スクロールとスライド操作による携帯端末向け個人認証

森 康洋[1,a)]　高田 哲司[1,b)]

概要：本研究では、携帯電話向けの画像認証の改良について報告する．画像を用いた個人認証は知識照合型個人認証の問題点である記憶負担を軽減しうる手法として提案されているが、その効果が最大限得られる手法においては安全性が不十分になる傾向があるという指摘がある．これに対して本論文では，4 つの工夫を適用することにより，その安全性を向上させるとともに、その改善にともなう記憶負担や操作負担の増加を最小限に抑制しうる案を考案した．このアイデアを基にした改良版画像認証をプロトタイプとして実装したので，本論文で詳解するとともに、４つの工夫がどのようにして安全性の向上と副作用として発生しうる記憶負担および操作負担の増加を抑制しうるかについて議論する．

Recognition-based Image Authentication for Mobile Phone with Scroll and Slide Operation

Yasuhiro Mori[1,a)]　Tetsuji Takada[1,b)]

Abstract: We report on some ideas to improve a recognition-based image authenticaiton scheme for smart phone users. A recognition-based image authentication was proposed for decrease a memory load of the secrets on a knowledge-based user authentication users. However, a security of the scheme is not enough for some cases. We consider four ideas to improve a security of the scheme without increasing a load on a secret memory and an input operation. And we also implemented a prototype system based on the ideas. We describe about the ideas and prototype system. We also explain how these ideas make possible to improve the security with a reasonable usability issue.

1. はじめに

現在，知識照合型個人認証が様々な場面で利用されている．この手法の欠点は，秘密情報を記憶保持し，認証時に誤りなく入力できなければならない点にある．しかしこの秘密情報には，安全性維持のため記憶保持を困難にする可能性の高い以下のような制約が設けられていることが多い．

- 辞書に存在する単語とその定型的変形語の利用禁止
- 容易に推測されうる情報の利用禁止
- 複数のサービスでの同一秘密情報の使い回し禁止

したがって，多くの利用者はその履行が難しく，所有物認証や生体認証の利用、またはパスワードマネージャなど記憶負担を軽減する手法の適用が検討され始めてている．

[1] 電気通信大学
The University of Electro-Communications
[a)] m1110146@edu.cc.uec.ac.jp
[b)] zetaka@computer.org

この知識照合型個人認証の記憶負担に関する改善策として，画像を用いた個人認証が提案されている．これは文字等の記号列を秘密情報にするかわりに画像を利用した記憶照合型の個人認証手法である．しかし，これらの手法も実用に至っていない．画像を用いる最大の理由は秘密保持負担の改善であるが，実際にその効果が最も期待できるのは，以下の三カテゴリーの画像認証のうち、3) の再認手法であると言われている [5].

1) Drawmetric (描画手法)
2) Cued-recall (手がかり付き想起手法)
3) Recognition (再認手法)

一方、再認式画像認証の問題点は理論的安全性が低いという点である．それを改善するためは、次の３つの方法がある

a) 秘密となる画像枚数を増やす
b) 画像の順序を秘密情報とする

c) 回答選択時の選択候補となる画像枚数を増やす

このうち a) は純粋に記憶負担を増加させることになるため採用しない．b) も記憶負担を増やす懸念はあるものの，総当たり攻撃への安全性改善の他に推測攻撃に対する改善効果も見込めるためその応用を検討する．そして c) は利便性に影響を及ぼす懸念があるものの，スマートフォンでの利用を想定すれば，操作手法を工夫することによりその影響を最小限にとどめることが可能だと考えた．

そこで本研究では，一覧表示された多数の選択肢からまず候補を絞り込み，次に絞り込まれた選択肢の中から秘密になっている画像を入力するという 2 段階の操作による個人認証を提案する．またこの認証手法の想定状況をスマートフォンやタブレットとし、入力操作にスクロールとスライドによる操作を導入することで負担増加を最小限に抑えることを可能にする個人認証手法を提案する．

2. 関連研究

人間の記憶には以下のような特性があるといわれている [1].

(1) 思い出したことを再現するよりも，提示された項目の中から記憶しているものを選ぶほうが容易であるということ．
(2) 文字列よりも画像の方が記憶しやすいということ．
(3) 出来事に関する記憶は長期記憶に分類され，特にその中でも自身の思い出の記憶はイメージと情緒を伴い忘れにくいということ．

そしてこれらの特性は，記憶性の改善を目指すうえで重要なものである．

この特性のうち (1),(2) に基づいた手法として，Dhamija らが提案した Déjà Vu[6] がある．この手法は，一覧表示したランダム画像から秘密情報として設定した複数間の画像を順不同で選択する，というものである．しかし，画像とはいえ使用しているランダムアート画像はユーザに馴染みのないものであり，記憶性を充分に向上させているとは言い難い．

また別の認証手法として，村松らの研究 [8] がある．村松らの手法は，ユーザが撮影した写真を一覧表示し，それを時間順順に並び替えさせるというものである．これは，一覧表示されたものを認識して行う点，画像を用いる点，その画像がユーザにより撮影されたものであるという点が，それぞれ上述した人間の記憶の特徴の三つに当てはまっている．しかしこの手法では，使用できる画像の種類が写真だけであり，並び替えの順序も時間順に固定されている．これはユーザが自分に合わせた秘密情報を作成することを阻害し，結果として記憶性を損なっていると考える．

3. Scroll & Slide 認証

3.1 概要

提案手法は、タッチスクリーンが装備された携帯端末向けの画像認証システムである．ここではニーモニック認証 [2] を基本とし，この手法の拡張として新たな手法を提案する．提案手法では以下の拡張を試みる．

(1) 安全性向上
 (1.1)対総当たり攻撃
 (1.2)対推測攻撃
 (1.3)対覗き見攻撃
(2) 記憶負担増加の抑制
(3) 操作負担増加の抑制

上記の拡張を試みるために、本研究で考案した手段は以下の通りとなる．

- 好きな画像集合を秘密情報として利用可
- 好きな順序付けを秘密情報として利用可
- 回答操作の 2 段階化
- スクロールとスライドによる入力操作

本論文では提案する認証手法を Scroll and Slide 認証 (以降、SS 認証とする) と名付けた．次節では SS 認証の利用方法について述べる．

3.2 利用手順

3.2.1 秘密情報設定処理

SS 認証における秘密情報の設定処理について説明する

1) 100 枚の画像をユーザに用意させる．この画像群を認証システムに登録する
2) 登録画像をシステムを通じてい提示し，その中から秘密とする画像を回答順とともに秘密情報として設定する．秘密情報の画像枚数は対象とするシステムが要求する安全性に応じて決定する．一例を示す．秘密情報として画像 3 枚を選択した場合、理論的安全性 (総当たり攻撃に対する安全性) は 1/970,200 (およそ 20bit) となる．ちなみに 4 桁暗証番号認証の理論的安全性は 1/10,000 で、およそ 13bit となる

3.2.2 秘密情報入力処理 (認証処理)

秘密情報の入力操作は以下の 2 step からなる．

Step 1)回答候補画像の絞り込み

利用者により登録された 100 枚の画像から 25 行 × 4 列の縦長長方形になる画像グリッドを生成する．これをスマートフォンの画面上に提示して利用者に操作させるが，スマートフォンの画面には一度に 4 行 × 4 列分の画像しか表示されないものとする．つまりスマートフォンの画面上には画像グリッドの一部分しか一度には閲覧できないことになる．

この状況を利用し，本 step では画像グリッドの中から

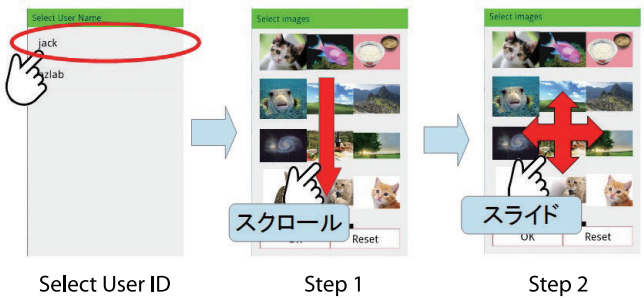

図 1 秘密情報入力処理の 2 steps

自分の秘密情報である画像がすべてスマートフォン画面内に表示されるように画像グリッドの表示領域を移動させる．画像グリッドはユーザの操作によって縦方向スクロールできるようになっており，また秘密情報となっている画像群は 4 行 x 4 列の表示領域の中に必ず入るようにシステムによって画像グリッド内に配置される．したがって認証利用者は，画像グリッドをスクロールして上記の要件を満たすように操作し Step 2 で操作する画像群を確定をする．これにより 100 枚の画像グリッドから，操作対象画像が 16 枚に絞り込まれたことになる．

Step 2)秘密画像の入力

Step 1 により操作対象画像は 16 枚となり，スマートフォン画面に一覧可能なかたちで表示される状況となった．これはニーモニックガード [2] と同一状況である．次に SS 認証ではグリッド機構を用いた間接選択による秘密画像の入力を行う．この原理は grIDsure[3] や SecureMatrix[4] と同じである．

認証画面は仮想的に 4 行 × 4 列の格子があると仮定し、その格子のうち、事前に決定しておいたマスに秘密画像が表示されるように 4 x 4 の画像群を縦横にスライドさせる．秘密情報指示用のマスの位置は事前に決定しておく．マスの数は 1 つから秘密画像枚数個まで自由に決定できる．またこのマスは秘密情報として記憶してもらっても良いが，それは強制ではなく認証操作中でなければ変更可能とする．ただし覗き見攻撃への効果を確かにするため，以下の 2 点は担保する．

1) 過去の選択用マスの位置を知ることはできない
2) 選択用マスの位置を変更してから，それが認証操作で実際に使用可能になるまでには若干の時間差を設ける．

これらはどちらも覗き見攻撃を安易に成立させないための配慮である．1) を要件とする理由は、一連の認証操作を動画として攻撃者に録画された場合を想定した対策である．2) の要件は時間差を設けないと、その場で選択用マスの位置決定と認証操作の双方を行い、それを攻撃者に覗き見される懸念があるからである．

4. 考察と今後の課題

3.1 節で述べた目指す拡張について，上記の仕組みでどうしてそのような効果が見込めるかについて述べる．また今後の課題についても述べる

1) 安全性向上

1.1) 対総当たり攻撃

総当たり攻撃への安全性が増える根拠は二つある．一つは秘密情報に順序が含まれる点である．これはニーモニックガードと同じ理由であるが，使用する画像種と順序付けについて一切の制約を置かないこととした．これにより利用者が自身で個人認証に最も好ましいと思う画像をシステムに登録し、そして記憶が可能な順序付けを自由に行うことになる．これは記憶負担への影響を最小限にしうると考える

もう一つは、回答操作が 2 段階になっている点である．100 枚の画像から 16 枚に絞り込む過程はニーモニックガードとは異なる点であり，本論文での設定条件だと Step 1 の操作で最大 25 の選択肢が見込めるため、その分だけ理論的安全性は増加することになる．

2.2) 対推測攻撃

これは秘密情報に順番が含まれることにより担保されると考える．画像を単純に秘密情報として利用し，順不同での回答を認めると．この攻撃に対して脆弱になる可能性がある．これに対して，順序が秘密に含めることでこの懸念は減少できると考える．また認証に利用する画像集合をすべてを利用者によって選択または撮影された写真にすることで、本攻撃を困難にする効果もあると推測している．

2.3) 対覗き見攻撃

これは Step 2 のグリッド機構による間接選択手法を導入したことにより担保されうる安全性である．秘密画像を直接選択するかわりに、秘密画像をグリッド内の特定のマスにあわせるという操作によって、選択用マスの位置を知らない攻撃者は入力画像の特定が困難になる．結果として，覗き見攻撃によって第三者に入力値が特定され，悪用される懸念が減ることになる．またこの選択用マスの位置は、厳密には秘密とせず、適宜更新可能にしている．これにより、秘密情報の記憶負担を不用意に増大させないように配慮する．

2) 記憶負担増加の抑制

本認証手法を利用する上で、利用者が記憶すべき情報は次の通りである．

- 秘密画像群とその回答順序
- 秘密画像選択用マスの位置

これらのうち、後者の情報は使い捨て可能である．したがって、秘密情報として厳密に記憶保持が求められるものではない．結果として，記憶負担については、ニーモニッ

クガードと同程度である．しかし画像種と順序付けにかかわる制約を取り払うことにより記憶負担に変化が見られるかどうかについては今後検証を行いたいと考えている．

3) 操作負担増加の抑制

ニーモニックガードと比較して回答操作は 2 Steps になるため操作負担は増加する．しかし、スマートフォンを利用するユーザにとって縦スクロールや画像グリッドのスライド操作は、タイピング操作と比較して軽微な部類の操作になるのではと推測している．また認証操作において利用者が待たされたり、計算や思考を要求される処理はない．したがって、利用者が感じる負担は想像されるほど大きなものにはならない可能性があると考えている．この検証については今後の課題である．

4.1 今後の課題

今後の課題は、被験者実験により上記の仮説が成り立つかどうかを検証することにある．以下にあらためて整理する．

- 記憶負荷評価
  利用可能な画像種ならびに順序付けに関する制約を取り払うことで記憶負担に変化が見られるかどうかについて検証する
- 安全性評価
  推測攻撃と覗き見攻撃に関して、安全性が担保されるかについて検証する
- 操作負荷評価
  認証操作にかかる操作時間ならびに利用者が感じる操作負担について検証する

5. おわりに

本研究では，知識照合型個人認証の改良として再認方式の画像認証を取り上げその改善を目指した手法として Scroll and Slide 認証を提案したこの手法では，ニーモニックガードを基礎とし、いくつかの工夫を施すことにより安全性を向上させつつ，それにともなう記憶負担や操作負担を増大させないような手法を考案した．

今後はプロトタイプシステムを利用して被験者実験を実施し、想定されている拡張が実現されるかどうかを検証する予定である．

参考文献

[1] 桝野隆平：パスワードの脆弱性と対策－認知心理学の知見を生かして，情報処理学会研究報告.CSEC，Vol.49，No.9，pp.1-6 (2010).

[2] Mnemonic Security Inc.，最強の本人認証ソフトウェア ニーモニックガード，http://www.mneme.co.jp/mne/index.html，(accessed 2014-12-19).

[3] S. Brostoff, P. Inglesant, and M. Sasse: Evaluating the usability and security of a graphical one-time pin system, in Proc. of the 24th BCS Interaction Specialist Group Conf. pp.88-97, (2010).

[4] 株式会社 CSE，SECUREMATRIX，https://www.cseltd.co.jp/products/smx/index.htm，(accessed 2014-12-19).

[5] Renaud, K., Mayer, P., Volkamer, M., Maguire, J.: Are grahphical authentication mechanisms as strong as passwords?, Computer Science and Information Systems (FedCSIS), pp.837-844, (2013).

[6] Dhamija, R. and Perrig, A.: *Déjà Vu: A User Study Using Images for Authentication*, 9th Usenix Security Symposium, pp.45-58 (2000).

[7] Davis, D., Monrose, F., and Reiter, M.K.: On user choice in graphical password schemes, In Proc. of the 13th conference on USENIX Security Symposium, USENIX Association, pp.11-11, (2004).

[8] 松村健児，黒岩丈介，高橋勇，小高知宏，小倉久和：エピソード記憶の時系列情報を利用したユーザ認証システム，福井大学工学部研究報告，Vol.53，No.1，pp.61-67 (2005).