情報処理学会論文誌 Vol.60 No.12 2118–2126 (Dec. 2019)

スマートフォン上でのフリック入力を対象とした生体ビット列の生成手法に関する一検討

山神 亮[1] 山崎 恭[1,a)] 大木 哲史[2,b)]

受付日 2019年3月12日, 採録日 2019年9月11日

概要：近年，スマートフォンの急速な普及により，プライバシ保護のためのユーザ認証がますます重要となっている．そこで，スマートフォン上での安全かつ便利なユーザ認証手段として，スマートフォンにおける一般的なユーザインタフェースであるタッチパネルから取得可能な生体情報を利用する生体認証が注目されている．一方，生体認証では，ユーザの生体情報を格納したテンプレートを安全に管理・運用するための様々な手法がテンプレート保護技術として提案されている．テンプレート保護技術を用いた生体認証では，生体情報を秘匿したまま認証することが可能であるが，多くのテンプレート保護技術において，生体情報を有限体上の値に変換したビット列（以下，生体ビット列）が必要となる．しかし，既存手法の多くは，生体情報から生体ビット列を生成する際，本人の特定に有効な個人性が失われ，認証精度が低下する可能性がある．そこで，本稿では，スマートフォン上での安全かつ便利なテンプレート保護技術の実現を目的とし，スマートフォンにおける主要な文字入力手段であるフリック入力を対象とした生体ビット列の生成手法を提案するとともに，シミュレーション実験により提案手法の有効性を評価した．

キーワード：スマートフォン，テンプレート保護，タッチパネル

A Study on Biometric-bit-string Generation Method for Flick Input on Smart Phones

Ryo Yamagami[1] Yasushi Yamazaki[1,a)] Tetsushi Ohki[2,b)]

Received: March 12, 2019, Accepted: September 11, 2019

Abstract: Recently, with the rapid spread of smart-phones, user authentication for privacy protection is becoming increasingly important. Therefore, as secure and convenient user authentication means on a smart-phone, biometric authentication based on biometric information obtainable from a touch panel which is a common user interface in the smart-phone has attracted much attention. On the other hand, in biometric authentication, various methods have been proposed to securely manage and operate a biometric template that stores a user's biometric information as template-protection technologies. In the biometric authentication using template-protection technologies, it is possible to authenticate a user while concealing biometric information. In various template-protection technologies, the biometric information must be converted into a set of values on a finite field (hereinafter, called biometric bit strings). However, with the many current methods, individuality is lost when the biometric information is converted into biometric bit strings, which may degrade authentication accuracy. Therefore, to design a more secure and convenient template protection method for smart-phones, we propose a method to generate biometric bit strings from flick operation which is a major means of inputting characters on the smart-phone and demonstrate its effectiveness through some simulation experiments.

Keywords: smart phone, template protection, touch panel

1. はじめに

近年，スマートフォンの急速な普及により，利用者のプ

[1] 北九州市立大学大学院国際環境工学研究科
Graduate School of Environmental Engineering, The University of Kitakyushu, Kitakyushu, Fukuoka 808–0135, Japan
[2] 静岡大学大学院総合科学技術研究科
Graduate School of Integrated Science and Technology, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[a)] y-yamazaki@kitakyu-u.ac.jp
[b)] ohki@inf.shizuoka.ac.jp

ライバシ情報を扱う機会が多くなり，プライバシ保護のためのユーザ認証がますます重要となっている．そこで，スマートフォンにおけるユーザ認証技術として，スマートフォンに搭載されているセンサから取得可能な生体情報を利用する生体認証方式が注目されている [1]．そのなかでも，スマートフォンに標準的に搭載されているタッチパネルから取得可能な筆記情報を対象とした生体情報に基づく生体認証方式は，指紋認証のように端末に生体認証用の特殊なセンサを別途搭載する必要がないという利点がある．

一方，生体認証には，他のユーザ認証にはない特有の問題点がある．その 1 つとして，生体情報は個人情報であり，使用可能な種類や数が限られているため，ユーザの生体情報を格納したテンプレートが漏洩した場合，生体情報を取り換えることが困難であるという点があげられる．また，生体認証には，偽生体情報の提示などの脅威も存在する．そこで，これらの問題点や脅威に対する対策として，テンプレートを適切に管理し，テンプレートの安全性を向上させる様々な手法がテンプレート保護技術として提案されている [2]．

テンプレート保護技術を用いた生体認証では，生体情報を秘匿したまま認証することが可能であるが，バイオメトリック暗号やキャンセラブルバイオメトリクス [2] など多くのテンプレート保護技術において，生体情報を有限体上の値に変換したビット列（以下，生体ビット列）が必要となる．しかし，既存手法の多くは，生体情報から生体ビット列を生成する際，本人の特定に有効な個人性が失われ，認証精度が低下する可能性がある．そのため，個人性を維持しつつ生体情報を有限体上の値に変換する様々な手法が提案されており，たとえば，指紋 [3], [4] や虹彩 [5] を用いた手法が報告されている．また，生体情報として筆記情報を対象とした手法 [6], [7], [8], [9] も報告されているが，これらの研究では，筆記情報を取得するための端末として，主にペンタブレットが使用されており，また，対象とする筆記情報は英文字署名が多く，筆記情報から抽出される特徴量の種類と数も必ずしも十分とはいえない．従来研究の中には，スマートフォンを使用し，対象とする筆記情報をイニシャルとした研究例 [10] も報告されているが，以下のような課題が残されている．まず，ユーザビリティを考慮した筆記情報を対象としていないことがあげられる．イニシャルは簡易な筆記情報ではあるが，スマートフォンの画面上に筆記するという動作自体が必ずしも自然であるとはいえず，ユーザが負担に感じる可能性があるため，スマートフォンを使用するうえでの自然な動作を筆記情報として選択する必要があると考えられる．次に，スマートフォンの利用環境を考慮した評価が行われていないことがあげられる．スマートフォンを利用する環境は多岐にわたり，各環境に応じて，得られる生体情報の性質が異なる可能性が考えられるため，様々な利用環境を考慮した評価を行うことが不可欠である．さらに，生体ビット列の評価が不十分であることがあげられる．従来研究では，生体ビット列の照合精度，乱数性，相関性の 3 つの観点から生体ビット列の性質の評価が行われているが，生体ビット列の安定性の観点からも評価が必要である．

そこで，本稿では，以上の点を考慮し，スマートフォン上での安全かつ便利なテンプレート保護技術の実現を目的とし，スマートフォンにおける主要な文字入力手段であるフリック入力を対象とした生体ビット列の生成手法を提案するとともに，シミュレーション実験に基づき，提案手法の有効性について評価した結果について報告する．

2. 生体ビット列生成手法

提案する生体ビット列生成手法（以下，提案手法）は，各ユーザから抽出される本人の特定に有効な特徴量の安定性を考慮し，安定性の高い特徴量を強調して生体ビット列を生成する点を特色とする．提案手法では，各ユーザの特徴量ごとに標準偏差を算出し，標準偏差が小さい特徴量をそのユーザから得られる安定性の高い特徴量と見なし，安定性の高い特徴量により多くのビットを割り当てて任意長のビット列を生成する．**図 1** に提案する生体ビット列生成手法の概要を示す．提案手法は，特徴抽出（Feature Extraction），ビット割当ての決定（Bit Assignment Determination），量子化（Quantization），符号化（Encoding）の 4 つの過程に大別される．

2.1 特徴抽出

スマートフォンのタッチパネルから取得可能な特徴量として，ある時刻におけるタッチパネル上での指の位置，指の接触/非接触を表すタッチ状態，タッチパネルを押す指の圧力である筆圧をそれぞれ 1 次特徴量とし，これらを用いて，スマートフォン上のフリック操作から本人の特定に有効な特徴量を抽出する文献 [11] の手法を参照して**表 1** に示す 7 種類の 2 次特徴量（以下，特徴量）を抽出する．ここで，抽出された特徴量に対して正規化を施す．いま，i 番目の特徴量を X_i（$1 \leq i \leq 7$），正規化後の i 番目の特徴量を F_i（$1 \leq i \leq 7$）とし，式 (1) のように定義される正規

表 1 特徴量の種類と説明 [11]
Table 1 Types and descriptions of features.

特徴量	説明
X 変位	フリックの開始から終了までの X 座標の変位量
Y 変位	フリックの開始から終了までの Y 座標の変位量
フリック長	フリックの開始から終了までの軌跡の長さ
フリック曲度	フリックの曲がり度合い
フリック速さ	フリックの開始から終了までの平均の速さ
フリック角度	フリックの角度（中心からのずれ）
圧力	フリックの開始から終了までの平均の圧力

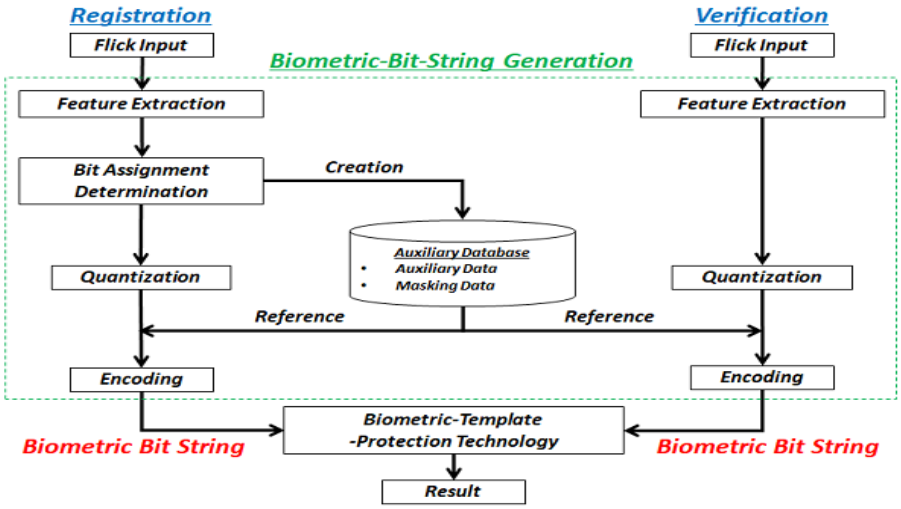

図 1 生体ビット列生成手法の概要
Fig. 1 Overview of biometric-bit-string generation.

化処理により，各特徴量を 0〜1 に正規化する．なお，式 (1) の $\max X_i$，$\min X_i$ は，それぞれ特徴量 X_i の最大値と最小値を表す．

$$F_i = \frac{X_i - \min X_i}{\max X_i - \min X_i} \tag{1}$$

2.2 ビット割当ての決定

ユーザごとに正規化後の各特徴量における標準偏差を算出し，各特徴量に割り当てるビット数を決定する．ここで，標準偏差の小さい特徴量は，そのユーザから安定した取得が可能であることを示している．そこで，提案手法では各ユーザについて，正規化された各特徴量の標準偏差を算出し，標準偏差の小さい特徴量により多くのビットを割り当てて任意長のビット列を生成する．具体的なビット割当ての過程を以下に示す．

(1) 標準偏差の算出
各ユーザについて，複数回のフリック入力から得られる複数個の各特徴量 F_i の標準偏差 σ_i（$1 \leq i \leq 7$）を算出する．

(2) ビット割当てに関する変数 x の算出
式 (2) に (1) で求めた各標準偏差の値を代入し，ビット割当てに関する変数 x を算出する．ここで，K は総ビット長を表す．また，式 (2) は，提案手法が標準偏差の小さい特徴量により多くのビットを割り当てる手法であるため，除算の特性である分母の値が小さいほど，計算結果が大きくなるということを考慮している．

$$\sum_{i=1}^{7} \frac{x}{\sigma_i} = K \tag{2}$$

(3) ビット割当ての決定
算出した変数 x と各標準偏差の値を再度式 (2) に代入する．このとき，左辺を展開した各項の値がユーザごとの各特徴量に対応するビット数となる．なお，式 (2) における総ビット長 K の値は任意に設定可能であるため，提案手法では任意長のビット列を生成することが可能である．ここで，決定したユーザごとの各特徴量に対応するビット数を補助データ（Auxiliary Data）として補助データベース（Auxiliary Database）に登録する．

表 2 量子化テーブル
Table 2 Quantization table.

F_i	$Q[F_i]$
$F_i < 0.25 \times \max f_i$	0
$0.25 \times \max f_i \leq F_i < 0.5 \times \max f_i$	1
$0.5 \times \max f_i \leq F_i < 0.75 \times \max f_i$	2
$0.75 \times \max f_i \leq F_i$	3

2.3 量子化

抽出した特徴量の揺らぎを低減するため，あらかじめ用意した量子化テーブルを参照し，特徴量を量子化する．量子化テーブルの作成には，各被験者から取得した複数回のフリック入力データ（以下，学習データ）を使用した．**表 2** に量子化テーブルの一例を示す．表 2 の $\max f_i$（$1 \leq i \leq 7$）は学習データの最大値を，$Q[F_i]$ は量子化インデックスを表す．また，提案手法では，テンプレート保護技術の分野で使用する生体ビット列のビット長を 2^n と設定する場合が多いことを考慮し，量子化レベルを 4 に設定した．ここで，補助データベースに格納した補助データを参照し，前節で決定したユーザごとの各特徴量に対応するビット数に従い，安定性の高い特徴量に対応する量子化インデックスを反復して出力する．なお，ここで出力する量子化インデックスの系列を $Q[F_i]'$ と定義する．

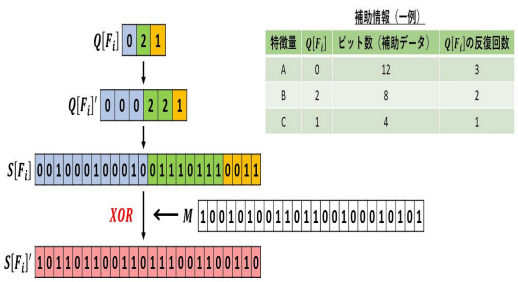

図 2 符号化の過程（例）
Fig. 2 Example of encoding process.

2.4 符号化

量子化インデックスの系列 $Q[F_i]'$ を “0” と “1” からなるビット列へ変換するための符号化を行う．符号化の過程の一例を**図 2** に示す．提案手法では，量子化インデックス間の差分値とビット列間のハミング距離が等しくなる性質を持つ Tompkins code を使用する．前節で述べたとおり，提案手法の量子化レベルは 4 と設定しており，総ビット長を 2^n とすることを考慮して Tompkins code を 4 ビットで表現する．ここで，図 2 において，$Q[F_i]'$ を符号化したビット列 $S[F_i]$ を生体ビット列とすると，$S[F_i]$ には同一のビット列（ビットパターン）が複数回出現することになるため，生体ビット列の統計的性質である乱数性や相関性の観点からは望ましくない影響を与える可能性がある．そこで，この問題に対する対策として，提案手法では，生成する生体ビット列のビット長に応じて乱数を与えるマスキングデータ（Masking Data）M を提案手法（生体ビット列生成システム）全体で 1 つ用意し，$S[F_i]$ と M の排他的論理和を算出することで乱数化したビット列 $S[F_i]'$ を生成し，これを生体ビット列と定義する．乱数化したビット列 $S[F_i]'$ は，乱数化前のビット列 $S[F_i]$ と比較して生体ビット列の自己相関を評価した際，低い相関値を示すことが期待される．ここで使用したマスキングデータは，補助データとあわせて補助データベースに登録する．

3. 信頼性評価実験

実際のフリック入力データを用いたシミュレーション実験により，後述する生体ビット列の照合精度，乱数性，相関性，安定性の観点から提案手法の信頼性を評価した．実験では，スマートフォン利用時におけるフリック入力の利用場面の一例として，Web ブラウザを起動した際の初期画面である Web 検索画面（以下，Web 検索）と主要オンラインショッピングサイトにおける商品検索画面（以下，商品検索）を想定し，日本語によるフリック入力を取得するため，以下に述べる 2 種類の実験を行った．

- 実験 1
  スマートフォンの利用環境として，座位時と歩行時の 2 種類を想定し，**図 3** に示す Web 検索を想定した文字入力画面を使用して，全平仮名 46 文字をランダムに並べ替え，10 文字単位で区切ってフリック入力を取得した．実験で取得した文字列は，「うろふまいやれわたも」，「ねめすえさくんしよの」，「ちかつてをほあらみゆ」，「にはこそひりむるけぬ」，「とおなきへせ」の 5 種類である．なお，被験者は日常的にフリック入力を利用しているが，取得する文字列がランダムであるとスムーズなフリック入力が得られず，被験者の個人性を反映したフリック入力が取得しにくくなる可能性が考えられたため，被験者が十分に慣れるまで各文字列のフリック入力を練習した後，フリック入力を取得した．
- 実験 2
  スマートフォンの利用環境を座位時に固定し，主要オンラインショッピングサイトにおいて商品を検索する状況を想定した文字列を取得した．実験では，主要オンラインショッピングサイトの 1 つである「楽天市場」において，楽天年間ランキング 2018 [12] で 1 位となったアイテムである「クリスタルガイザー」という文字列を検索することを想定し，図 3 で，「らくてんいちば」と入力し，**図 4** の商品検索を想定した文字入力画面において，「くりすたるがいざー」と入力することにより，フリック入力を取得した．

図 3 Web 検索を想定した文字入力画面
Fig. 3 Character input screen assuming web search.

図 4 商品検索を想定した文字入力画面
Fig. 4 Character input screen assuming product search.

実験の諸元を**表 3** に示す．ここで，本人間の比較回数は，本人の学習用データ 6 回と本人のテスト用データ 4 回の総当たりの回数であり，他人間の比較回数は，本人の学習用データ 6 回と他人のテスト用データ 36 回の総当たりの回数である．

以上，2 種類の実験で取得したフリック入力データを使

表 3 実験の諸元
Table 3 Experimental conditions.

使用端末	Apple iPhone6s MKQP2J/A
実験環境	実験 1：座位，歩行/実験 2：座位
入力手段	フリック入力
被験者数	10 名
取得データ数	各文字列 10 回 × 10 名
本人間の比較回数	240 回 （学習用 6 回（本人）× テスト用 4 回（本人）× 10 名）
他人間の比較回数	2,160 回 （学習用 6 回（本人）× テスト用 36 回（他人）× 10 名）

用し，フリック入力の個人性の評価を行い，その後，生体ビット列の照合精度，乱数性，相関性，安定性の 4 つの観点から生体ビット列の性質を評価した．

3.1 フリック入力の個人性

生体ビット列の評価に先行し，生体ビット列生成前のフリック入力データに，元来どの程度の個人性が含まれるか，また，その個人性は文字によりどの程度異なるかを評価する実験を行った．実験では，量子化・符号化前の各特徴量に対し，データを比較した際の絶対値差分を求め，その全特徴量についての総和を評価値として FMR（False Match Rate）と FNMR（False Non Match Rate）を算出した後，等誤り率（EER，Equal Error Rate）を算出した．実験 1 で取得した平仮名のうち，タップ操作で取得可能な「あ・か・さ・た・な・は・ま・や・ら・わ」は，7 種類の特徴量（表 1 参照）のうち圧力のデータしか取得できないためこれを評価対象から除き，残りの 36 文字を使用して，量子化・符号化前の等誤り率を算出した．その中から代表して，座位時，歩行時における EER の低い 8 文字と EER の高い 8 文字の結果を抽出したものを**表 4**，**表 5** に示す．ここで，表 4，表 5 に記載されている始点位置は，各平仮名のフリック入力が始まる位置であり，1 から 10 の数字は**図 5** のように定義している．たとえば，「あ・い・う・え・お」の始点位置は “1” となる．表 4，表 5 の始点位置に着目すると，EER の低い文字は始点位置の数字が図 5 の左側に位置することが多く，EER の高い文字は始点位置の数字が図 5 の右側に位置することが多いことが分かる．これは，被験者が全員右利きであり，端末を右手で持ち，右手の親指でフリック入力していたことに起因し，より親指の可動範囲が広くなる文字入力画面の左側において，個人性を反映したフリック入力が行われたものと推察される．

3.2 生体ビット列の照合精度

提案手法により生成された生体ビット列の照合精度を評価した．提案手法ではビット長を任意に設定できるが，今後，生体ビット列をテンプレート保護のための暗号鍵として使用することを考慮し，ここでは 1 文字あたりのビット長を 256 [bit] とした．実験では，生成された生体ビット列間のハミング距離に基づき FMR と FNMR を算出した後，EER を算出した．また，前節と同様の方法で量子化・符号化前の EER について算出し，両者を比較した．以下に，3 種類の実験結果について述べる．

表 4 量子化・符号化前の EER（座位時）
Table 4 EER before quantization and encoding (at the time of sitting).

(a) EER の低い 8 文字

平仮名	EER [%]	始点位置
ぬ	24.3	5
き	26.2	2
む	26.3	7
え	26.9	1
い	27.8	1
う	28.4	1
め	28.5	7
て	28.6	4

(b) EER の高い 8 文字

平仮名	EER [%]	始点位置
く	38.4	2
そ	38.4	3
ん	36.6	10
ふ	35.9	6
り	35.7	9
へ	35.5	6
す	35.1	3
ろ	35.1	9

表 5 量子化・符号化前の EER（歩行時）
Table 5 EER before quantization and encoding (at the time of walking).

(a) EER の低い 8 文字

平仮名	EER [%]	始点位置
と	25.4	4
れ	26.3	9
お	28.9	1
い	30.2	1
き	30.3	2
こ	30.3	2
も	30.9	7
む	31.0	7

(b) EER の高い 8 文字

平仮名	EER [%]	始点位置
ろ	39.8	9
え	39.8	1
め	37.7	7
ゆ	37.3	8
ん	37.1	10
り	36.4	9
く	36.0	2
せ	35.9	3

図 5 始点位置
Fig. 5 Start point.

3.2.1 各文字（1 文字）を対象とした照合精度

実験 1 で取得した平仮名のうち，フリック操作のみで取得可能な平仮名 36 文字を使用して EER を算出した．**図 6** に，座位時における各文字の特徴量と生体ビット列（以下，量子化・符号化前後）の EER を，**図 7** に，歩行時における各文字の量子化・符号化前後の EER をそれぞれ示す．図 6，図 7 より，座位時，歩行時ともに，ほとんどの文字は，量子化・符号化前と比較して，量子化・符号化後の方

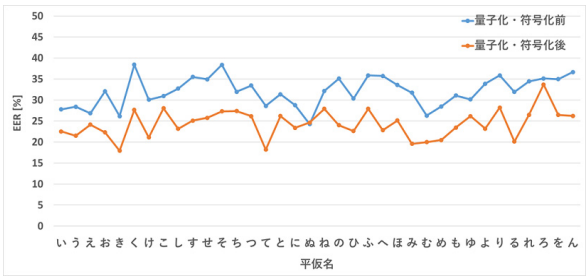

図 6 各文字の量子化・符号化前後の EER（座位時）
Fig. 6 EER of each character before and after quantization and encoding (at the time of sitting).

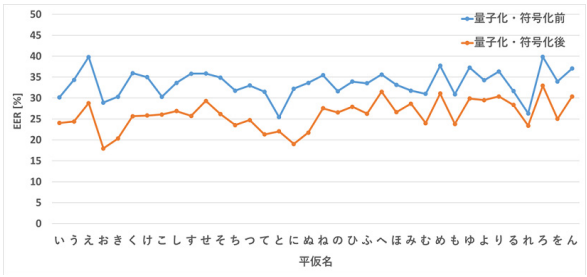

図 7 各文字の量子化・符号化前後の EER（歩行時）
Fig. 7 EER of each character before and after quantization and encoding (at the time of walking).

が，EER が低下していることが確認される．これは，提案手法がユーザごとに安定性の高い特徴量を強調する手法であり，抽出した 7 種類の特徴量から 256 [bit] の生体ビット列を生成していることから，各特徴量に割り当てるビット長が長くなったことで，より個人性を反映した生体ビット列が生成されたことに起因する結果であると考えられる．また，座位時と歩行時では，座位時の方が EER がわずかに低いことが確認される．これは，座位時の方が歩行時と比較して安定したフリック入力が行われていることを示していると考えられる．

3.2.2 複数文字を対象とした照合精度（実験 1）

前節の各文字を対象とした EER の結果に基づき，複数文字を対象とした EER を算出した．本実験では，座位時，歩行時ともに EER の小さい順に抽出した 16 文字と，EER の大きい順に抽出した 16 文字を評価対象とした．**図 8** にそれぞれの実験環境における複数文字を対象とした量子化・符号化後の EER の変化を示す．ここで，図 8 の「最小」は EER の小さい順に平仮名を組み合わせた結果を示し，「最大」は EER の大きい順に平仮名を組み合わせた結果を示す．図 8 の結果より，いずれの実験環境においても，組み合わせる文字数が増えると EER は低下する傾向にあることが確認される．たとえば，座位時に 8 文字を組み合わせた場合，生体ビット列のビット長は 2,048（$= 256 \times 8$）[bit] となり，EER の最小値は 2.3 [%]，EER の最大値は 7.5 [%] となることが確認される．これらの結果は，取得した 8 文字がどのような文字の組合せであっても，量子化・符号化後の EER がこれらの最小値と最大値の範囲内に収まる可能性が高いことを示していると考えられる．

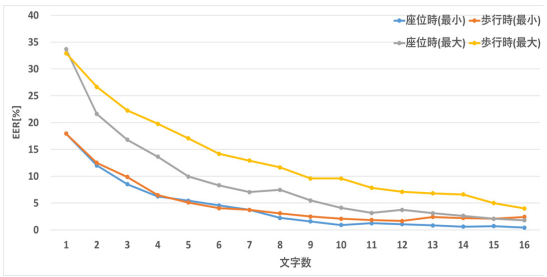

図 8 複数文字を対象とした量子化・符号化後の EER の変化
Fig. 8 EER of some characters before and after quantization and encoding.

3.2.3 複数文字を対象とした照合精度（実験 2）

実験 2 で取得した「らくてんいちば」，「くりすたるがいざー」のうち，フリック操作をともなわないタップ操作のみで取得可能な「ら・ば・た・が・ざ」と長音符（ー）を除く「く・て・ん・い・ち・く・り・す・る・い」の 10 文字を評価対象とし，EER を算出した．なお，評価対象において，「い」と「く」は重複しているが，実際の利用場面では，同一文字を複数回フリック入力する状況も想定されるため，本実験では，重複した文字も独立した 1 文字として評価対象に加えた．また，組み合わせる文字数は 10 文字であるため，総ビット長は 2,560（$= 256 \times 10$）[bit] となる．実験の結果，量子化・符号化前の EER は 11.4 [%]，量子化・符号化後の EER は 4.2 [%] となった．これらの結果より，実際の利用場面を想定した実験においても，量子化・符号化後の EER は小さい値となり，提案手法の有効性が示されたと考えられる．

3.3 生体ビット列の乱数性

生体ビット列は “0” と “1” から構成されるため，その乱数性は提案手法の安全性を保証する根拠の 1 つとなる．実験では，提案手法に基づき 256 [bit] の生体ビット列を 3,600 個生成し，各生体ビット列の “0” ビットの出現率について評価を行った．また，比較対象として，代表的な擬似乱数系列生成器の 1 つであるメルセンヌ・ツイスター [15] を用いて生成した連続する 1 億 [bit] の乱数から 3,600 個の開始点をランダムに選択し，各開始点から生体ビット列のビット長と同じ連続する 256 [bit] のビット列を抽出して “0” ビットの出現率を評価した．実験の結果を**表 6** に示す．表 6 より，平均値，標準偏差ともに，乱数化後の値は乱数化前の値よりも擬似乱数による結果に近い値が得られている．これは，乱数化後の生体ビット列と擬似乱数から抽出したビット列の分布が類似しており，両者は同等な性質を有することを示しているといえる．以上の結果から，提案手法に基づき生成された乱数化後の生体ビット列は，擬似乱数から抽出したビット列との識別が困難であるという点にお

表 6 “0” ビットの出現率
Table 6 The occurrence rate of “0” bit.

対象		平均値 [%]	標準偏差
乱数化前	実験 1（座位時）	51.1	9.2
	実験 1（歩行時）	51.1	9.5
	実験 2	52.0	9.6
乱数化後	実験 1（座位時）	50.7	2.3
	実験 1（歩行時）	50.6	2.2
	実験 2	50.9	2.1
擬似乱数	メルセンヌ・ツイスター	50.0	3.1

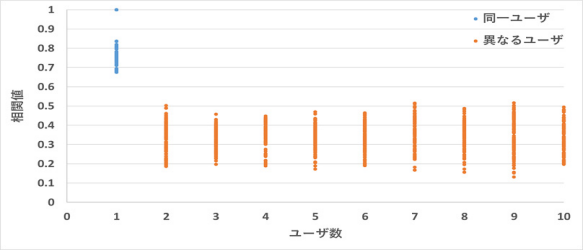

図 9 生体ビット列の相関値（実験 1，座位時）
Fig. 9 Correlation between biometric bit strings (experiment 1, sitting).

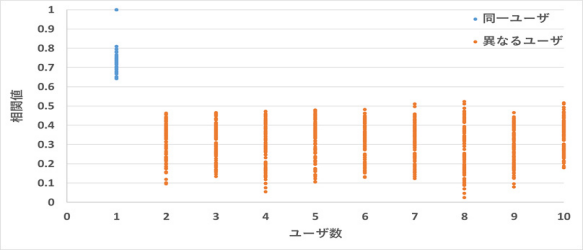

図 10 生体ビット列の相関値（実験 1，歩行時）
Fig. 10 Correlation between biometric bit strings (experiment 1, walking).

いて十分な乱数性を有すると考えられる．

3.4 生体ビット列の相関性

同一ユーザおよび異なるユーザからそれぞれ得られた生体ビット列のビット列間の相関値を，任意の 1 人のユーザについて比較した場合を**図 9**，**図 10**，**図 11** に示す．ここで図中の青点は同一ユーザの生体ビット列の相関値，赤点は異なるユーザの生体ビット列の相関値を示している．なお，本実験では生体ビット列間の位相は考慮していない．これらの結果より，実験環境を問わず，同一ユーザから得られた生体ビット列どうしには高い相関があり，異なるユーザから得られた生体ビット列どうしの相関は低いことが分かる．これは，提案手法から得られた生体ビット列の性質がユーザ間で明確に異なることを示しているといえる．さらに，生体ビット列の位相の観点から自己相関・相互相関を求め，提案手法におけるマスキングデータの有効性を評価した．**図 12**，**図 13**，**図 14** に，生体ビット列の自己相

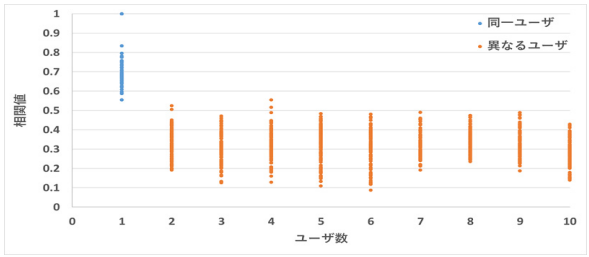

図 11 生体ビット列の相関値（実験 2）
Fig. 11 Correlation between biometric bit strings (experiment 2).

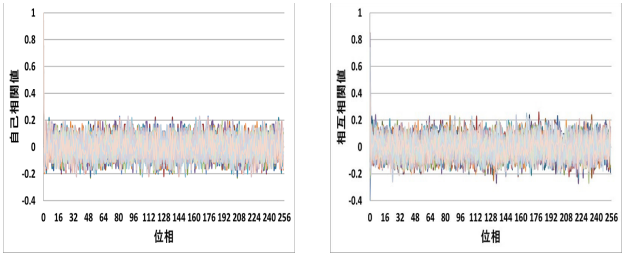

図 12 生体ビット列の自己相関・相互相関（実験 1，座位時）
Fig. 12 Auto and cross-correlation between biometric bit strings (experiment 1, sitting).

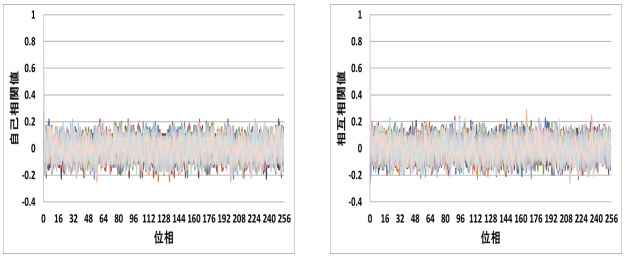

図 13 生体ビット列の自己相関・相互相関（実験 1，歩行時）
Fig. 13 Auto and cross-correlation between biometric bit strings (experiment 1, walking).

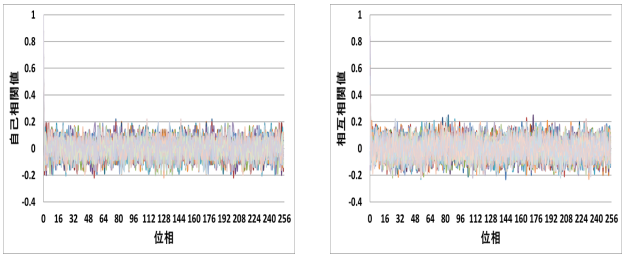

図 14 生体ビット列の自己相関・相互相関（実験 2）
Fig. 14 Auto and cross-correlation between biometric bit strings (experiment 2).

関・相互相関を求めた結果を示す．ここで，評価に使用した生体ビット列は，各ユーザから得られた生体ビット列よりランダムに複数個選択したものを対象とした．自己相関値は，同一ユーザの生体ビット列間の位相を 1 ビットずつ右にシフトしたときの相関値を求めた結果，相互相関値は，異なるユーザの生体ビット列間の位相を 1 ビットずつ右にシフトしたときの相関値を求めた結果である．これらの結

表 7 各ユーザ内で一致したビット数
Table 7 Number of matched bits in each user.

対象	平均値	割合 [%]
実験 1（座位時）	209	81.8
実験 1（歩行時）	208	81.2
実験 2	209	81.6

果より，同一ユーザから生成された生体ビット列の位相をずらした系列，異なるユーザから生成された生体ビット列の位相をずらした系列ともに，相関値が低いことが確認された．このことから，マスキングデータによる乱数化の有効性を示すことができたと考えられる．実験結果からは，特に相関値の高いユーザは見られず，全ユーザが安定して低い値を示していることが確認された．これらの結果は，提案手法が安定性の高い特徴量を反復して使用する手法であり，ユーザごとに安定性の高い特徴量が異なることから，ユーザ間で生体ビット列のハミング距離が大きくなったことに起因するものであると考えられる．

3.5 生体ビット列の安定性

生体ビット列の安定性を評価するため，各ユーザ内での複数の生体ビット列間のハミング距離を算出した．総ビット長とハミング距離の差分値は，各ユーザ内での複数の生体ビット列間で一致するビット数を表す．**表 7** に，各ユーザ内で一致したビット数の平均値とその割合を示す．なお，平仮名 1 文字あたりの総ビット長は 256 [bit] である．表 7 の結果は，各ユーザ内で生体ビット列を生成した際，安定して同じビットが生成されるビット数の平均値が約 210 [bit] であることを示しており，一例として，生成した生体ビット列に対し，誤り訂正符号を用いて生体情報の誤差を許容するテンプレート保護技術 [13], [14] を適用する場合，約 45 [bit] の誤り訂正が必要となることを示しているといえる．

4. 結論と今後の課題

本稿では，スマートフォン上での安全かつ便利なテンプレート保護技術の実現を目的とし，スマートフォン上でのフリック入力を対象とした生体ビット列の生成手法を提案するとともに，シミュレーション実験に基づき，提案手法の有効性を評価した．今後の課題として，より多くの実利用環境を想定した評価や生成した生体ビット列に基づくテンプレート保護技術の実現，日本語以外のフリック入力への適用可能性の検討などがあげられる．

謝辞 本研究の一部は，JSPS 科研費 JP16K00190 の助成を受けたものです．生体ビット列の乱数性評価に関して貴重なコメントをいただいた北九州市立大学宮﨑武博士に深謝します．

参考文献

[1] Tresadern, P.A., McCool, C., Poh, N., Matejka, P., Hadid, A., Levy, C., Cootes, T.F. and Marcel, S.: Mobile Biometrics: Combined Face and Voice Verification for a Mobile Platform, *IEEE Pervasive Computing*, Vol.12, No.1, pp.79–87 (2013).
[2] Jain, A.K., Nandakumar, K. and Nagar, A.: Biometric Template Security, *EURASIP Journal on Advances in Signal Processing*, Vol.2008, pp.1–17 (2008).
[3] Nandakumar, K., Nagar, A. and Jain, A.K.: Hardening Fingerprint Fuzzy Vault Using Password, *Proc. ICB 2007*, LNCS, Vol.4642, pp.927–937 (2007).
[4] Jin, Z., Ong, T.S., Tee, C. and Teoh, A.B.J.: Generating revocable fingerprint template using polar grid based 3-tuple quantization technique, *Proc. IEEE 54th Int. Midwest Symp. Circuits and Systems* (*MWSCAS 2011*), pp.1–4 (2011).
[5] Rathgeb, C. and Uhl, A.: Adaptive fuzzy commitment scheme based on iris-code error analysis, *Proc. 2nd European Workshop on Visual Information Processing* (*EUVIP 2010*), pp.41–44 (2010).
[6] Feng, H. and Wah, C.C.: Private key generation from online handwritten signature, *Information Management and Computer Security*, pp.159–164 (2002).
[7] Vielhauer, C., Steinmetz, R. and Mayerhöfer, A.: Biometric Hash based on Statistical Feature of Online Signature, *Proc. 16th Int. Conf. Pattern Recognition* (*ICPR 2002*), Vol.1, pp.123–126 (2002).
[8] Freire-Santos, M., Fierrez-Aguilar, J. and Ortega-Garcia, J.: Cryptographic key generation using handwritten signature, *Proc. SPIE*, Vol.6202, pp.225–231 (2006).
[9] Goubaru, Y., Yamazaki, Y., Miyazaki, T. and Ohki, T.: A consideration on a common template-based biometric cryptosystem using on-line signatures, *Proc. IEEE 3rd Global Conf. Consumer Electronics* (*GCCE 2014*), pp.131–135 (2014).
[10] Yamagami, R. and Yamazaki, Y.: Biometric Bit String Generation from Handwritten Initials on Smart Phones, *Proc. 4th Int. Workshop on Information and Communication Security* (*WICS 2017*), pp.516–521 (2017).
[11] 松原慶朋，西村治彦，佐村敏治，吉本裕行，谷本良平：電子端末上でのフリック操作による新たな生体認証技術，信学技報，BioX2015-39, MBE2015-50, NC2015-34, pp.91–96 (2015).
[12] 楽天株式会社：楽天年間ランキング 2018，楽天市場（オンライン），入手先 ⟨https://event.rakuten.co.jp/rankingyearly/⟩（参照 2018-01-30）.
[13] Juels, A. and Wattenberg, M.: A fuzzy commitment scheme, *Proc. 6th ACM Conf. Computer and Communications Security* (*CCS '99*), pp.28–36 (1999).
[14] Juels, A. and Sudan, M.: A fuzzy vault scheme, *Proc. IEEE Int. Symp. Information Theory* (*ISIT 2002*), p.408 (2002).
[15] 松本 眞：Mersenne Twister with improved initialization (2002)，入手先 ⟨http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/MT2002/mt19937ar.html⟩（参照 2019-07-01）.

山神 亮

2017 年北九州市立大学国際環境工学部情報メディア工学科卒業．2019 年同大学大学院博士前期課程修了．同年株式会社野村総合研究所入社．在学中，バイオメトリクスとテンプレート保護技術に関する研究に従事．

山崎 恭 （正会員）

1993 年早稲田大学理工学部電子通信学科卒業．1998 年同大学大学院理工学研究科博士後期課程修了．博士（工学）．日本学術振興会特別研究員（DC2，PD），早稲田大学理工学部助手を経て，2001 年北九州市立大学国際環境工学部助教授（2007 年より准教授）．主に，情報セキュリティとその応用に関する研究に従事．電子情報通信学会，画像電子学会，IEEE，ACM 各会員．

大木 哲史 （正会員）

2002 年早稲田大学理工学部電子情報通信学科卒業．2004 年同大学大学院理工学研究科電子・情報通信学専攻修士課程修了．2010 年早稲田大学理工学術院情報・ネットワーク専攻博士（工学）取得．2010 年早稲田大学理工学総合研究所次席研究員，2013 年産業技術総合研究所特別研究員を経て，2017 年より静岡大学大学院総合科学技術研究科講師．情報セキュリティ全般，特に個人認証を中心としたネットワークセキュリティに関する研究に従事．電子情報通信学会会員．