

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

電気通信大学 森康洋, 高田哲司

— 背景と目的 —

知識認証の欠点:
秘密情報の記憶が困難
その改善手法の1つが画像認証

画像認証の分類

- 再生手法
- 手がかり付き再生手法
- 再認手法

再認手法(画像選択認証)

- 【利点】記憶しやすい
- 【欠点】安全性が低い

【既存手法(ニーモニックガード)】



- ・ 利用画像:
好きな画像を利用
- ・ 秘密情報:
順序付き画像群

同手法を利用

<http://www.mneme.co.jp/wm/index.html>

改善方法	問題点
秘密情報数を増やす	記憶負担増大
選択順序を設ける	
候補数を増やす	操作負担増大

採用

【目的】
理論的安全性を向上させつつ
負担増大を抑える

— 提案手法 —

【秘密情報】

- ・ 順序付き画像複数枚
- ・ 画像回答位置

【手順】

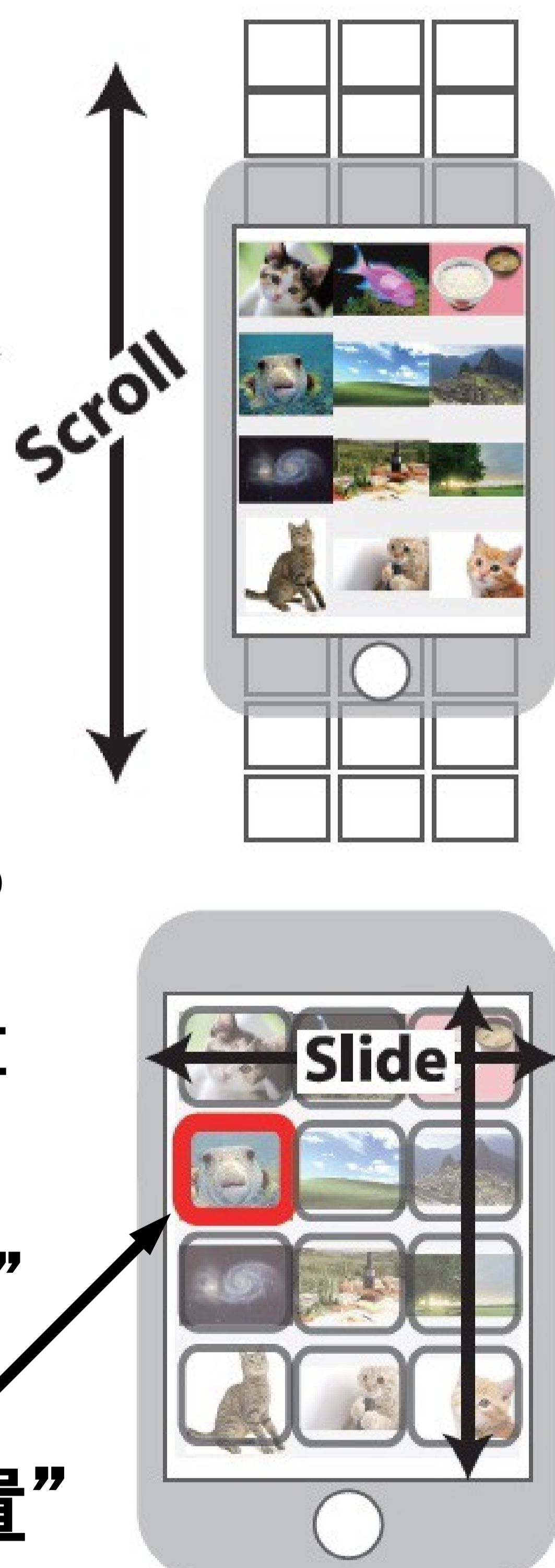
手順1. 回答候補決定

- 大きな画像群から
小さな画像群に
回答候補を絞り込む
- 画面に表示されている
画像が回答候補となる
- 正解画像は1画面に
表示される範囲に配置

手順2. 回答入力

- 回答画像を“回答位置”
に移動させて選択

“回答位置”



【安全性向上】

- ・ 順序付けを秘密情報とする
- ・ 回答候補数を増やす

【負担増への対策】

- ・ 好きな画像を好きな順序で
- ・ 回答操作の2段階化
- 大きな回答候補を絞り込む

【覗き見攻撃耐性向上】

- ・ スライドによる入力操作

【利点】

1. 理論的安全性の向上かつ
操作負担増加は最小限
2. 覗き見攻撃耐性あり
- 正解画像を間接選択するため
- 複数回の覗き見には耐性なし

— 評価結果 —

【記憶保持】

- 順序付き画像4枚で検証
- 1週間後に認証失敗
したのは7人中1人

【認証時間(平均)】

- 手順1: 3.304秒
- 手順2: 10.738秒
- 全体: 14.042秒

【安全性】

- ・ 理論的安全性: 581,400通り
- 100枚から20枚に候補を絞り
その後4枚の画像を順番に選ぶ
- ・ 推測攻撃成功率
- 画像一致: 4/25
- 完全一致: 1/25