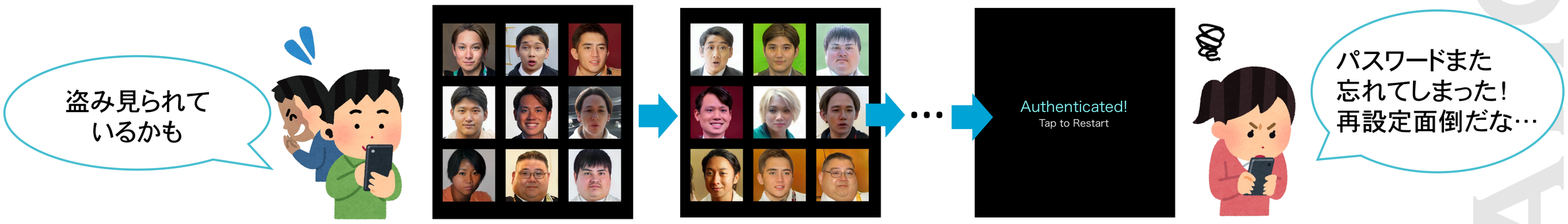
SecHack365

盗まれにくく、忘れにくい 面影の選択による認証手法

おもかげパスワード

研究駆動コース
35R 村上あさひ

おもかげパスワードとは



これを解決するのが…おもかげパスワード!!!

のぞかれても盗まれにくく、忘れることがない新しい個人認証システム

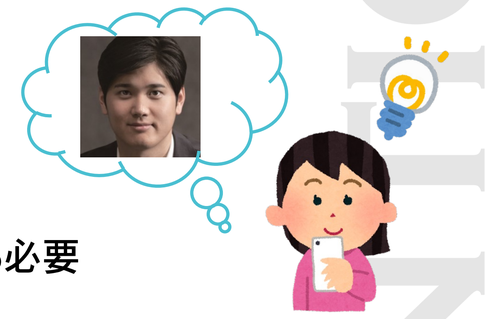
のぞかれても盗まれにくいヒミツ

パスワード顔画像そのものではなく
「おもかげ画像」のみを提示
4回認証画面が提示され、
表示される顔画像は毎回全て異なる


パスワード
顔画像

パスワード顔画像は表示されない
1回目と同じ顔画像はない

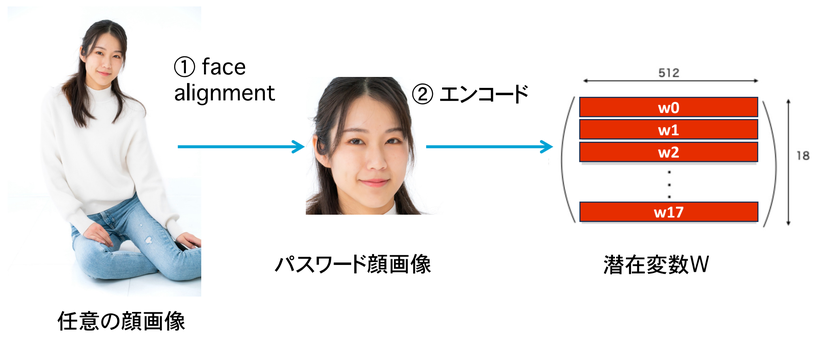
忘れることがないヒミツ



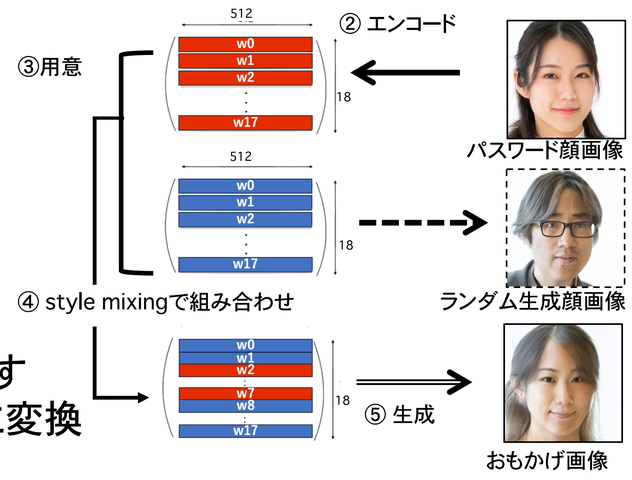
パスワード顔画像に設定した人の顔を
思い浮かべるだけで
認証問題を解くことができる
そのため、パスワードをわざわざ覚える必要
がなく、忘れる心配がない

https://www.airsleep.jp/ohtani/

おもかげパスワードの仕組み (StyleGAN)



① face alignmentで任意の顔画像の顔領域を切り出す
② エンコードで①をベクトルの集合である潜在変数Wに変換



③ ランダム生成顔画像の潜在変数を用意する
④ style mixingでベクトルを組み合わせて
新たな潜在変数を構成
⑤ 潜在変数からおもかげ画像を生成!
⑥ パスワード顔画像から生成されたおもかげ
画像を正解画像とする
⑦ それ以外のフリー画像の8枚の画像から
生成されたおもかげ画像を不正解画像とする
⑧ 認証画面に⑥と⑦を組み込み、完成

本当にのぞかれても盗まれにくい?

1 評価実験1

おもかげパスワードの使いやすさは?のぞかれても大丈夫?

・正規ユーザの役割(普通に使う人)
　パスワード顔画像を自由に設定、練習を行い、認証問題を3回解いてもらう
・非正規ユーザの役割(のぞいて盗む悪い人)
　他者が認証問題を解いている動画を見た後、同じ認証問題を3回解いてもらう
・実験参加者
　本システムを利用したことのない16名
　(情報系の理工学部14名 理工学部以外2名)(男性8名 女性8名)

	正規ユーザの認証成功率		非正規ユーザの認証成功率			
	全体	SUS	1回目	2回目	3回目	全体
全体	100.0%	66.3	37.5%	43.8%	56.3%	45.8%

	提案手法	図形	ランダムアート	顔画像	パスコード認証	パターン認証
認証成功率(正規)	100.0%	100.0%	100.0%	88.9%	100.0%	100.0%
認証成功率(非正規)	45.8%	27.8%	61.1%	50.0%	100.0%	72.2%

2 ユーザ調査

のぞき見耐性向上のために面影度合いを薄くしよう

・評価実験1から面影度合いを薄くしようと考えユーザ調査を行う
・しかし面影の認識は個人個人によって大きく異なった
　→ 一様に面影度合いを薄くすることはできない

3 評価実験2

個人個人に面影度合いをチューニングしてのぞき見耐性を向上させよう

・1人の実験参加者が認識可能な面影度合いにチューニング
・認証問題を解く動画を作成
・他の10人の実験参加者に動画を見てもらい、同じ認証問題を3回解いてもらう

正規ユーザの認証成功率	非正規ユーザの認証成功率			
全体	1回目	2回目	3回目	全体
100.0%	0%	0%	20.0%	6.7%

本当に忘れない?

おもかげパスワードの評価実験1に参加の16名のうち連絡のとれた
15名に同じ認証問題を解いてもらう(男性:7名、女性:8名)
評価実験から開いた期間は平均154日(5ヶ月弱)、標準偏差17日

段階	評価方法	評価結果
第1フェーズ	何も見せずに解いてもらう	13名
第2フェーズ	パスワードに設定した人の名前だけを教える	2名
第3フェーズ	設定したパスワード顔画像を見せる	0名
第4フェーズ	おもかげ画像を見せる	0名

長い期間空いていても全体の87%が何も見ずにパスワード顔画像を
思い出すことができたことから、覚えやすく忘れにくいことが言える

おもかげパスワードの社会実装

メーカーで製品セキュリティ部門の方と議論して得られた課題

おもかげパスワード独自の脅威:顔の類似度から機械が突破できる?

・機械が面影を識別できるかを顔画像間類似度を用いてミニマムに検証
・結果は、正解画像同士は比較的高い値であり、正解画像と不正解画像同士
　でも高い値を示すものもあった
→機械による突破の可能性が示唆されたことから、より深い検証をしていきたい

法的な観点から:実在する人物の顔画像を扱うことへの課題整理

おもかげパスワードの態様で実施されている場合は肖像権に対する侵害とは
考えられないというコメントを弁護士からいただいている
ただし、おもかげパスワードで使用する顔画像データの特徴点が個人識別
符号に該当し、個人情報として取り扱うことになるため、おもかげパスワードの
サーバ管理者は個人情報取扱事業者として対応する必要がある

今後は、小学校や専修大学無人コンビニプロジェクトを対象に社会実装を目指す

外部発表:コンピュータセキュリティシンポジウム(CSS2023)
「おもかげ」を用いた個人認証手法の提案と評価
村上あさひ・橋本俊甫・石川琉聖・神薗雅紀・服部祐一・猪俣敦夫・井上博之・石井健太郎

デモ公開中

NICT National Institute of Information and Communications Technology