スマートフォンのホーム画面を用いた代替認証手法の提案

2017SC050 西田正樹 2017SC053 野首優斗
指導教員：河野浩之

1 はじめに

スマートフォンにおける認証技術が進歩するにつれ, 様々な認証方式が登場してきた. 例えば, 指紋や顔を認証要素として用いる生体認証は広く普及し, 我々の生活の一部になりつつある. 一方, 何らかの原因によって本人であるのにもかかわらず認証ができないといったような, 有事の際を想定して開発されている認証方式は少ない. 現に, 情報処理学会に掲載されている過去 10 年間の研究の中で, スマートフォンにおける代替認証を主のテーマとした研究は 1 件であった [1]. また, スマートフォンにあらかじめ設定していたパスワードの入力を, 規定回数以上に間違えると再入力までの時間が延長されるだけであり, パスワードを完全に忘却してしまった際には端末を初期化するしかない, という現状がある.

このような現状を踏まえ, 本研究では, スマートフォンにおける最適な代替認証手法を提案する. また, 実験等の一連の作業を通して, 代替認証手法のより良い提案を行うことを本研究の目的とする.

2 知識情報を用いた認証方式

2 章では, 知識情報を用いた認証方式について説明する. 2.1 節では, 代替認証として最適な秘密情報, 2.2 節では, 知識情報を用いた関連研究の比較, 2.3 節では, 代替認証において最適な知識情報について述べる.

2.1 代替認証として最適な秘密情報

認証に用いられる要素は, 知識情報, 所持情報, 生体情報の 3 つに大別される [5]. 今回想定する有事の際とは, パスワードを完全に忘却してしまった, あるいはパスワード設定の際に誤ったパスワードで登録してしまった等の理由で, 自身のスマートフォンのロックが解除できなくなってしまった場合である. このような事態は滅多に起こることではないが, その際にはスマートフォンの初期化といったような, ユーザにとって負荷の大きい対処法を取らざるを得ない場合がほとんどである.

したがって, 本研究は非常に限定的な場面を想定したものであり, 認証要素として生体情報を用いるような実装に高いコストがかかるシステムは不向きである. また, 上述したような有事の際に, ある特定のものを所持している可能性は低いため, 所持情報を用いた認証方式は代替認証としては適切ではないと考えられる. 以上の議論より, 代替認証手法に用いる認証要素としては知識情報を採用するのが最適であると考えられる.

2.2 知識情報を用いた関連研究の比較

表 1 は, 知識情報を用いた関連研究の比較を行ったものである. 知識情報を認証要素として利用する研究の中でも映像記憶やエピソード記憶を用いる等, ユーザが秘密情報を保持する為の工夫が施されている研究に着目した.

表 1 知識情報を用いた認証方式の関連研究の比較

著者	認証手法	課題
安齋 [1]	アプリのインストールの有無およびアプリの利用時間に関する質問	インストールされるアプリの偏り (LINE, Twitter 等の SNS アプリ)
飯澤 [2]	Web ページ閲覧履歴	不正画像選出の難易度が高い
増井 [3]	エピソード記憶からパスワードを生成	質問によっては誤答を生成することが困難
稲村 [4]	パターンロック方式	認証方式の複雑化によるユーザの学習負担の増加

2.3 代替認証として最適な知識情報

知識情報とは言わずもがな人間の記憶に大きく依存するものであるが, 認証要素として用いる場合には, それが長期記憶となっている必要がある. 一般的にパスワードはそれを入力するときのみ意識するものであるが, 秘密情報の復習のタイミングが不規則であり, 完全に忘却してしまうリスクがある.

一方で, 復習が無意識的かつ頻繁に行われるような秘密情報を認証要素として用いれば, パスワードを利用する場合と比較して忘却のリスクが低下する. また, そのような秘密情報は知識情報の中でも忘却しにくく, 代替認証として最適な認証要素になると考えられる.

3 スマートフォンのホーム画面を用いた代替認証手法の提案

3 章では, スマートフォンのホーム画面を用いた代替認証手法の提案について説明する. 3.1 節では, 提案する認証手法の概要について, 3.2 節では不正解の選択肢として用いるダミー画像について, 3.3 節では提案する認証手法の安全性について述べる.

3.1　提案する認証手法の概要

2 章の内容を踏まえ, 認証要素としてスマートフォンのホーム画面を用いた認証手法を提案する. スマートフォンにおけるホーム画面は毎日の閲覧によって, 無意識的かつ頻繁に復習がなされ, 長期記憶として定着している可能性が高い. また, レイアウト, 入手アプリケーションには個人の特徴が現れる. これらの性質からスマートフォンのホーム画面は, 代替認証で用いる認証要素として有用であると考えられる.

本提案手法の大まかな手順を以下に示す. ユーザが設定しているホーム画面のページ数を m 枚とし, 各ページに対する提示画像枚数を n 枚とする. (n, m は自然数)

提案手法の手順

1. 認証開始画面が表示され, ユーザが認証を開始すると 1 枚のホーム画面の画像が表示される（図 1）.
2. ユーザは表示された画像が自身のホーム画面であれば「はい」をタップ, そうでなければ「いいえ」をタップする.
3. n 枚の中から 1 枚選ぶ処理を, m 回繰り返す.
4. ここまででユーザが, 「はい」をタップすることで選択した画像が全て正解画像であれば認証成功となる. そうでなければ 1 回目の認証失敗の場合は認証失敗となり, 2 回目の認証失敗の場合は, これ以上認証出来ませんと表示される.
5. 認証失敗となった場合, それが 1 回目の認証であるときのみ, 再度認証開始画面に戻る（図 1）.

本提案手法は, 認証要素としてスマートフォンのホーム画面を用いるため, Android と iPhone の両者共に認証手法としての働きが期待できる. しかし, ホーム画面のレイアウトにある程度規則性が見られる iPhone と比較して, 機種が多岐に渡り, かつホーム画面のレイアウトの規則性が乏しい Android におけるダミー画像生成は, 非常に困難であると考えられる. よって, 本研究ではまず初めに iPhone アプリケーションとしての認証手法の提案を行っていく.

図 1 1 枚のホーム画面の画像

3.2　不正解の選択肢として用いるダミー画像

当認証手法では, 不正解の選択肢として用いるダミー画像が必要である. また, それらのダミー画像がそれぞれ独立している必要があり, ホーム画面の独立性を分解すると以下の 2 点に大別されると考えられる.

①ホーム画面上のアプリケーションの種類
②ホーム画面上のアプリケーションの配置

①,②を考慮したダミー画像について以下に述べる.

ダミー画像に含まれるアプリケーションと, ユーザのホーム画面上のアプリケーションの関連度が低い場合, 攻撃者に見破られやすいものとなってしまう. なぜなら, 性別や年代によって入手アプリケーションには一定の偏りがあり [6], ユーザの容姿だけで十分な推測が可能となってしまうからである. また, [6] のようなランキングを参考にして性別と年代ごとにダミー画像を変化させたとしても, 攻撃者がユーザの親しい友人である場合, 「この友人は現在就職活動中であるから, 就職関連のアプリケーションを入手している可能性が高い」というような推測が可能となってしまう.

これらを踏まえ当認証手法では, ユーザのホーム画面上の入手アプリケーションをその画面内だけで並び替えたものをダミー画像として採用する. これにより, ホーム画面のアプリケーションの種類を変化させることなくダミー画像を作成することができ, ①の独立性を保つことが可能となる.

ホーム画面上のアプリケーションの配置構成 [7] は, ユーザによって千差万別であると考えられる. 使用頻度の高いアプリケーションを右手親指でタップしやすい位置や, 認識しやすくするために画面の角に配置するなど, レイアウトを工夫しているユーザは散見されるが, 全ユーザに当てはまる規則性とするには弱く参考になるデータも乏しい.

一方で, iPhone のホーム画面下部にはドックと呼ばれる帯部が搭載されており, ドックに使用頻度の高いアプリケーションを固定するという行為は一般的であると考えられるため, 当認証手法ではドックの部分を切り取ってダミー画像を作成することとした. また, ドック部分に含まれないホーム画面上のアプリケーションをランダムに並び替えることによって, ②の独立性の保持を図った. なお, ダミー画像に含まれる壁紙は, ユーザと同一の壁紙で統一することとした.

ホーム画面 1 ページあたりにおけるアプリケーションの配置可能数の最小値を s, 最大値を t とし, 作成可能なダミー画像のバリエーション数を X とすると, X の範囲は以下の式 (1) のようになる.

$$s! \leqq X \leqq t! \tag{1}$$

3.3 提案する認証手法の安全性

本提案手法の安全性は, ホーム画面のページ数および正解画像選択画面における選択肢の数によって求められる. ユーザが設定しているホーム画面のページ数が m であり, 各ページそれぞれに対する提示画像枚数が n であるとすると, 1 回の認証における当認証手法の安全性は式 (2) のようになる.

$$\left(\frac{1}{n}\right)^m \tag{2}$$

4 スマートフォンのホーム画面を用いた代替認証手法の構築

4 章では, スマートフォンのホーム画面を用いた代替認証手法の構築について説明する. 4.1 節では, 構築環境について, 4.2 節では, システムの構成について, 4.3 節では, Xcode での開発について述べる.

4.1 構築環境

今回, 構築環境は表 2 に示す. iPhone のアプリ開発は, Swift と Xcode 用いるのが一般的である. よって, プログラミング言語は Swift を用いて, 開発環境は Xcode を利用する.

表 2 構築環境

PC	macbook air
OS	macOS Big Sur
メモリ	4GB
開発ツール	Xcode12.2
プログラミング言語	Swift5.2.5

4.2 システムの構成

図 2 にシステムの構成について示す.

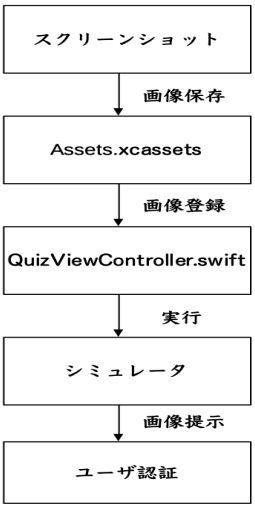

図 2 システムの構成

スクリーンショットを用いて抽出した画像を, 画像ファイルの Assets.xcassets に保存する. Assets.xcassets に保存した画像を, QuizViewController.swift のプログラムに登録する. 画像が登録されたプログラムを実行し, シミュレータを起動させる. よって, ユーザはシミュレータに提示された画像を見て認証を行う.

4.3 Xcode での開発

図 3 に認証の正誤判断プログラムを示す. なお, このプログラムは, 画像に関する問題が 50 個出された場合のものである.

```
import UIKit
var fcount = 0
class ScoreViewController: UIViewControl
ler {
  var correct = 0
  @IBOutlet weak var scoreLabel: UILab
  el!
  override func viewDidLoad() {
  super.viewDidLoad()
  if (correct == 50 ){
  scoreLabel.text = "認証成功"
        }
  else if(f_count == 0 ){
  scoreLabel.text = "認証失敗1回目"
  fcount = fcount + 1
        }
  else if(fcount == 1){
  scoreLabel.text = "これ以上認証出来ません"
  fcount = fcount + 1
        }
    }
   }
  }
```

図 3 認証の正誤判断プログラム

5 スマートフォンのホーム画面を用いた代替認証手法の実験

5 章では, スマートフォンのホーム画面を用いた代替認証手法の実験について説明する. 5.1 節では, 実験の手順について, 5.2 節では, 実験結果について, 5.3 節では, 考察について述べる.

5.1 実験の手順

情報系学部所属の学生 7 名による認証実験[*1]を行った. 認証に用いる正解画像として, 各ユーザの主観で最も使用頻度が高いと思われるホーム画面 1 ページを採用した. 3.1 節の提案手法の手順において $n = 50, 40, 30, 20, 10$ と変

[*1] 実験は南山大学研究審査委員会の審査の上, 個人情報保護に十分配慮し実施した

動させ, $m = 1$ に固定した. それぞれの場合における認証成功の可否および認証開始から認証終了までに要した時間を調査した.

また, 本提案手法では, 3.2 節の式 (1) において $s = 8$, $t = 24$ として実験を行った. $s = 8$ とした理由は, バリエーション数を最低 10000 以上確保することと, ホーム画面上のアプリケーションの 3 分の 1 に当たるからである. $t = 24$ とした理由は, 現在 (iOS14 時点) のホーム画面 1 ページあたりにおけるアプリケーションの最大配置可能数が 24 であるからである.

したがって, 本提案手法ではホーム画面 1 ページあたりの入手アプリケーション数が 8 以上のユーザである, という制約を設ける必要がある. 以上を踏まえると, 本提案手法におけるダミー画像のバリエーション数は以下の式 (3) のようになった.

$$8! \leqq X \leqq 24! \tag{3}$$

5.2 実験結果

表 3 に画像提示枚数別の認証成功人数および平均認証所要時間を示す.

表 3 画像提示枚数別の成功人数および平均所要時間

提示枚数 (枚)	成功人数 (人)	平均所要時間 (秒)
10	7	13.8
20	7	25.2
30	7	33.5
40	7	40.4
50	7	100.6

今回, 画像提示枚数である n を $n = 50, 40, 30, 20, 10$ と変動させ実験を行った結果, 全ての場合において 7 名全ての被験者が正解画像の選択に成功した. また, 画像提示枚数は平均認証所要時間と比例する傾向が見られた.

5.3 考察

今回の実験を通して, 被験者が認証に失敗するという事象は見受けられなかった為, 20 代前半の理系学部生という条件の下においては, スマートフォンのホーム画面という認証要素自体の利用可能性を示すことができた.

また, 画像提示枚数が 40 枚から 50 枚にかけての平均認証所要時間が 2 倍以上となったことから, ユーザの負担が著しく増加することが読み取れ, 今回の実験の条件下における適切な画像提示枚数は 40 枚付近であることがわかった.

実験に併せて各被験者それぞれにおけるホーム画面の合計ページ数を調査したところ, 7 名の平均ページ数が約 4.3 枚であることがわかった.

以上を踏まえると, 本提案手法で想定される安全性の一例は以下の式 (4) のようになった.

$$\left(\frac{1}{40}\right)^4 = \frac{1}{2560000} \tag{4}$$

一方, 今回の実験で用いた正解画像は, ユーザの主観で最も使用頻度が高いと思われるホーム画面 1 ページであり, それ以外のページについては記憶が曖昧になっている可能性がある. これを踏まえると, ホーム画面の全てのページにおける適切な画像提示枚数が 40 枚付近であるとは断言できない為, ユーザのホーム画面のうち使用頻度の低いページにおいても同様の実験を行い, 本提案手法の有効性を検討する必要がある.

また, ページ表示時間と画面接触時間を記録し, 注視の度合いを注視継続率として算出するといった手法 [2] を組み合わせることができれば, ユーザの注視継続率に応じて画像提示枚数を変動させるような機能が実現できると考えられる.

6 むすび

本研究では, 認証要素として知識情報の中でも比較的忘却しにくいと考えられる, スマートフォンのホーム画面を用いた代替認証手法を提案した. 5 章で示した通り, 画像提示枚数別の認証成功人数および平均認証所要時間の調査を通して, 一定条件下におけるスマートフォンのホーム画面という認証要素自体の利用可能性を示すことができた.

参考文献

[1] 安齋将之, 小倉加奈代, ベット B. ビスタ, 高田豊雄, “スマートフォンにおけるアプリの利用時間を用いたフォールバック認証手法の検討,” 第 80 回全国大会講演論文集, Vol.2018, pp. 501-502, 2018.

[2] 飯澤悠介, 中村嘉隆, 稲村浩, “ブラウザの Web ページ閲覧履歴に基づくスマートフォン端末向け画像認証方式の検討,” 第 80 回全国大会講演論文集, Vol.2018, pp. 375-376, 2018.

[3] 増井俊之, “EpisoPass: エピソード記憶にもとづくパスワード管理,” コンピュータセキュリティシンポジウム 2013 論文集, pp. 933-940, 2013.

[4] 稲村勝樹, 新林直樹, “改良型パターンロック覗き見耐性向上手法の提案と評価,” 情報処理学会論文誌, pp. 179-188, 2018.

[5] 日立ソリューションズ, https://www.hitachi-solutions.co.jp/security/sp/column/authentication/02.html , 参照 Sep9, 2020.

[6] [2019 年版] 男女×年代別 実際によく使われているアプリランキング, https://manamina.valuesccg.com/articles/526, 参照 Sep9, 2020.

[7] [日本一] 41 名の iPhone ホーム画面を晒してみた！ 1148 個のアプリがここに！, https://appleshinja.com/iphone-home, 参照 Sep9, 2020.