、行動パターンの変化にあわせて変わっていくものである。そのためライフスタイル認証がライフスタイルの変化に対応していくためには、検証前に登録されるテンプレートを行動パターンの変化にあわせて更新していかなければならない。

ライフスタイル認証においてテンプレート更新に関する既存研究は存在しないが、生体認証においてはいくつかの研究が行われている。生体情報は人間の行動パターンのように必ず変化するものではないが、センサーの精度であったり、環境条件、傷の有無や経年変化によって入力情報が登録時と変わることがある。そのため生体認証においてもテンプレート更新は必要な技術となっているのである。

本論文では、検証モードで入力するライフスタイル情報が変化するケースを考え、それぞれのケースについてのテンプレート更新手法を提案する。また、そのうちの一つのケースについて実験を行い、ライフスタイル認証におけるテンプレート更新の有用性について確認する。実験についてはライフスタイル認証の認証要素としてWi-Fi情報を利用した。本論文の構成は以下の通りとなっている。2章では、生体認証におけるテンプレート更新技術の既存研究について紹介する。3章では、ライフスタイル情報が変化する四つのケースについて紹介し、それぞれのケースについてテンプレート更新手法を提案する。4章では、本研究の実験で利用したWi-Fi認証手法の概要について説明する。5章では、ライフスタイル情報が変化する一つのケースについてWi-Fi情報を利用して実験を行い、テンプレート更新の有用性を確認する。6章では、テンプレートを更新するシステムについて説明する。最後に7章で結論を述べる。

2. 生体認証におけるテンプレート更新

生体認証とは人間の生体的特徴を利用する認証手法である。この生体的特徴は個人ごとに異なっており、基本的には生涯変わらないものである。そのため、テンプレートと呼ばれる生体情報をあらかじめ登録しておき、認証時に再

度生体情報を入力してテンプレートと同じかどうか照合するといった認証手法が可能となる。しかしながら、実際には入力された生体情報がいつも完全に同じものとは限らない。生体情報を読み取る端末の劣化であったり、入力環境の変化や、例えば指を傷つけたなどの要因での生体的特徴そのものの変化などで、入力情報は時間とともに変化する。これらの経年変化によりテンプレートが個人を特徴づける情報から遠ざかっていき、認証精度の低下をもたらす要因となる。

この問題を解決するためには、入力される生体情報の変化とともに、テンプレートを更新していく必要がある。テンプレートを登録時のままとしておくと、テンプレートと認証時に入力される生体情報の特徴が一致なくなっていくが、テンプレートを更新することによって両者の特徴量を離さないようにするのである。

生体認証におけるテンプレート更新手法についてはこれまでいくつか研究されており、本章では既存手法について紹介していく。

2.1 テンプレート選択

システムによってはユーザーごとに複数のテンプレートが登録されているケースがある。そのため、テンプレート更新時に対象のテンプレートを選択する必要がある。選択手法についての研究がされている。この手法ではシステム稼働時に入力される情報を一定期間収集されたのちに、バッチ処理にて行われる。収集された対象不明の情報は、クラスタリング手法 [3] や編集手法 [4] によりクラス分類され、対象のテンプレートが選択される。

2.2 自動更新

この更新手法は、登録済みのテンプレートに非常に本人らしい入力情報を加えてテンプレートを更新する手法である。非常に本人らしい入力情報とは、テンプレートとの一致率が更新実行閾値を超えた情報のことである。この手法では、認証時に入力された認証情報をテンプレート更新の素材とし、テンプレートを自動的に更新していく手法である。この手法はさらに、オンライン更新 [5][6][7] とバッチ更新 [8] の2つが提案されている。オンライン更新手法では、テンプレート更新は認証と同じタイミングに行われ、認証情報入力後すぐにテンプレートが更新される。一方でオフライン更新手法では入力された認証情報がある程度データベースにためられ、一度にバッチ処理にてテンプレート更新が行われる。オンライン更新手法では情報が入力されるたびにテンプレートが更新されるため、入力される順序によってテンプレートとの一致率が変化し、順序が更新結果に影響をもたらすこととなる [6]。

2.3 行動認証への活用

テンプレート更新手法は生体認証だけではなく、意識的な行動を利用した行動認証（ライフスタイル認証ではない）にも活用されているのでここで紹介する。端末の動きを用いた認証手法 [9] や腕の振りを利用した認証手法 [10] にもテンプレート更新は活用されている。このようにテンプレート更新手法は人の動きを利用した認証手法にも活用できることがわかり、ライフスタイル認証にも活用されることが期待される。

3. テンプレート更新手法

ライフスタイル認証では認証時に入力する情報が、入力するたびに移り変わっていく可能性がある。入力する認証情報が変わる一方でテンプレートが登録時から変わらないとすると、認証精度は徐々に下がっていくこととなる。認証精度を保つためには、認証情報の変化に伴い、テンプレートを更新していく必要がある。本章ではライフスタイル認証において入力情報が異なるケースを考え、ケースに応じたテンプレート更新手法を提案する。

3.1 ユースケース

本節ではライフスタイル認証において、入力する認証情報が変わるケースについて説明する。認証情報が変わるケースを以下の3ケースに分けて考える。

- 行動のゆらぎ
行動情報の特徴として、人は常に同じ動きをとるとは限らず、行動情報にはゆらぎが含まれている。ライフスタイルにおいてもそれは同じであり、人は習慣化されたリズムで日々生活を送っているが、その情報はまったく同じになるとは言えない。例えば、毎朝同じ時間の電車に乗っている人がいたとしても、ある日電車が遅れて乗る時間が遅くなるかもしれないし、道路混雑等でいつもの電車に乗り遅れるかもしれない。このように、何らかの要因で人間の行動は似ているかもしれないが、まったく同じとはならず、そのため認証情報も変化して入力されることとなる。
- ライフスタイルの変化
人間のライフスタイルは時が来れば大きく変化することがある。例えば就職や引っ越しなどが大きくライフスタイルが変化するタイミングである。自宅の近所で買い物をする人は引っ越しをすると、普段行く店も変わってくる。また職場等への交通手段も変わってくるだろうし、起床や就寝の時間も変わるかもしれない。このようにライフスタイルが大きく変化するタイミングがあり、この時、認証情報はこれまでと大きく変わることとなる。
- 複数のライフスタイル
現在のライフスタイルを残しつつ、別の生活パターン

が新たに増えることがある。例えば、一時的な長期出張などである。出張中はこれまでとは違った生活パターンとなるが、出張が終われば元と同じライフサイクルとなるし、平日は出張先での生活で、休日は家に戻りこれまでと同じ生活パターンとなるケースも考えられる。出張に限らず、曜日で生活パターンが異なるのはこのケースにあたる。このように複数の生活パターンを持ち、それに伴いライフスタイル認証における認証情報も複数パターン存在するケースがある。

3.2 ケースに応じた更新手法

本節では節で述べられたケースについて、それぞれに応じたテンプレートの更新手法を提案する。なお、人間のライフスタイルは [11] によると、一日周期のリズム現象であり、一日単位で行動パターンが繰り返される。そのため本論文でのライフスタイル認証は一日単位でデータを扱うことを前提とする。また、テンプレート更新手法提案の前に以下を定義する。

N_d : ある日 d に入力された認証情報

T_{d-1} : ある日 d に使用されるテンプレート

T'_{d-1} : T_{d-1} の特徴抽出前情報

$E(T'_d)$: 特徴抽出関数

一般的に個人認証を行う際は、入力情報に対し特徴抽出を行い認証処理に用いる。ここでは特徴抽出処理を $E()$ で表し、 $T_d = E(T'_d)$ の関係があるとしている。この定義に対して、次にテンプレート更新処理について説明する。

3.2.1 行動のゆらぎ

ある日 d のテンプレート T_{d-1} を更新して次の日のテンプレート T_d を作成することを考える。 T_{d-1} と d 日目の入力情報である N_d を作用させて次のように T_d を定義する。

$$T'_d = (1 - \alpha(d)) T'_{d-1} + \alpha(d) N_d \quad (1)$$

$$T'_1 = N_1, d \in \mathcal{N}$$

ここで $\alpha(d)$ は任意の d で $0 \leq \alpha(d) \leq 1$ を満たす、 d に依存する数とする。例えば $\alpha(d) = \frac{1}{2}$ とすると T'_d は T'_{d-1} と N_d の単純平均となるし、 $\alpha(d) = \frac{2}{d+1}$ とすると、(1) 式は以下で表される。

$$\begin{aligned} T'_d &= \frac{N_1 + 2N_2 + \dots + dN_d}{1 + 2 + \dots + d} \\ &= \frac{\sum_{n=1}^d nN_n}{\sum_{n=1}^d n} \end{aligned}$$

このケースの更新手法は、2.2 節で説明されたオンライン更新手法と同様の手法である。

3.2.2 ライフスタイルの変化

ライフスタイルが完全に変わった場合は、変化する前のテンプレート情報はユーザー本人の特性を表したデータで

はなくなる。そのためこのケースでのテンプレート更新は T_{d-1} を用いずに T_d を表すのがよい。すなわち、

$$T'_d = N_d \quad (2)$$

と表す。(2) 式は、(1) 式で $\alpha(d) = 1$ としたものであり 1 つの式に整理することができる。しかしケースとして、行動情報のゆらぎなのかライフスタイルの変化なのかはシステムが自動的に判断できないため、ユーザーからの指示が必要となる。

3.2.3 複数のライフスタイル

元のライフスタイルを保持したまま、新たに別のライフスタイルで生活を行うケースについて考える。例えば、曜日によって勤務先が変わるケースや、長期出張で出張から戻れば元のライフスタイルに戻るが出張中は別のライフスタイルになる、といったケースである。このケースでは元のライフスタイルを表したテンプレートを更新していくと、複数のライフスタイルの情報が取り込まれたテンプレートとなり、認証精度が低下していく恐れがある。そのため、元のテンプレートには更新を行わず保持したまま、新たにテンプレートを作成してそのテンプレートに対して日々更新処理を行っていくべきである。

このケースの更新手法は、2.1 節で説明された手法と同様の手法である。また、ライフスタイルの変化と同様、複数のライフスタイルのケースもユーザーからの指示があつて初めて、システムがケース判断をすることができる。

4. Wi-Fi 認証

本章では実験で利用したライフスタイル認証の一つである、Wi-Fi 認証の手法について説明する。この手法では、スマートフォンセンサーで取得される Wi-Fi 情報を活用する。取得される Wi-Fi 情報には、無線 LAN アクセスポイントの端末情報である、SSID(Service Set Identifiers) や BSSID(Basic Service Set Identifiers) が含まれており、本手法では BSSID を利用した。

4.1 行動情報の特徴

人間の日々の行動習慣は、似る傾向にはあるが、いつも同じとは限らずゆらぎが存在するものである。そのため、ライフスタイル認証のように行動情報を利用した認証手法は、人間の行動のゆらぎを考慮し、この行動のゆらぎを吸収できるようにデータ処理をしなければならない。Wi-Fi 認証ではスマートフォンが取得した無線 LAN 端末の BSSID と、その ID を取得した時間を認証情報として利用するが、行動のゆらぎはこの BSSID と取得時間に反映される。つまり、BSSID のゆらぎとは、人間は毎日同じ場所に訪れるとは限らないことを意味しており、時間のゆらぎとは、人間は毎日同じ時間に行動をするとは限らないことを意味する。Wi-Fi 認証ではこの BSSID のゆらぎと時間のゆらぎ

が存在することを考慮し、吸収するよう処理を行う必要がある。なお、本論文ではスマートフォンが取得する BSSID を単にアドレスと呼ぶこととする。

4.2 データ形式

本節では Wi-Fi 認証で利用する、スマートフォンセンサーが取得するアドレスと取得時間を扱う際の、データ形式について説明する。3.2 節でも述べた通り、本実験での Wi-Fi 認証も一日単位でデータを扱うこととする。Wi-Fi 認証で扱う一日分のアドレスと取得時間の関係を行列を用いて表現することとし、用いる行列は次の通り定義する。

行列 M_x の集合を \mathbb{M} とし、 \mathbb{t} を一日を 24 時間に分けた時の一時間単位 $\{0, 1, \dots, 23\}$ の集合、 x をアドレス $\{x_1, x_2, \dots, x_n\}$ の集合、 $c(t_i, x_j)$ を $t_i \in \mathbb{t}$ と $x_j \in x$ に関する関数とする。また、 $c(x_j) = [c(0, x_j) \ c(1, x_j) \ \dots \ c(23, x_j)]^T$ とする。このとき、行列 M_x を以下の通り定義する。

$$M_x = \begin{bmatrix} c(x_1) & c(x_2) & \dots & c(x_j) & \dots & c(x_n) \end{bmatrix}$$

Wi-Fi 認証で利用するデータは上で定義した M_x の形式で表される。ここで時間情報を一時間単位としているのは、時間のゆらぎを吸収するためである。一時間単位でデータを扱うことで、Wi-Fi をキャッチした時間が多少ずれていても同じデータとして扱うことが可能となる。

また、行列 M_x の操作として以下を定義する。

$$X_x, Y_y, Z_z \in \mathbb{M}$$

$$\begin{aligned} X_x &= \begin{bmatrix} c_1(x_1) & c_1(x_2) & \dots & c_1(x_l) \end{bmatrix} \\ Y_y &= \begin{bmatrix} c_2(y_1) & c_2(y_2) & \dots & c_2(y_m) \end{bmatrix} \\ Z_z &= X_x + Y_y \\ &= \begin{bmatrix} c_3(z_1) & c_3(z_2) & \dots & c_3(z_n) \end{bmatrix} \end{aligned}$$

としたとき、

$$z = x \cup y$$

$$c_3(z_i) = \begin{cases} c_1(z_i) + c_2(z_i) & (\text{if } z_i \in (x \cap y)) \\ c_1(z_i) & (\text{else if } z_i \in x) \\ c_2(z_i) & (\text{else if } z_i \in y) \end{cases}$$

と定義する。

4.3 データタイプ

1 章で述べた通り、ライフスタイル認証システムは登録モードと検証モードからなる。登録モードではテンプレートの登録が行われ、検証モードでは入力された認証情報とテンプレートの比較が行われる。Wi-Fi 認証で扱うデータ種類はテンプレートと認証情報、また比較結果が存在し、テンプレートを T 、認証情報を N 、比較結果を R とすると、 $T, N, R \in \mathbb{M}$ である。

4.4 データ処理

本節ではスマートフォンが取得したデータを Wi-Fi 認証で扱う形式に変換する処理について説明する。

4.4.1 認証情報

ある日にスマートフォンセンサーが取得したアドレスの集合を $\alpha = \{a_1, a_2, \dots, a_n\}$ とし, t_i 時から $t_i + 1$ 時の間にアドレス a_j を取得した場合, $c(t_i, x_j) = 1$, 取得しなかった場合, $c(t_i, x_j) = 0$ とする. このとき認証情報 N_α を,

$$N_\alpha = \begin{bmatrix} c(a_1) & c(a_2) & \dots & c(a_n) \end{bmatrix} \in \mathbb{M}$$

とする.

4.4.2 テンプレート

4.4.1 節で述べた認証情報と, 3.2.1 節で述べた処理を用いて Wi-Fi 認証における特徴抽出前のテンプレートを作成することができる. 本節では Wi-Fi 認証におけるテンプレートを作成するための特徴抽出処理について説明する.

• アドレス選定

Wi-Fi 認証における特徴抽出前テンプレートは, 更新処理を行うごとにスマートフォンが取得するアドレスの数が増えていくことになる. このアドレス情報はユーザーの特性を表す一方で, アドレスの中にはほとんど特性を表さないものも存在する. ユーザーの自宅やよく行く場所に設置されている端末のアドレスであればユーザーの特性を表すものとなるが, 街中ですれ違った人が持っていた無線 LAN 端末のアドレスだとユーザーの特性を表すものとはならない. このようなユーザー特性を持たないアドレスがテンプレートの情報に含まれていると, 認証精度を下げる要因になってしまう. そのためテンプレートを作成するためにはユーザー特性を持たないアドレスを切り捨て, ユーザー特性を持つアドレスを抽出する必要がある.

• 二値化

Wi-Fi 認証における特徴抽出前テンプレートは, 更新処理を行うごとに値が徐々に小さくなっていくことが多い. ユーザー特性を持った情報が, 値が小さくなることで, その特性が薄れていく恐れがある. テンプレートからユーザー特性が薄れると, 認証精度を下げる要因になってしまう. そのためユーザー特性を持った情報は値を大きく, 逆に特性を持たない情報は値を切り捨てられるよう, 二値化処理を行う. 二値化パラメータを b としたとき, 以下の変換処理を行う.

$$c(t_i, x_j) = \begin{cases} 1 & (\text{if } c(t_i, x_j) > b) \\ 0 & (\text{otherwise}) \end{cases}$$

アドレス選定処理を $S()$, 二値化処理を $B()$ とすると, 特徴抽出処理は以下で表される.

$$\begin{aligned} T &= E(T') \\ &= B(S(T')) \end{aligned}$$

4.5 認証手法

4.4.1 節で作成した認証情報と 4.4.2 節で作成したテンプレートを比較して認証を行う手法について説明する. テンプレートを T , 認証情報を N , 比較結果を R としたとき, 認証合否は以下で定義される.

$$R = C(T, N)$$

$$P(R) \geq k \Rightarrow \text{認証成功}$$

$$P(R) < k \Rightarrow \text{認証失敗}$$

ただし, $C(T, N)$ をテンプレートと認証情報の比較関数, $P(R)$ を比較結果から一致率を算出する関数, k をセキュリティパラメータとする. これらについて次で説明する.

4.5.1 比較関数

テンプレート T と認証情報 N の比較関数について, 以下の通り定義する.

$$\begin{aligned} R &= C(T, N) \\ &= T + N \end{aligned}$$

なお, 行列 M_x の加算については 4.2 節で定義した通りである.

4.5.2 一致率算出関数

比較結果 R から一致率を算出する関数について定義する前に m を定数として, $CNT(M_x, m)$ を以下の通り定義する.

$$t_i \in \{0, 1, \dots, 23\}, x_j \in x \text{ として}$$

$CNT(M_x, m)$ を $c(t_i, x_j) = m$ を満たす (t_i, x_j) の組み合わせの個数とする.

$CNT(M_x, m)$ を使い, 一致率算出関数を以下の通り定義する.

$$P(R) = \frac{CNT(R, 2)}{CNT(R, 1) + CNT(R, 2)}$$

4.5.3 セキュリティパラメータ

セキュリティパラメータについては, 本実験で設定した値を 5 章で説明する.

5. 実験

本章では 4 章で説明した Wi-Fi 認証を利用して, (1) 式でテンプレート更新を行い実験を行った.

5.1 実験データ

本節では実験で使用したデータについて説明する.

5.1.1 採取方法

被験者に常時スマートフォンを携帯させ, スマートフォンのセンサーで Wi-Fi の情報を採取した. 採取したデータには Wi-Fi の BSSID とそのデータをキャッチした時間が含まれている.

5.1.2 データセット

以下の通りデータ採取を行った。

- 被験者人数：47人
- データ採取期間:30日

データの採取はスマートフォンアプリで5分ごとに行っており、採取したデータはスマートフォン端末に保存した。

5.2 実験ケース

データを採取した30日間の期間をA:1~10日, B:11~20日, C:21~30日に3分割し、以下の3ケースで実験を行った。

- ケース1
Aのデータでテンプレート更新を行い、Cのデータで認証を行う。
- ケース2
Bのデータでテンプレート更新を行い、Cのデータで認証を行う。
- ケース3
A+Bのデータでテンプレート更新を行い、Cのデータで認証を行う。

また、それぞれのケースでTAR(True Acceptance Rate)とFAR(False Acceptance Rate)を算出し、評価を行った。

5.3 設定パラメータ

本実験では、(1)式での $\alpha(d)$ 、セキュリティパラメータ k 、二値化パラメータ b について以下の通り設定した。

$$\alpha(d) = \frac{2}{d+1}$$

$$k = 0.01$$

$$b = \alpha(d) \cdot k$$

5.4 実験結果

実験結果は表1となった。図1は結果を棒グラフで表したものである。

表1 実験結果

	ケース1	ケース2	ケース3
TAR	0.770	0.830	0.828
FAR	0.023	0.022	0.023

ケース1とケース2の結果を比較するとケース2の方が精度が良く、Aの期間と比べBの期間のデータの方が認証対象となったCの期間のデータと類似していたことがわかる。一方でケース2とケース3を比較すると、ほぼ同じ結果となっている。これはAの期間に登録されたテンプレートがBの期間更新することで、認証精度を上げたことを示している。この結果からテンプレート更新の有用性が

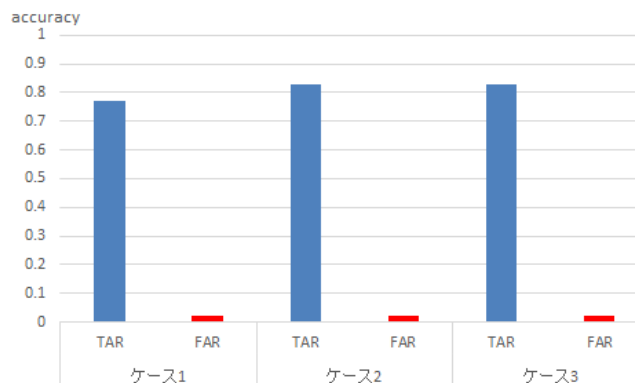


図1 実験結果

わかる。

5.5 考察

本実験のケース3ではA, Bの順序でテンプレート更新を行った。AとBではBの方がCのデータと類似していたため、ケース3のテンプレート更新により認証精度が上がることとなったが、仮にAの方がCと類似していたとすると、テンプレート更新の結果、認証精度が低下する可能性がある。しかし本実験では認証に失敗したデータも更新に利用しており、結果テンプレートがユーザーの特徴から乖離していった可能性もある。認証に失敗した情報をテンプレート更新に使用するかは検討が必要であり、次章で詳しく検討を行う。

6. 更新システム

本章ではテンプレート更新(1)式における $\alpha(d)$ について検討する。本論文の実験では特に考慮しなかったが、 $\alpha(d)$ の値によってテンプレートの更新スピードが変わるため、テンプレートと認証情報の一致率によって $\alpha(d)$ の値は変化されるべきである。一致率が大きい場合はテンプレートがユーザーの特徴を表した量となっているため大きく更新する必要はない。逆に一致率が小さい場合は、テンプレートがユーザーの特徴から離れていっているため、大きく更新する必要がある。そこで、ここでは $\alpha(d)$ の値を2種類設定し、認証時の一致率によって $\alpha(d)$ の値が自動的に変化するシステムを検討する。

6.1 $\alpha(d)$ の設定

本実験では $\alpha(d) = \frac{2}{d+1}$ として実験を行ったが、このような d に依存する値に設定すると、 d が大きくなったとき、 $\alpha(d)$ は無視できるほど小さな値になってしまう。すなわちテンプレートはほぼ更新されなくなるということである。そこで本章の検討では $\alpha(d)$ の値を以下の2つ用意し、一致率によって選択されることとする。

$\alpha_1(d)$: d に依存する数 (ex. $\frac{2}{d+1}$)

$\alpha_2(d)$: d によらない定数 (ex. 0.1)

$\alpha(d) = \alpha_2(d)$ の時, d の値によらずテンプレートは一定の割合で更新されることとなる. テンプレートと認証情報の乖離が大きくなった時は, d の値によらずテンプレートが更新されるよう, $\alpha(d) = \alpha_2(d)$ を選択する.

6.2 $\alpha(d)$ の選択

テンプレートと認証情報の一致率によって $\alpha(d)$ を選択することにしたが, 4.5 節に記述された通り, 認証合否も一致率の値によって判断されている. 認証成功時にはテンプレートはユーザーの特徴を表しているとして $\alpha(d) = \alpha_1(d)$ を選択し, 認証失敗時にはテンプレートと認証情報の乖離が大きいたして $\alpha(d) = \alpha_2(d)$ を選択する.

しかしながら認証失敗時に常に $\alpha(d) = \alpha_2(d)$ としてテンプレートを更新すると, なりすましの問題が発生する. 他者の情報が認証情報として入力されたと仮定して, この入力情報をもとにテンプレート更新を行うと, $\alpha_2(d)$ の割合で他社の情報がテンプレートに含まれることとなる. これが繰り返されると, このテンプレートは他者の特徴を表した量と変化していくことになる. この問題の解決策として, ライフスタイル認証の特性を考慮する.

ライフスタイル認証はその精度の問題で, 1つの要素で完全な認証システムを構築することは困難である. 実現するためには複数の要素を組み合わせるなどの手段が必要となってくる. ここでは説明のために次のようなパスワード認証との2段階認証システムを仮定する. 1つ目のライフスタイル認証が失敗した場合, 2つ目のパスワード認証へと移行し, パスワードが正しければ認証成功, パスワードが誤っていれば認証失敗とする. このシステムで, ライフスタイル認証が失敗しパスワードが正しかった場合は, ライフスタイル認証のテンプレートと認証情報が乖離していたとして $\alpha(d) = \alpha_2(d)$ を選択してテンプレート更新を行う. しかしパスワードも誤っていた場合は, ライフスタイル認証の認証情報は他者の入力であったと判断し, テンプレート更新は行わない.

以上を整理すると, 図2に表されるテンプレート更新システムとなる.

7. おわりに

本論文ではライフスタイル認証における認証情報が移り変わっていくケースを考え, それぞれのケースに対して生体認証における手法を参考にしたテンプレート更新手法を提案した. またそのケースの中で人間の行動がゆるぎケースについて実験を行い, テンプレート更新手法の働きについて確認した.

ライフスタイル認証はユーザーが明示的な動作をせず

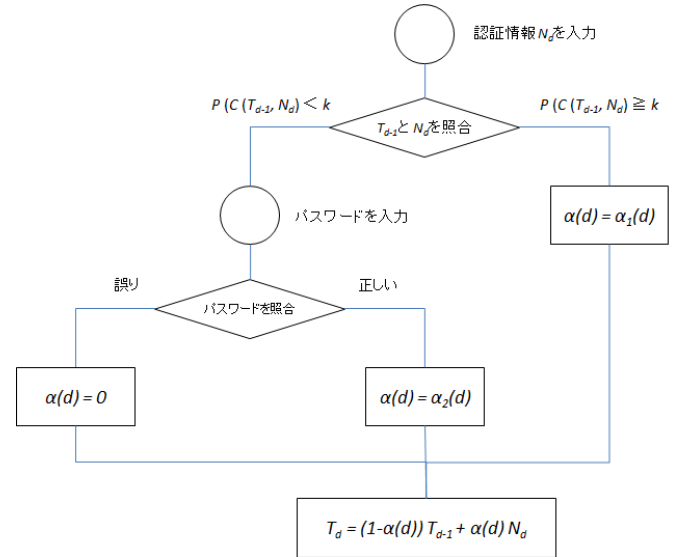


図2 テンプレート更新システム

に認証する手法であるが, テンプレート更新についてはケースに応じてユーザーが動作する必要がある. なぜなら, ケースに応じて更新手法が異なっており, ユーザーはシステムにどのケースかを入力しなければならないからである. 今後の課題としては, 入力情報が変化していくケースをシステムが自動的に判断できるような手法を検討していくことである.

謝辞

本論文の研究は, 次世代個人認証技術講座(三菱 UFJ ニコス寄付講座)による.

参考文献

- [1] Lex Fridman, Steven Weber, Rachel Greenstadt and Moshe Kam: *Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location*. IEEE Systems Journal, Cryptography and Security. (2015)
- [2] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi: *A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User*. 2015 Third International Symposium on Computing and Networking, pp. 463-469 (2015)
- [3] Umut Uludaga, Arun Rossb and Anil Jaina: *Biometric template selection and update: a case study in fingerprints*. Pattern Recognition Volume 37, Issue 7, July 2004, pp.1533-1542 (2004)
- [4] Biagio Freni, Gian Luca Marcialis and Fabio Roli: *Template Selection by Editing Algorithms: A Case Study in Face Recognition*. SSPR&SPR 2008, LNCS 5342, pp. 745-754, (2008)
- [5] Xudong Jiang and W. Ser: *Online Fingerprint Template Improvement*. IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume:24, Issue: 8, pp. 1121-1126 (2002)
- [6] Choonwoo Ryu, Hakil Kim and A. K. Jain: *Template Adaptation based Fingerprint Verification*. 18th International Conference on Pattern Recognition, Volume:4, pp. 582-585 (2006)
- [7] Xiaoming Liua, Tsuhan Chena and Susan M. Thorntonb: *Eigenspace updating for non-stationary process and its*

- application to face recognition*. Pattern Recognition 36, pp. 1945-1959 (2003)
- [8] Fabio Roli and Gian Luca Marcialis: *Semi-supervised PCA-Based Face Recognition Using Self-training*. Joint IAPR International Workshops, August 17-19, 2006, pp. 560-568 (2006)
- [9] 石原 進, 太田 雅敏, 行方 エリキ, 水野 忠則: 端末自体の動きを用いた携帯端末向け個人認証, 情報処理学会論文誌 Vol.46 No.12 pp.2997-3007. (2005)
- [10] 松尾 賢治, 奥村 文教, 橋本 真幸, 小池 淳, 久保田 彰, 羽鳥 好律: 腕の振りに基づく生体認証とテンプレート更新による経時変化の抑制, 電子情報通信学会論文誌 B Vol.J91-B No.6 pp.695-705. (2008)
- [11] 小林良輔, 疋田敏朗, 鈴木宏哉, 山口利恵: 行動センシングログを元にしたライフスタイル認証の提案, コンピュータセキュリティシンポジウム 2016.