Nish!gaki Laboratory

利便性と安全性を兼ね備えた画像認証方式の実現に向けて

山本匠[1,2]　西垣正勝[1,3]

[1] 静岡大学創造科学技術大学院
[2] 学術振興会特別研究員 DC
[3] 科学技術振興機構，CREST

パスワードの問題点

Nish!gaki Laboratory

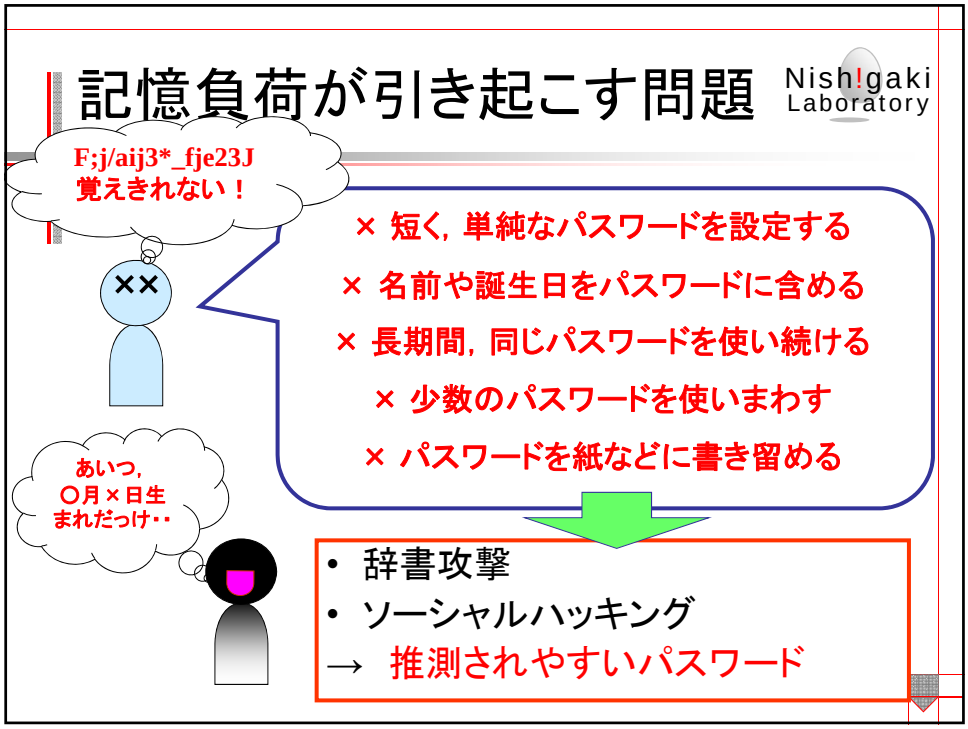
推測されにくいが覚えにくい

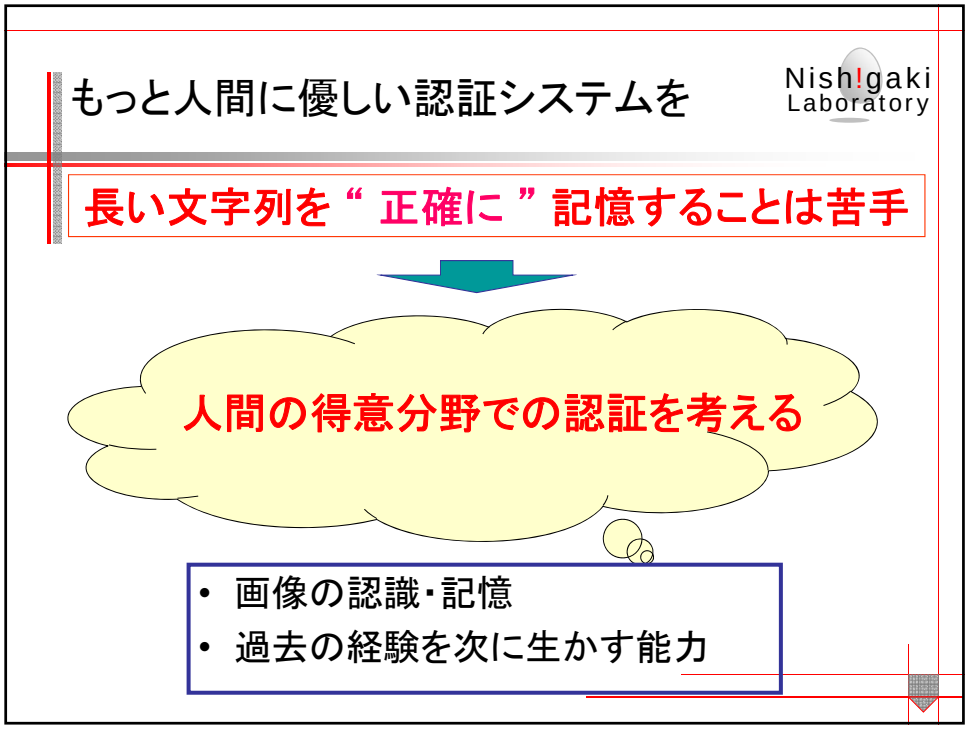
・文字数／桁数を多くする
・ランダムな文字列／数字列にする

記憶負荷に関する
利便性と安全性のトレードオフが存在

覚えやすいが推測されやすい

・文字数／桁数を少なくする
・意味のある文字列／数字列にする


記憶負荷が引き起こす問題
Nish!gaki Laboratory
F;j/aij3*_fje23J
覚えきれない！
××
× 短く，単純なパスワードを設定する
× 名前や誕生日をパスワードに含める
× 長期間，同じパスワードを使い続ける
× 少数のパスワードを使いまわす
× パスワードを紙などに書き留める
あいつ，
○月×日生
まれだっけ‥
• 辞書攻撃
• ソーシャルハッキング
→ 推測されやすいパスワード


もっと人間に優しい認証システムを
Nish!gaki Laboratory
長い文字列を“ 正確に ”記憶することは苦手
人間の得意分野での認証を考える
• 画像の認識・記憶
• 過去の経験を次に生かす能力

コンセプト

Nish!gaki Laboratory

人間は過去に解いた経験のある問題に
再度直面したとき，以前の経験から
初見のときよりも早く解くことができる

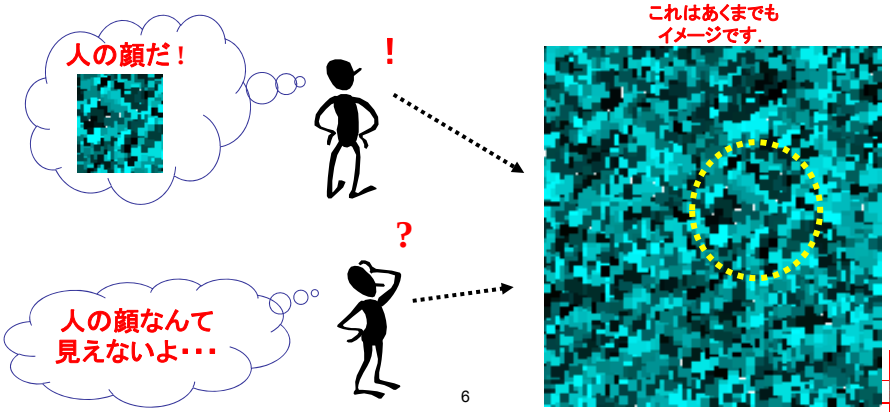
・一度経験すると二度目は簡単

・何度も経験すると慣れる

人間の認識能力を利用

Nish!gaki Laboratory

ゲシュタルトの法則：
人間はランダムドットの中にさえ，
意味を見出すことがある！！



6

ランダムドット認証

Nish!gaki Laboratory

ゲシュタルトの法則:
人間はランダムドットの中にさえ,
意味を見出すことがある！！

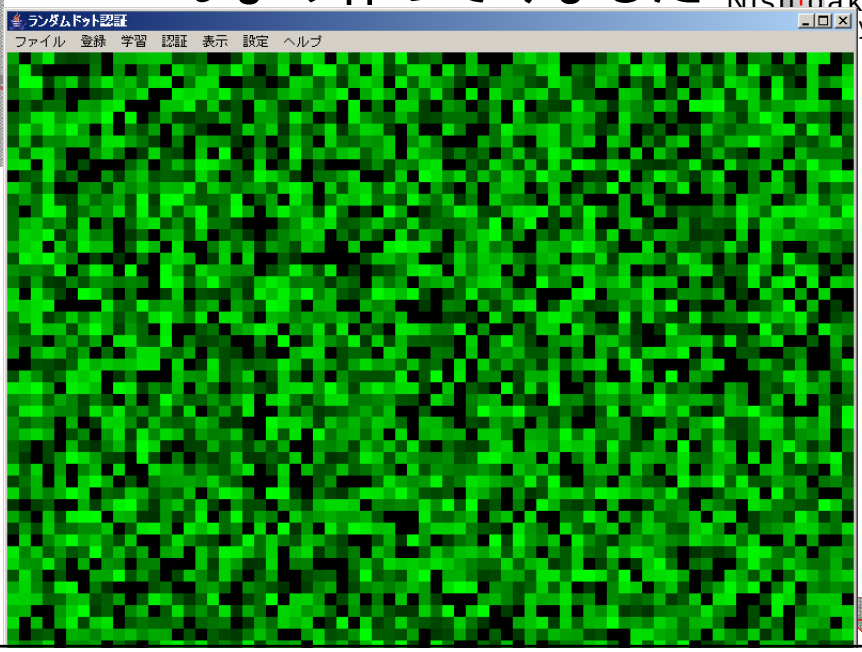
↓

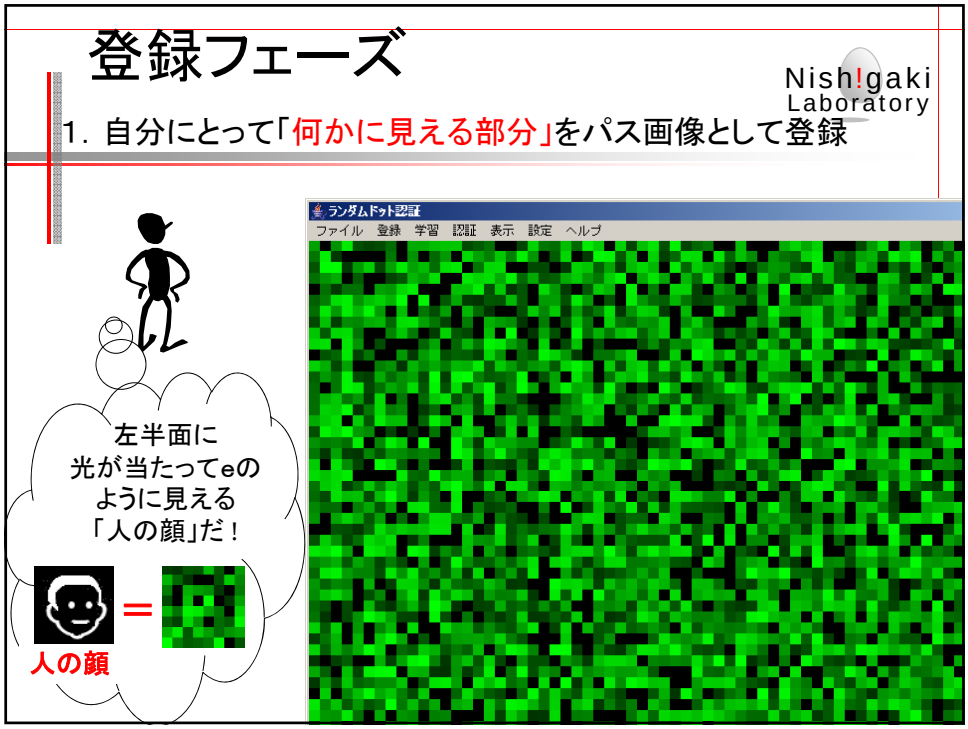
意味を見出すことができたランダムドットの
小ブロックを,「ウォーリーを探せ」認証の
キャラクタだと捉えれば,
ランダムドット認証が可能になる？？

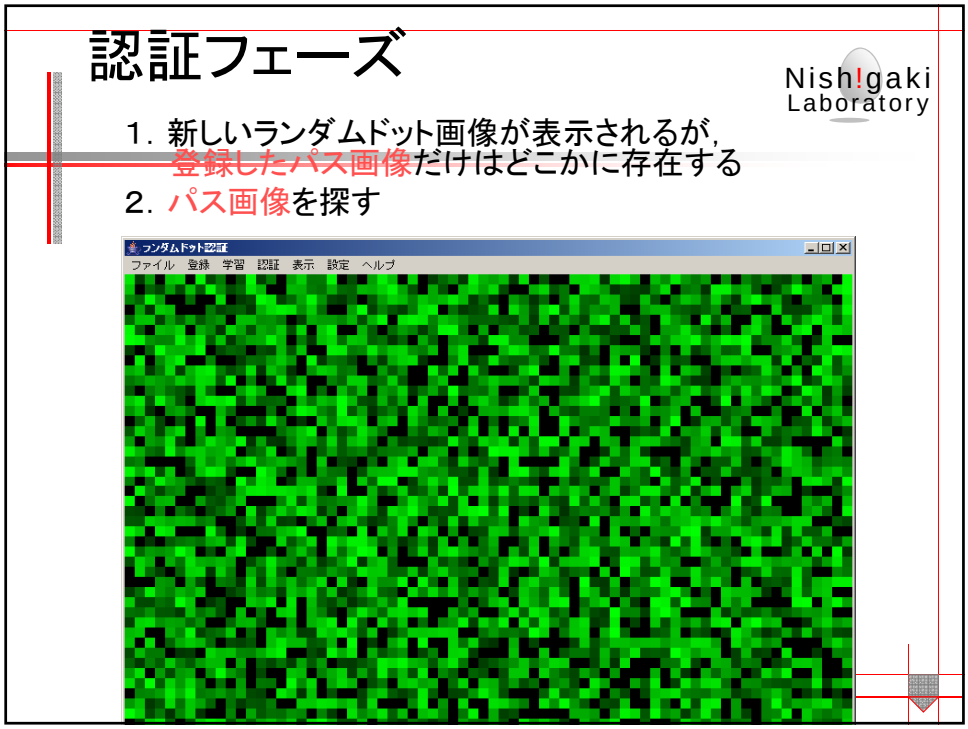
パスワードの覗き見・漏洩への対処にもなる！？

こんなの作ってみました

Nish!gaki Laboratory




登録フェーズ
Nish!gaki
Laboratory
1．自分にとって「何かに見える部分」をパス画像として登録
左半面に
光が当たってeの
ように見える
「人の顔」だ！
＝
人の顔
ランダムドット認証
ファイル 登録 学習 認証 表示 設定 ヘルプ


認証フェーズ
Nish!gaki
Laboratory
1．新しいランダムドット画像が表示されるが，
登録したパス画像だけはどこかに存在する
2．パス画像を探す
ランダムドット認証
ファイル 登録 学習 認証 表示 設定 ヘルプ

ランダムドット認証の特長

Nish!gaki Laboratory

ランダムドット画像を認証に利用することで

- 正規ユーザは
  - ランダムドットに意味を見出している
  ⇒ランダムドット画像の記憶が容易
- 攻撃者は
  - ランダムドットに意味を見出していない
  ⇒無意味なランダムドットなので，覗き見ても記憶が困難
- 他人にパス画像の内容を教えることも困難
- 内容を推測しても，正解位置を探し出すことは困難

ランダムドット認証の欠点

Nish!gaki Laboratory

- ランダムドット画像に意味を見出すことがそれほど容易ではない
- ランダムドット画像から，正解のパス画像を探すのに時間がかかる

正規ユーザの負荷が増加

上記の負荷を減らし，覗き見にも強い認証を実現する

12

モザイク認証

不鮮明化画像の使用

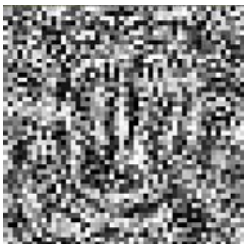
Nish!gaki Laboratory

- 一見すると無意味な画像
  - 無意味な画像を記憶することは人間でも困難
  - 言葉で表現・伝達ができない

攻撃者への漏洩を困難にできる ⇒ 本人の記憶も困難

しかし

本人には「スキーマ」を与えることで記憶を容易に



不鮮明化画像

スキーマの獲得

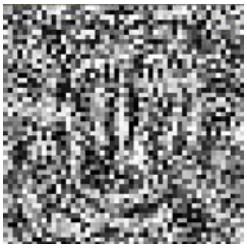
Nish!gaki Laboratory

スキーマとは，何をどのように覚えたか

⇒ 「記憶の関連づけの知識」

- 不鮮明化画像が有意味な画像として認識できる
- 一度経験すると，以後，簡単に意味が見えるようになる

⇒ 認識・記憶を容易にできる



不鮮明化画像

スキーマ

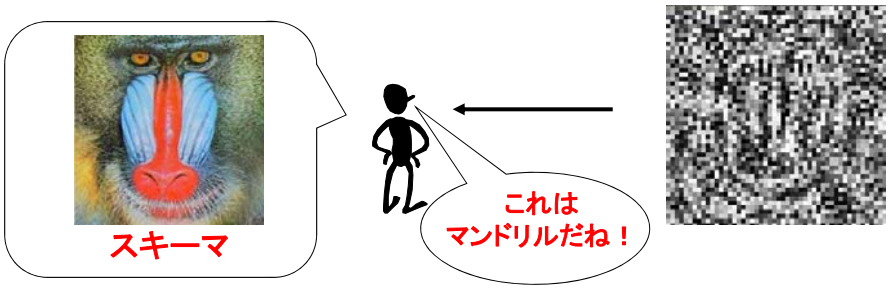
モノトーン化
モザイク化
DCT係数に乱数
などの画像処理

オリジナル画像

スキーマとは？

Nish!gaki Laboratory

- スキーマとは，何をどのように覚えたか
  ⇒「記憶の関連づけの知識」



人間は無意識のうちに，常時スキーマというフィルタを通して外界からの情報を認識している

15

認識の原理

Nish!gaki Laboratory

ボトムアップでの認識を進める

↓

意味がわかる

↓

トップダウンでそれをとらえなおす

オリジナル画像を知っている人

Nish!gaki Laboratory

ボトムアップでの認識を進める

↓

オリジナル画像がピンとくる

↓

トップダウンでそれをとらえなおす

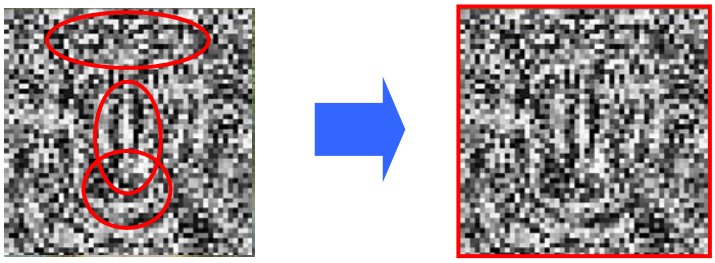
↓

不鮮明化画像を完全に認識できる

オリジナル画像を知っている人

Nish!gaki Laboratory

- スキーマにより，ピンとくるのでトップダウンで不鮮明化画像をとらえることができる



オリジナル画像を知らない人

Nish!gaki Laboratory

ボトムアップでの認識を進める

ピンとこない

オリジナル画像がピンとくる

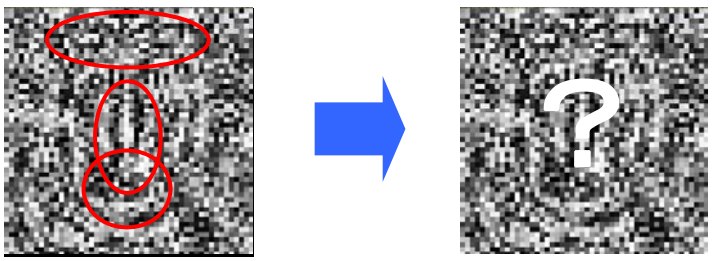
トップダウンで不鮮明化画像をとらえることが
できないので不鮮明化画像の意味を理解できない

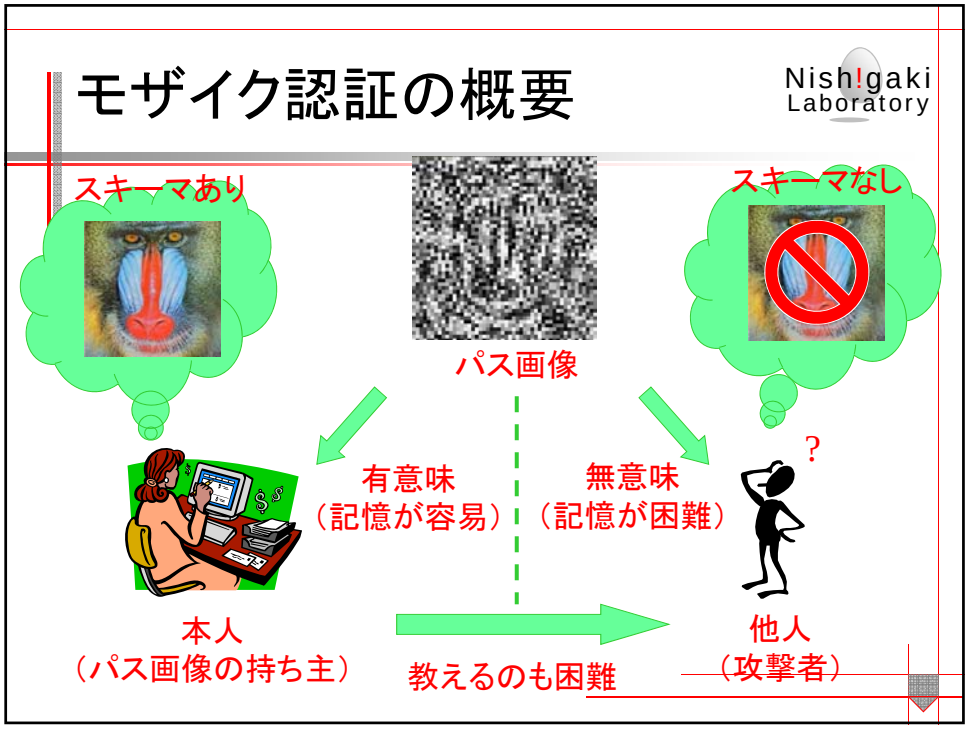
オリジナル画像を知らない人

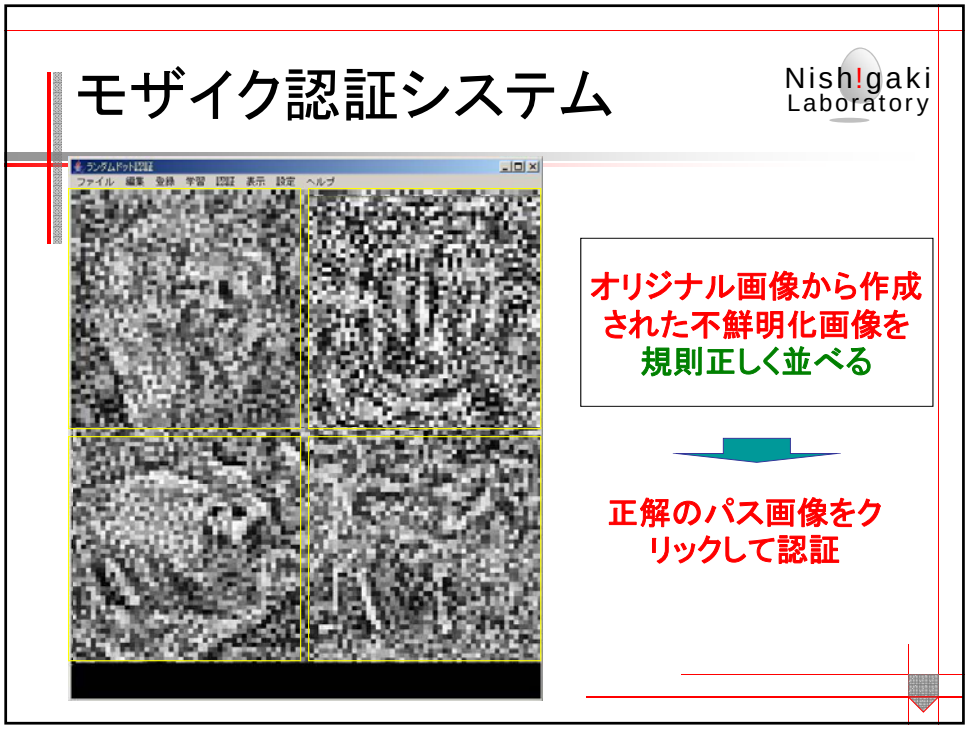
Nish!gaki Laboratory

- スキーマを持っていないのでトップダウンでとらえることができない

→意味を理解できない




モザイク認証の概要
Nish!gaki
Laboratory
スキーマあり
スキーマなし
パス画像
?
有意味
（記憶が容易）
無意味
（記憶が困難）
本人
（パス画像の持ち主）
他人
（攻撃者）
教えるのも困難

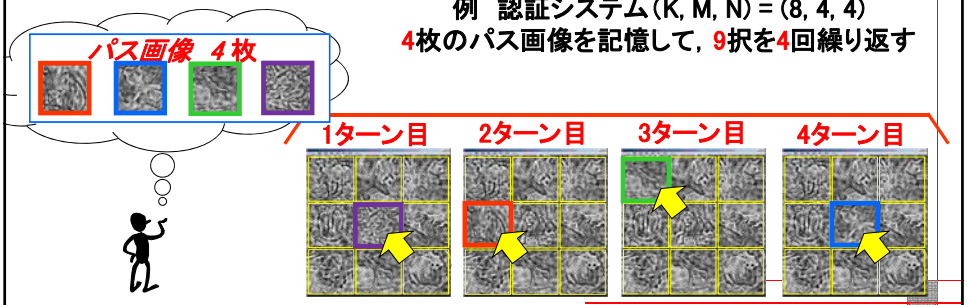

モザイク認証システム
Nish!gaki
Laboratory
オリジナル画像から作成
された不鮮明化画像を
規則正しく並べる
正解のパス画像をク
リックして認証

実運用ではn択を数回繰り返す.

Nish!gaki Laboratory

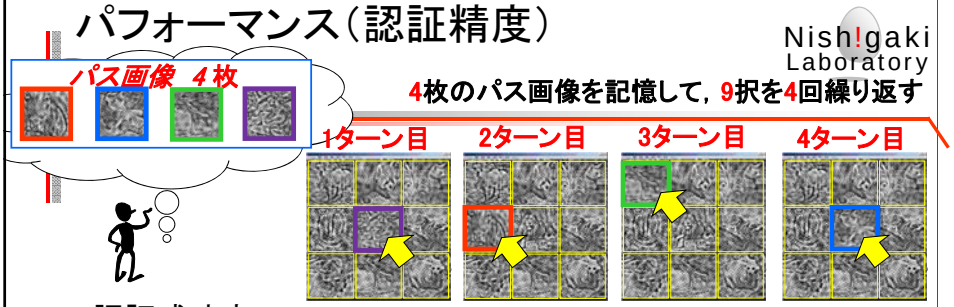
- **M**枚のパス画像を記憶してもらい，(**K+1**)択を**N**回繰り返す
  - K：囮画像の枚数
  - M：ユーザが記憶すべきパス画像の枚数
  - N：選択の繰り返し数

例　認証システム(K, M, N) = (8, 4, 4)
4枚のパス画像を記憶して，9択を4回繰り返す



パフォーマンス(認証精度)

Nish!gaki Laboratory



- 認証成功率
  - 従来の画像認証(鮮明な写真やイラストを使う)方式と同程度(ユーザの負荷は少ない)
- 覗き見攻撃成功率
  - 攻撃者に非常に有利な環境(従来の画像認証では100%攻撃に成功する環境)でも，成功率を減らすことが可能
- 推測成功率
  - 攻撃者に非常に有利な環境でも，パス画像の内容を言葉で伝えた際のパス画像推測成功率を減らすことが可能，

利便性と安全性への課題

Nish!gaki Laboratory

- 利便性
  - 使用環境（脅威のレベル）に応じた不鮮明化の度合い（およびその他のパラメタ）の調整
    - 覗き見の脅威が小さい環境では，趣味・嗜好からパス画像が推測されない程度の不鮮明化でOK
  - 加齢による影響の調査
    - 画像の再認自体は加齢の影響を受けにくいことが，認知心理学の世界で良く知られている
    - 不鮮明化画像の再認は・・・？

25

利便性と安全性への課題

Nish!gaki Laboratory

- 安全性
  - 囮画像（パス画像以外の画像）の潤沢な確保
    - あらかじめ大量に保存したり，通信を介して取得したりすることは，安全性および運用の面で好ましくない．
  - 総当たり数の壁
    - 4桁PIN（暗証番号）程度の総当たり数しかない．
    - 利便性を低下させずに総当たり数を増やしたい．
  - より強力な覗き見攻撃への耐性
    - ビデオカメラによる認証情報の盗撮
    - 複数回の盗撮にも耐えうる方式の検討．

26

まとめ

Nish!gaki Laboratory

- 人間の能力をうまく活用することで，利便性と安全性を兼ね備えた画像認証方式の実現を目指した．
- 利便性と安全性の面では，まだ不十分な点は多い．今後も両者を同時に高める方法を追求していく予定である．

- キーワード
  - 画像の再認，経験を次に生かす能力，スキーマ，
  - 不鮮明化画像，モザイク認証，脳内認証

Nish!gaki Laboratory

ご清聴ありがとうございました