

# スマートフォンを用いた音声情報に基づく 生体ビット列の生成手法に関する研究

原田 亜紀<sup>†</sup> 山崎 恭<sup>†</sup>

<sup>†</sup> 北九州市立大学国際環境工学部情報メディア工学科

## 1. はじめに

近年、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生体認証が注目されている。生体認証では使用可能な生体情報の種類と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は難しい。そのため、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[1]。テンプレート保護技術を用いた生体認証では、誤り訂正符号を用いて生体情報の誤差を許容する手法が主流であるが、これらの手法では、生体情報を有限体上の値で表現するため、生体情報を有限体上の値に変換したデータ(以下、生体ビット列)が必要となる。

そこで、本稿では生体情報としてスマートフォンとの親和性が高く、端末に搭載されたマイクロフォンを用いて取得可能な音声情報に着目し、音声情報から発話内容に依存しない話者の個人性を反映した生体ビット列を生成する一手法を提案するとともに、実際の利用環境を想定したシミュレーション実験により、提案手法の信頼性を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

音声情報から、特徴量としてメル周波数ケプストラム係数(Mel-Frequency Cepstrum Coefficients, MFCC)とその時間変化である $\Delta$ MFCCを抽出し、LBGアルゴリズムを用いてコードブックを生成する。ただし、コードブックのレベル数は32レベル、特徴量の次元数は、MFCCのときに12次元、MFCC+ $\Delta$ MFCCのときに24次元とする。その後、コードブックの量子化代表ベクトルの各要素を、4ビットのビット列へ変換して生体ビット列を生成する。このとき、ビット列への変換方法として、(a)通常の2値化と、(b)Gray codeの2種類を検討した。

## 3. 信頼性評価実験

無響室において、10名の被験者からスマートフォンを使用して取得した音声情報に基づき生体ビット列を生成するシミュレーション実験を行った。生体ビット列に変換する前後の状態における認証精度を、等誤り率(Equal Error Rate, EER)を用いて評価した結果を表1に示す。表1より、30秒の音声に対し、特徴量としてMFCC+ $\Delta$ MFCCを使用し、Gray codeを使用して生体ビット列を生成した場合、生体ビット列への変換に伴う認証精度の低下が最も小さいことが

確認された。また、生体ビット列における“0”の出現率は、平均で約48.65[%]であり、提案手法で得られた生体ビット列は十分な乱数性を有すると言える。さらに、生体ビット列間の自己相関と相互相関を算出した結果、同一ユーザから得られた生体ビット列同士には高い相関のあることがわかり、異なるユーザに属する生体ビット列間の相関値は、比較的0に近い値となることが確認された。これらの結果は、生体ビット列の性質がユーザ間で明確に異なることを表していると言える。

一方、実際の利用環境を想定した比較的雑音レベルの小さい環境として、①空調無しの人無研究室、②空調有りの人無研究室、③車通りの無い屋外の3通りを選定し、それぞれの環境において生体ビット列を生成した。このとき、各環境の雑音レベルの平均値は、それぞれ①33.9[dB]、②46.4[dB]、③48.6[dB]である。各環境における生体ビット列の認証精度を表2に示す。表2より、比較的雑音レベルの小さい環境では、生体ビット列が雑音に対する頑健性を有することが確認される。

表1: ビット列変換前後の認証精度(EER[%])

		15秒の音声	30秒の音声
MFCC	変換前	3.49	3.33
	変換後 (a)	7.89(+4.41)	5.54(+2.21)
	変換後 (b)	5.88(+2.39)	4.18(+0.85)
MFCC + $\Delta$ MFCC	変換前	5.32	3.33
	変換後 (a)	10.94(+5.62)	5.72(+2.39)
	変換後 (b)	7.12(+1.80)	4.04(+0.71)

表2: 雑音環境下における認証精度(EER[%])

環境	無響室	空調無	空調有	屋外
EER	4.04	4.94	6.30	6.45

## 4. まとめ

スマートフォンから取得した音声情報に基づく生体ビット列の生成手法を提案し、提案手法の有効性を評価した。今後の課題として、特徴量に対する重み付けや、より信頼性の高い生体ビット列の生成手法に関する検討などが挙げられる。

## 参考文献

[1] 高橋健太, 村上隆夫, “バイオメトリクス・セキュリティの最新動向,” 第3回バイオメトリクスと認識・認証シンポジウム(SBRA2013), 2013.