2V-08

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

飯澤悠介[†1]　中村嘉隆[†1]　稲村浩[†1]
公立はこだて未来大学 システム情報科学部[†1]

1. はじめに

スマートフォン端末の普及につれ，対応サービスが増加し，重要な個人情報が端末内に保存されるようになった．それに伴い，他者の不正利用による情報漏洩を防ぐため，端末自体の保護に対する重要性も増してきている．一般に端末保護の安全性と端末利用の利便性はトレードオフの関係にあり，これらを考慮した端末保護手法が必要となる．

現在は，「固定式パスワード認証」や，「パターン認証」を用いた端末保護手法が主流である．これらの手法は安全性を向上させるために複雑なものを用意するほど，端末利便性が低下するという問題がある．また，一部のスマートフォン端末には身体の部位を利用した生体認証が導入されている．生体認証は利便性が高い反面，一度認証用の生体情報が流出すると，他者による不正利用を防ぐことが困難になる．例えば，スマートフォン端末には指紋認証が多く搭載されているが，指紋を複製する方法が存在しており，認証の安全性に対する脅威となっている．本研究では利便性と安全性の両者を満たしたスマートフォン端末向け認証方式の実現を目的とする．

2. 関連研究

2.1 利便性と安全性へのアプローチ

利便性向上に向けたアプローチとして Dhamija, R ら[1]や高田ら[2]らの画像認証がある．画像認証とは何枚かの画像を提示し，その中から利用者が設定した画像を選択することによって認証を行う．人間が文字より認識しやすい画像を選択する再認方式を用いることで利便性の向上が望める．安全性向上に向けたアプローチとして西垣ら[3]や Ngu ら[4]の個人の生活に関わる履歴情報を用いた認証がある．他人には把握することが困難で，生活の中で常に変化する情報を用いることによって安全性の向上が望める．

2.2 スマートフォン端末への画像認証適応時の課題

スマートフォン端末で用いる際に生じる課題として以下の 3 つが挙げられる．

① 提示画像の抽出対象の決定
② 正解画像・不正解画像の決定
③ 提示画像の選出

An image based authentication method on Webpage browsing history for smartphone
†1 YUSUKE IIZAWA, YOSHITAKA NAKAMURA and HIROSHI INAMURA, School of System Information Science, Future University of Hakodate.

3. 提案手法

3.1 各課題に対してのアプローチ

課題①に対しては，利用者個人の自発的行動であり，行動の想起が容易であると考えられる Web ブラウザの閲覧に着目し，閲覧履歴に含まれる画像の抽出を行う．課題②に対しては，コンテンツのレイアウトやテキスト情報が含まれるほうが想起しやすいため，Web ページ全体のスクリーンショットを提示画像として用いることとする．課題③に対しては，関心のある内容は記憶に残りやすい特性に従い，利用者の閲覧履歴に残る画像を正解画像，利用者の閲覧したことのない画像を不正解画像とする．

3.2 提案システム構成

提案システム構成を図 1 に示す． Web ページを閲覧する度に取得したデータをスマートフォン端末内の BrowserDB に蓄積する．利用者が端末を起動後，正解画像 Web ページ URL と複数の不正解画像 Web ページ URL を取得し, スクリーンショットを抽出, 画像保存領域に保存し，認証画面に提示する．利用者は提示画像群の中から正しく正解画像を選択することで認証成功となる．認証成功後に閲覧行為をした場合，提示画像群が更新され，正解・不正解画像ともに閲覧履歴に基づいて画像を変化させることで利用者の画像登録の負担を軽減する仕組みとなっている．

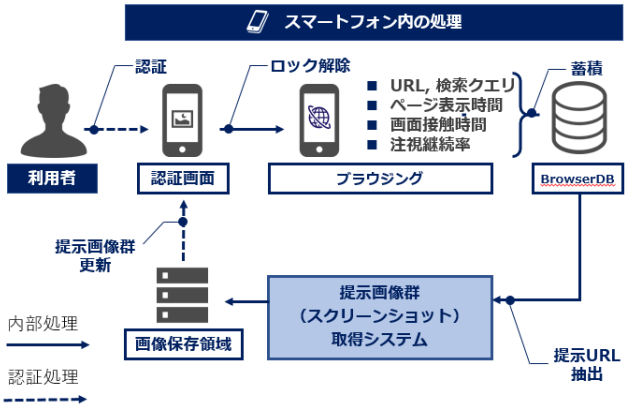

図 1 提案システム構成

3.3 正解画像の選出

ブラウザを用いて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．最も注視継続率が高い Web ページを正解画像 Web ページ URL として抽出する．Web ページp_iごとのページ表示時間rp_iと画面

接触時間tp_iを用いて注視継続率gc_iは以下の式で求める．

$$gc_i = \frac{tp_i}{rp_i}$$

3.4 不正解画像の選出

図 2 に不正解画像となる Web ページ URL 抽出までの流れを示す．正解画像となる Web ページを閲覧したときと同一の検索クエリの閲覧済み Web ページの URL を BrowserDB から取得する．次に，正解画像の検索クエリの検索結果から 30 件程度の URL を抽出する．閲覧済み URL と検索結果から抽出した URL からドメインを抽出し，閲覧済み URL と同一のドメインを含まない Web ページ URL を不正解画像抽出用の Web ページ URL として抽出する．

図 2 不正解画像 Web ページ URL 抽出の流れ

4. 基礎実験

基礎実験として，客観的な注視継続率という計測方法で選択した正解画像を，不正解画像を含む画像群から正しく選択可能かを調査した．被験者は公立はこだて未来大学システム情報科学部の男子学生 5 名(A~E)である．典型的な検索動作を行わせるため，被験者にまず検索するキーワードを決めてもらった．以下の手順でキーワードに関する内容の Web ページ閲覧を 10 分間行ってもらった．

- Web ページのロード終了後にコンテンツの閲覧を行う
- Web ページのコンテンツを閲覧する際は画面に親指を接触させたまま閲覧する

検索終了後，正解画像 1 枚と不正解画像 3 枚が表示される認証画面に移ってもらい閲覧した画像を選択してもらった．この 1 通りの動作を被験者 1 人に対して 3 セッション行ってもらった．

5. 実験結果・考察

実験の結果を表 1 に示す．全被験者合わせて 15 回のうち 13 回が正しく正解画像を選択することが出来ている．したがって提案手法は認証に使用できる可能性があるといえる．被験者 B の 2 回目と被験者 D の 1 回目のみ失敗しているが，後にヒアリングを行った結果，被験者がよく閲覧していた部分がスクリーンショット画像に表示されていないことがわかった．これについては Web ページ内でどの部分を注視していたかなどを分析することにより，選択成功確率を向上させることが可能であると考えられる．また，選択には成功しているものの，多く被験者が正解画像の選択まで時間がかかる傾向が見られた．実験後のヒアリングの結果，被験者のほとんどが消去法で正解画像を選択していることがわかった．具体的には，不正解画像を見て「これは違う」「これは見た記憶がない」と排除していくことで正解画像を選択しているという事である．原因としては正解画像の検索クエリを使用して不正解画像を取得していたので，不正解画像と正解画像の類似度が高くなり，記憶の混同が発生してしまったと考えられる．この問題は不正解画像で検索するクエリを正解画像のジャンルから離すことで改善可能であると考えられる．

表 1 セッションごとの被験者の選択結果

		被験者				
		A	B	C	D	E
セッション	1	成功	成功	成功	失敗	成功
	2	成功	失敗	成功	成功	成功
	3	成功	成功	成功	成功	成功
成功数		3	2	3	2	3

6. 最後に

本稿では，認証のための正解画像を閲覧した Web ページから利用者の注視行動を基に取得，不正解画像を利用者の閲覧していない Web ページから取得することにより，利便性と安全性の両立を図った． 本稿では，提案手法について評価実験を行い，認証手法として利用できる可能性を示した．

今後の課題として，利便性向上のための不正解画像選出についての改善策の検討，提示方法の検討，覗き見攻撃など想定される攻撃に対しての安全性の評価を行う．また，提示画像に対する他者の不可視対策も検討する．

参考文献

[1] Dhamija, R., and Perrig, A. : Deja Vu: A User Study Using Images for Authentication, Proc.9th conference on USENIX Security Symposium(SSYM'00), pp. 45-58 (2000).

[2] 高田司，小池英樹 : あわせ絵 : 画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法，情報処理学会論文誌，Vol. 44, No. 8, pp. 2602-2612 (2003).

[3] 西垣正勝，小池誠 : ユーザの生活履歴を用いた認証方式 -電子メール認証システム，情報処理学会論文誌，Vol. 47, No. 3, pp. 945-956 (2006).

[4] Ngu, N., and Stephan, S.:PassFrame: Generating image-based passwords from egocentric videos, 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp46–49(2017).