Pict Place Authentication: 再認式画像認証における回答方法変更による安全性改善の試み

吉田 光宏[1,a)]　高田 哲司[1,b)]

概要：PIN やパスワードに代わる個人認証として画像認証が提案されている．その中でも再認式画像認証は秘密情報の記憶保持が最も容易な手法であると言われており，既存の知識照合型個人認証の代替として期待されている．しかし，再認式画像認証には安全性が低いという問題が残されている．そこで本研究では再認式画像認証における秘密の回答方法に着目し，新しい回答方法を導入した「Pict Place Authentication(PPA)」を提案する．従来の再認式画像認証における回答方法は画像選択であったのに対し，PPA では画像を配置することで回答入力とする．この変更により，ユーザが記憶する画像枚数を増加させることなく安全性を改善することが可能になる．PPA の有用性評価を行うために本研究ではプロトタイプシステムを実装し，クラウドソーシングを用いた評価実験を行なった．その結果，従来手法との比較で秘密情報の記憶負担は同等程度であること，また提供しうる安全性は改善可能であることが示された．

キーワード：画像認証，ユーザブルセキュリティ

Pict Place Authentication: Realizing better security for Recognition-based Graphical Authentication by an alternative credential input scheme

Mitsuhiro Yoshida[1,a)]　Tetsuju Takada[1,b)]

Abstract: There are three categories in the proposed image-based graphical authentication schemes. Among them, recognition-based graphical authentication (RbGA) is expected to be an alternative to the conventional authentication because it is considered to be easy for users to retain a user credential. However, the security level of RbGA is almost same with 4-digit personal identification number authentication. We, then, propose a novel RbGA named “Picture Place Authentication” (PPA). We changes the credential input scheme. The scheme of PPA is to place credential images to a pre-determined position in the image-grid instead of simply picking up the images. This change could improve security without increasing the number of credential images. We implemented a prototype system and conducted an online experiment through a crowd-sourcing service. The result shows that the memory load of a user credential is comparable to that of conventional authentication methods.

Keywords: Graphical Authentication, Usable Security

1. はじめに

知識照合型個人認証の一手法として画像認証が提案されている．画像認証とは，画像や絵を秘密情報とする認証手法である．人間は文字列よりも絵のほうが記憶しやすいという特性（画像優位性効果）があることから [1]，パスワードや暗証番号 (PIN) よりも秘密情報を記憶保持しやすいと言われている．画像認証は秘密情報の想起方法の違いから以下の 3 種類に分類することができる．

[1] 電気通信大学
The University of Electro-Communications
[a)] mthrysd.uec@gmail.com
[b)] zetaka@computer.org

(1) 再生式 (recall)
(2) 手がかり付き再生式 (cued-recall)
(3) 再認式 (recognition)
これらの画像認証のうち，再認式画像認証は認証時に画像群が回答候補として提示され，その中から秘密情報とした画像を選択することで認証を行う手法である。人間は，過去に記憶した情報を思い出すこと（再生）よりも，今見ている情報が過去に記憶した情報と一致するか確認すること（再認）の方が得意であるとされている [2]．実際に Stobert ら [3] は，再生式・手がかり付き再生式・再認式画像認証における秘密情報の記憶可能性を比較するために，秘密情報を記憶してから何時間後のログインに成功することができるか計測した．その結果，再生式 167 時間，手がかり付き再生式 153 時間，再認識 180 時間となり，再認式画像認証が最も長く記憶可能であることが明らかになった．

しかし，再認式画像認証にも安全性とユーザビリティ・秘密情報の記憶可能性の間にトレードオフの関係が存在する．ここで本論文では理論的安全性を示す値として，ユーザが取り得る秘密情報の数 (the Number of Possible Credentials(NPC)) を用いる．本論文における理論的安全性とは総あたり攻撃に対する安全性のことを指し，その値は一般的に NPC の逆数となる．例えば 4 桁暗証番号の場合，$NPC = 10,000$ となる．よって NPC の値が大きいほど，理論的安全性は高いということになる．

これをふまえて先行研究に目を向けると，様々な再認式画像認証が提案されているが [7][8][10][11][13][14][15][16]，実用化されている事例は Passfaces[8] をはじめとして少数であると言わざるを得ない．その理由は，認証手法が提案する理論的安全性が低いからだと考える．先行手法における安全性は，その多くが 4 桁暗証番号と同等程度の安全性であり，記憶負担の軽減という利点は見込める一方で，提供される安全性は想定される利用シーンで望まれる域に達しておらず，それが普及に至らない原因だと考える．したがって，ユーザビリティを損なうことなく安全性を改善することが再認式画像認証の課題であると言える．

再認式画像認証における NPC は，一般に「回答候補として認証画面に表示される画像群の画像枚数」と「秘密情報として回答する画像枚数」によって決定される（詳細は 2 章で述べる）．すなわち，再認式画像認証の安全性改善は以下の 2 つの値を増やすことで実現できる．

i) 回答候補である画像群の画像枚数
ii) 秘密情報とする画像枚数

しかし，方法 i) は個人認証のユーザビリティ，特に操作時間に影響する可能性がある．再認式画像認証では，認証画面に表示される画像群から秘密情報となっている画像を探し出し，回答する必要がある．つまり，表示される画像群の枚数が増えると，多くの画像群の中から秘密情報となっている画像を探さなければならなくなり，回答までの時間が長くなる懸念があるからである．したがって，方法 i) は望ましい改善方法とは言い難い．一方，方法 ii) についても望ましい改善方法とは言えない．秘密情報の画像枚数を増やすことはユーザが記憶保持しなければならない画像を直接増やすことであり，ユーザの記憶負担を増やすことになるからである．

そこで本研究では，ユーザビリティを維持しつつ再認式画像認証の理論的安全性を向上させることを目的とし，その方法として秘密情報の回答方法に着目した新たな再認式画像認証を提案する．

以降，本論文では 2 章で再認式画像認証の理論的安全性に関する議論をし，3 章で提案手法について説明する．4 章で提案手法の評価実験について説明し，その結果について述べる．5 章で考察を述べ，6 章で本研究で明らかになったことについてまとめる．

2. 既存手法の安全性

本章では，既存の再認式画像認証の安全性についてまとめ，その改善に関する考察を行う．

2.1 再認式画像認証の安全性

これまで提案されている再認式画像認証は [7][8][10][11][13][14][15][16]，一般的に以下の 3 つの処理を行うことで認証を行う．

p1) システムがユーザに回答候補となる画像群を提示する
p2) ユーザがシステムに対し，秘密情報である画像を回答する
p3) (**p1**, **p2**) の処理を必要回数分繰り返す

また **p2** の処理では，「一枚の画像」を回答する手法 [8][10][11][14][16] と「複数枚の画像」を回答する手法 [7][13][15] がある．さらに **p2** で複数枚の画像を回答する手法の一部は，「画像の回答順序」も秘密情報とする手法がある [13][15]．これらの整理から，再認式画像認証の安全性は以下に示す 4 つの変数 (n, m, o, r) を入力とする 2 つの式（式 A, B）で表すことができる．

n： **p1** において，システムがユーザに提示する画像枚数 $(n > 1, n > m)$
m： **p2** において，ユーザがシステムに回答する画像枚数 $(m \geq 1)$
o： **p2** におけるユーザの回答が「順序付き」か「順不同」か $(o = \{true\,(\text{順序付き}), false\,(\text{順不同})\})$
r： **p3** における繰り返し回数 $(r \geq 1)$

(式 A) if $(o == false)$ then: $NPC = ({}_nC_m)^r$
(式 B) if $(o == true)$ then: $NPC = ({}_nP_m)^r$ [*1]

[*1] 著者らの知る範囲において $o = true$ の場合 $r = 1$ である．

表 1 再認式画像認証の設計変数と安全性 (NPC)，認証時間

	設計変数 (n,m,o,r)	NPC	認証時間 (s)
Photographical Authentication[10]	(4, 1, false, 10)	1,048,576	40
Déjà Vu[7]	(25, 5, false, 1)	53,130	36
あわせ絵 [12]	(10, 1, false, 4)	9,999	24.6
スキーマ [14]	(9, 1, false, 4)	6,561	28.4〜32.8
PassFaces [9]	(9,1, false, 4)	6,561	20
VIP(type1)[15]	(10, 4, true, 1)	5,040	5〜6
Story[13]	(9, 4, true, 1)	3,024	-
Use Your Illusion[16]	(27, 3, false, 1)	2,925	11.5〜25.8

ここまでの議論に基づき既存の再認式画像認証について整理したものが**表 1** である．

2.2 再認式画像認証の安全性改善に関する考察

前節の議論をふまえ，安全性改善方法について考察する．NPC が大きいほど理論的安全性が高いことになるが，そのためには以下の 2 つの方法が考えられる．

方法 1) 変数 (n, m, r) の値を増やす

方法 2) 変数 $o = true$ とする

しかし，これらの方法には問題がある．方法 1 のうち m を増やす方法は，ユーザが記憶保持すべき画像枚数を増やすことになるため記憶負担が増える．再認方式の画像認証は「過去に見たことのある画像」を選択する認証手法であり，記憶負担を低減できる可能性を持っているが，それでも多くの画像をユーザが記憶保持できるとは限らない．ユーザが実際に記憶保持すべき画像枚数 M は $M = m \times r$ となるが，表 1 にある先行研究でも文献 [10] の手法を除くと，M は 3〜5 枚という設計になっている．

また方法 1 において n, r を増やす方法は，認証時にユーザが秘密情報を探索する画像枚数が増えることになり認証時間が長くなることが懸念される．表表 1 で認証画面に提示される画像枚数が最も多い 40 枚である文献 [10] の手法の場合，認証時間は平均で 40 秒となっている．よって方法 1 による安全性改善は，ユーザビリティを犠牲にすることと引き換えで得られる利点であり，望ましい改善法とは言いがたい．

また方法 2 の改善方法も望ましい方法とは言いがたい．この方法は，方法 1 で m を増やすのと同様と考えることができ，秘密情報を増やすことにより安全性を改善するとみなすことができる．回答順序については秘密となる画像群を用いてストーリを作ることで記憶保持を可能にするという方法が提案されているが，それもユーザにとって容易なこととは言いがたい．文献 [13] の実験によると，認証時の入力ミスが 236 件発生したが，それらのミスの 75%以上は「正しい画像を間違った順序で回答した」というものであり，この結果から文献 [13] の著者らは「回答順序を秘密情報とするべきではない」と結論づけている．

したがって，上記以外の方法で理論的安全性を改善しつつ，それと同時に認証時間や記憶負担に悪影響を及ぼさない手法を考える必要がある．

3. 提案手法

ここで我々は，Pict Place Authentication(PPA) と呼ぶ新たな画像認証手法を提案する．この手法における着目点は再認式画像認証の回答方法である．従来の再認式画像認証はシステムより提示された画像群の中から，事前に秘密情報として登録しておいた画像（秘密画像）を「選択」するものであった．これに対して提案手法は，回答方法を「秘密画像を単に選択する」のではなく「秘密画像を既定の位置に配置する」方法に変更する．提案手法における秘密情報の定義を**図 1**(2) に示す．この図では 4 枚の画像を特定の位置に配置した例を示しているが，このように提案手法では (画像-配置場所) の組み合わせがすべて正しい場合に認証成功となる．

提案手法は回答方法に工夫を加えたという点で順序付き回答方式 $(o = true)$ と同様であるとも言える．しかし著者らは，再認式の手法を生かした改善提案だと考えている．順序付き回答方式との違いは以下の 2 点である．

- 秘密情報設定時に秘密情報の定義内容を視覚的に捉えることが可能
- 認証時に定義した秘密情報を視覚的に再現させる点にある．

ユーザが記憶すべき秘密情報の情報量は，秘密画像の枚数分に相当する配置場所も記憶する必要が生じるので，記憶すべき情報量は 2 倍になる．しかし，秘密情報の設定を視覚的に行い，かつ認証時にも秘密情報を視覚的に再現する操作になることから，再認による効果も手伝って秘密情報を再現できることが期待される．

3.1 操作手順

PPA における操作方法について「秘密情報の登録」と「認証」の 2 つに分けて説明する．

PPA における秘密情報の登録は以下の 4 手順で行う (図 1)．

(1) **ユーザ名の入力**

登録するユーザ名を入力する．すると図 1(1) の秘密作成画面が表示される．

(2) **秘密情報の配置場所の決定**

PPA がランダムに秘密画像の枚数分 n の配置場所を決定する．決定された位置は認証画面内でオレンジ色の枠線でハイライトされる (図 1(1))．

(3) **秘密情報の作成**

秘密作成画面 (図 1(1)) が表示される．画面には m 個の配置位置があり，そこに回答候補となる画像群 m 枚が表示される．この画像群からユーザは秘密情報にしたい画像 n 枚を決定し，それをオレンジ枠となっている配置位置の 1 つへ Drag & Drop で移動する．こ

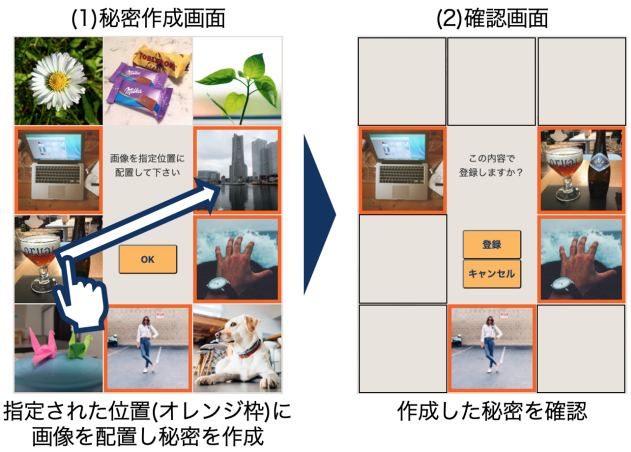

図 1　PPA における秘密情報登録手順

図 2　PPA の認証手順．Drag&Drop 操作で秘密画像を正しい位置に配置し直し，その結果が正しければ認証成功．

れを n 枚分行うことで秘密情報を作成する．ただし，複数枚の画像を同一配置位置に配置することはできない．(画像-配置位置) は 1 対 1 の関係とする．作成が完了したら “OK” ボタンを押す．

(4) **秘密情報の確認**

秘密情報の作成が完了すると，秘密情報の確認画面が表示される（図 1(2) 確認画面）．この画面ではユーザが記憶すべき画像と配置位置のみが提示される．秘密情報の内容を確認したら “登録” ボタンを押す．これで秘密情報の登録が完了となる．

次に「認証」時の操作について説明する (**図 2**)．秘密情報の登録時と同様，ユーザ名を入力する．すると，秘密情報入力画面が表示される（図 2(1)）．この画面における画像の配置位置は認証を行うたびに毎回ランダムに配置される．したがって，秘密情報である各画像が既定の配置位置に表示されている場合もあれば，されていない場合もある．既定の位置に表示されていない場合，該当する画像を Drag&Drop 操作することで既定の位置に表示されるよう移動する．m 枚の秘密画像すべてを既定の位置に配置し終えたら “OK” ボタンを押す．この際の画像配置のうち，既定の m 個の配置位置に既定の秘密画像が正しく配置されていれば認証成功となる．なお銀行 ATM と同様，一回の認証試行で 3 回までの回答入力を認めており，3 回連続で秘密情報の検証に失敗すると，認証失敗となる．

4. 評価実験

本研究の目的は「秘密情報の記憶負担やユーザビリティを維持しつつ，再認式画像認証の理論的安全性を向上する」ことである．そこで我々は PPA における秘密情報の記憶負担とユーザビリティを明らかにするため，実験参加者による評価実験を行った．本章では，本実験における実験方法と結果について述べる．

4.1 概要

本実験では，PPA の「秘密情報の記憶負担」ならびに「ユーザビリティ」を評価するために，Web ブラウザ上で動作するプロトタイプシステムを実装した．「秘密情報の記憶負担」については実験を通じて得られる認証成功率を客観値とし，またアンケート結果で主観的な印象を測定することとした．「認証時間」については，実際にシステムを使用する際にかかる操作時間をプロトタイプシステムを通じて測定し，客観値として用いた．なお，本実験では既存の再認式画像認証と比較を行うため，「順不同の画像認証」と「順序付き画像認証」の 2 つのシステムもプロトタイプシステムとして実装したうえで，同様の方法で評価を実施した．以降では「順不同の画像認証を」“ImgAuth”，「順序付き画像認証」を “ImgAuthOA” と略記する．この前提のもと，我々は以下の 4 つの仮説を立てた．この仮説は記憶負担について，PPA は ImgAuthOA より優れている（H1）と想定し，ImgAuth と同等である（H2）と想定したものである．また認証時間について，PPA は ImgAuth・ImgAuthOA と同等である（H3, 4）と想定したものである．

- 記憶負担に関する仮説：
  PPA<ImgAuthOA（H1），PPA≈ImgAuth（H2）
- 認証時間に関する仮説：
  PPA≈ImgAuthOA（H3），PPA≈ImgAuth（H4）

4.2 実験方法

秘密情報の記憶保持に関する評価を行うため，7 日間の間隔を空けて 2 回認証を実施する形で評価を行った．実験手順は以下の通りである．

step 1) 実験説明
step 2) 秘密情報の登録と認証操作の確認
step 3) 計算問題
step 4) 認証試行
step 5) アンケート

実験 1 日目は上記手順の step 1 から step 5 までを，7 日後

表 2　1 日目の実験参加者に関する情報

	PPA	ImgAuth	ImgAuthOA
参加人数 (人)	52	36	47
男, 女 (人)	41, 11	29, 7	35, 12
年齢層 (平均年齢)	39.9	40.0	41.9

の 8 日目には step 1, 4, 5 を実施した．なお 8 日後の実験は 1 日目の実験で step 4 の認証に成功した実験参加者のみを参加させた．また step 3 は秘密情報の短期記憶に関する評価を目的として実験参加者に課したタスクであり，ワーキングメモリを利用する作業として 1-3 桁数字までの四則演算 30 問を行わせたものである．

実験はオンラインで実施し，実験参加者は Yahoo クラウドソーシング [19] を通じて募集した．3 つの認証システム (PPA，ImgAuth，ImgAuthOA) の評価を行うため，実験参加者を 3 グループに分け，各実験参加者は 3 システムのうち 1 システムについて評価を行った (Between-subject design)．1 日目の実験を完了した参加者には 50 円分のポイントを，8 日目の実験を完了した参加者はさらに 100 円分のポイントを報酬として支払った．150 人の参加者を募集し，そのうち所定の測定を完了した参加者は 135 人であった．実験参加者に関する情報を**表 2** に示す．

4.3　実験結果

4.3.1　認証成功率

1 日目及び 8 日目における 3 システムごとの認証成功率を**表 3** に示す．なお表 3 内の認証成功率の下に記載されている 2 つの数値は (認証成功人数/実験実施人数) を示す．1 日目の実験について，PPA では 47/52 人 (90.4%) が認証に成功した．ImgAuth と ImgAuthOA では全員が認証に成功した．この結果に対しフィッシャーの正確確率検定により多重比較を行った結果，有意差が見られなかった ($p = .08, p = .06, p = 1.0$)．

8 日目の実験について，PPA では 33/45 人 (73.3%) が認証に成功した．ImgAuth では 31/35 人 (88.6%) が認証に成功した．また ImgAuthOA では 35/42 人 (83.3%) が認証に成功した．この結果に対し χ^2 検定を行った結果，有意差は見られなかった ($\chi^2(2) = 3.188, p = 0.2$)．

4.3.2　認証時間

評価対象 3 システムにおける認証成功時の認証時間を表 3 の最下行に示す．秒数で記載している値が平均値であり，その下に記載している 2 つの値は中央値と標準偏差を示している．この結果に対し, Shapiro-Wilk 検定により正規性の検定を行った後, Kruskal-Wallis 検定を行った結果, 有意差が見られた ($\chi^2(2) = 3.188, p < 0.05$)．さらにウィルコクソンの順位和検定により多重比較を行ったところ，PPA と ImgAuth の間に有意差が見られ ($W = 3162, p < 0.05$)，PPA と ImgAuthOA の間に有意差が見られた ($W = 9216, p < 0.05$)．一方で ImgAuth と ImgAuthOA の間には有意差が見られなかった ($W = 4603, p = 0.06$)．

4.3.3　アンケート結果

8 日目のアンケートで，PPA と ImgAuthOA のグループに対し以下のアンケートを行った．

質問：実験手法（PPA or ImgAuthOA）と ImgAuth を比較し，どちらの秘密情報が覚えやすいと思いますか（2 値回答）

アンケートに対する回答結果を**表 4** に示す．この結果に対し χ^2 検定を行ったところ，有意差は見られなかった ($\chi^2(1) = 0.274, p = .60$)．

5.　考察および制限

評価実験の結果をふまつつ，仮説の検証に基づく秘密情報の記憶負担と認証時間に関する考察，ならびに PPA の安全性について議論する．

5.1　記憶負担に関する議論

4.3.1 節の議論から，今回評価を行った 3 システム間において認証成功率に有意差は見られなかった．また秘密情報の記憶保持に関する主観的印象についてアンケートを通じて調査を行なったが，これについても有意差は見られなかった．これらの結果から，記憶負担に関する仮説 H1 については棄却となり，仮説 H2 については成立すると解釈することができる，という結果となった．

なお表 4 の結果については PPA と ImgAuthOA の間で再検証の余地があると考えている．ImgAuthOA, PPA を ImgAuth と比較すると秘密情報の量は確実に増えるため，多くの参加者が「ImgAuth の方が覚えやすい」と回答するのは想定通りである．そのような状況下において ImgAuthOA や PPA の秘密情報の方が覚えやすいと回答した実験参加者の人数をみると (PPA, ImgAuthOA) = (7 人 (15.6%), 4 人 (9.5%)) となっている．この結果は，PPA と ImgAuthOA の秘密情報を比較した場合，ユーザは PPA の方を好意的に受け止める可能性がある，とみることもできる．PPA と ImgAuthOA の比較を目的とした再検証については今後の課題とする．

なお今回の実験では参加者の一部が秘密情報を記憶保持せずに記録していたという事例が発生していた．8 日目のアンケートで「秘密情報をどこかに記録していましたか？」という質問を行ったところ，(PPA, ImgAuth, ImgAuthOA) = (10 人, 2 人, 9 人) の参加者が「記録していた」と回答した．したがって，今回の実験結果には本来あるべき方法で評価したものではないデータも含まれており，実際の認証成功率は報告値よりも小さい可能性があることをふまえる必要がある．

表 3　認証成功率および認証成功時の認証時間

	PPA	ImgAuth	ImgAuthOA
認証成功率（1 日目）	90.4% (47/52)	100% (36/36)	100% (47/47)
認証成功率（8 日目）	73.3% (33/45)	88.6% (31/35)	83.3% (35/42)
平均認証時間 (Median, SD)	24.4 秒 (16.9, 20.44)	13.2 秒 (9.1, 1.86)	15.7 秒 (10.1, 17.10)

表 4　アンケートに対する回答結果（人）

	PPA	ImgAuthOA
ImgAuth の方が覚えやすい	38	38
実験手法の方が覚えやすい	7	4

5.2　認証時間に関する議論

実験によって得られた結果から，仮説 H3 および H4 はいずれも棄却された．その原因として，操作方法が参加者にとって困難であった可能性が挙げられる．参加者が実験中に行ったクリック操作および Drag&Drop 操作の回数を数えると，ImgAuth，ImgAuthOA で操作された総クリック回数はそれぞれ 571 回，715 回，PPA で操作された総 Drag&Drop 回数は 1,165 回であった．PPA における総 Drag&Drop 回数が ImgAuth，ImgAuthOA における総クリック回数が多いことから，参加者にとって PPA の操作が困難であったため認証時間が長くなったと考えられる．

5.3　理論的安全性に関する議論

PPA の安全性について述べる．PPA では (秘密画像 × 各画像の配置位置) の 2 情報が秘密情報となる．したがって，我々が想定する PPA の NPC 値は上記のそれぞれについて “通り数” を算出し，その積が回答となる．それぞれの通り数は以下の様になる．

- 秘密画像の通り数：認証画面に提示される画像群の画像数 n から秘密画像 m 枚を選択する．この時の通り数は ${}_nC_m$ となる．
- 各秘密画像の配置位置：上記の項目で選択された m 枚の画像を，n 個の配置可能場所の中から事前に決定されている m 個の配置位置に並べる．この時の通り数は ${}_nP_m$ となる．

したがって PPA における NPC は以下の式で表すことができる．

$$NPC = ({}_nC_m) \times ({}_nP_m)$$

3 章で述べたプロトタイプの設定値は $(n, m) = (10, 4)$ であるため，NPC の値は $NPC = 1,058,400$ となる．これは 6 桁暗証番号による個人認証と同等程度の安全性である．

しかしながら，今回の実験で使用したプロトタイプシステムの実際の NPC 値は前述した値よりも小さくなる．その原因はユーザインタフェースにある．プロトタイプシステムでは n 枚の回答候補画像が n 個の配置可能位置に必ず表示される仕様になっている．つまり，攻撃者が入力した回答が偶然正しい秘密情報になる確率が高くなる状況になっているのである．以下に詳細について説明する．

n 枚の画像の配置パターンは全部で $n!$ 通りある．このうち正解となる秘密画像の配置パターン数は，m 枚の秘密画像が m 箇所の配置位置に正しく配置されれば良いので，残りの $n - m$ 箇所の位置に配置される $n - m$ 枚の画像配置はランダムでよいこととなる．よって正しい秘密情報となる配置パターン数は全部で $(n - m)!$ 通りとなる．よって (n, m)=(10, 4) の場合，正しい秘密情報となるパターン数は 1 通りではなく 720 通りとなる．全配置パターンは 3,628,800 通りとなるので，無作為回答が偶然正解になる確率は 1/5,040 となる．これは 4 桁暗証番号認証よりも安全性が低い結果となる．

今回のプロトタイプ実装で 3 章で述べた実装にした理由は，比較実験を想定して実装を行なったためである．4 章で述べた通り，比較評価を行うため PPA だけでなく ImgAuth や ImgAuthOA もプロトタイプ実装した．その際，ユーザインタフェースがほぼ同等に見える形で実装することが望ましいと考えたためである．本来の安全性となる実装は，ユーザが画像を配置した場所のみ画像が表示され，それ以外の配置位置は空欄になるべきであった．よってプロトタイプ実装を修正し，あらためて評価実験を行うことは今後の課題である．

ただし，上記の問題ゆえに今回の評価実験は無意味になるとは考えていない．理由は，秘密情報の定義ならびに回答入力操作に違いは生じないからである．秘密画像を選択し，それを既定の位置に置くという認証行為自体は全く同じであり，差として生じるのは，回答入力結果の画面表示だけである．著者の想定できていない影響がないとは言いがたいものの，今回の結果は提案手法の評価として有益な結果を提示していると考えている．

5.4　制約について

システムの利用に対するモチベーション：実験で使用したプロトタイプシステムは，実際に参加者がサービスを利用するために用いたものではなかった．よって参加者のシステムの利用に対するモチベーションが適切ではなかった可能性がある．

オンライン実験によるシステムの理解度の制約：今回の実験は一般的な参加者による評価を行うために，Yahoo クラウドソーシングによって参加者を募集し，オンラインで実験を実施した．よってすべての参加者がシステムの使用方法について正しく理解できていたかは定かでない．しかし実験 1 日目の step 1（実験説明）でシステムの理解度として，覚える秘密情報に関する質問をし，その質問に正しく回答することができると実験を続けることができた．

オンライン実験による環境の制約：実験をオンラインで実施したため，参加者が実験に落ち着いて取り組める環境であったかは定かでない．参加者が別の作業を行いながら実験に参加していた可能性がある．しかし実験 1 日目の step 1（実験説明）で「実験中に別の作業を行わないで下さい」という文面で参加者に対し注意を促した．

秘密情報の記録：実験では秘密情報を記録したと回答した参加者が一定数存在した．この参加者以外にも秘密情報を何かしらの手段で記録していた参加者がいる可能性がある．

6. 結論

背景として再認式画像認証が提案されているが，実用化されている事例は少数である．その理由として理論的安全性が低いことが要因の一つであると考えた．そこで我々はユーザビリティを維持しつつ再認式画像認証の理論的安全性を向上することを目的として本研究を行った．

従来の再認式画像認証についてまとめ，安全性改善に関する議論をした上で，再認式画像認証の回答方法に着目することで安全性改善を試みた．従来の再認式画像認証の回答方法は「秘密画像の選択」であったのに対し，我々は「秘密画像の配置」によって回答する PPA を提案した．PPA の有用性を評価するためにプロトタイプシステムを実装し，オンライン実験を行った．記憶負担に関する仮説と認証時間に関する仮説を，従来手法との比較によって検証した結果，秘密情報の記憶負担は同程度であること，認証時間は PPA が有意に長くなることが示された．今後は従来手法との群間比較を行うことでより詳細に PPA の有用性について検証する．また本来想定していた理論的安全性をとるシステムを実装し検証する予定である．

参考文献

[1] A. Paivio, T. Rogers, and P. C. Smythe.: Why are pictures easier to recall than words?, Psychonomic Science, 11(4):137-138, 1968.

[2] F. Haist, A. P. Shinamura, and L. R. Squire.: On the Relationship Between Recall and Recognition Memory, *Journal of Experimental Psychology: Learning, Memory and Cognition*, 18:691–702, (1992).

[3] Stobert, E. and Biddle, R.: Memory retrieval and graphical passwords, *Proc. the 9th Symposium on Usable Privacy and Security (SOUPS'13)*, (2013).

[4] Stobert, E., Forget, A., Chiasson, S., Van Oorschot, P.C. and Biddle, R.: Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords, *Proc. Annual Computer Security Applications Conference (ACSAC)*, (2010).

[5] Gao, H., Jia, W., Ye, F. and Ma, L.: A survey on the use of graphical passwords in security, *JOURNAL OF SOFTWARE*, Vol. 8, No. 7, pp.1678-1698, (2013).

[6] Biddle, R., Chiasson, S. and Van Oorschot, P.C.: Graphical passwords: Learning from the first twelve years, *ACM Computing Surveys*, Vol. 44, No. 4, (2012).

[7] Dhamija, R. and Perrig, A.: Déjà Vu: a user study using images for authentication, *Proc. the 9th conference on USENIX Security Symposium*, (2000).

[8] Passfaces Corporation: Passfaces: Two Factor Authentication for the Enterprise, available from < http://www.passfaces.com > (accessed 2020-07-01).

[9] Brostoff, S. and Angela Sasse, M.: Are Passfaces More Usable Than Passwords? A Field Trial Investigation, *People and Computers XIV — Usability or Else!*, pp.405-424, (2000).

[10] Pering, T., Sundar, M., Light, J. and Want, R.: Photographic authentication through untrusted terminals, *IEEE Pervasive Computing*, Vol.2, pp.30-36, (2003).

[11] 高田哲司，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.2002-2012, (2003)．

[12] 高田哲司，大貫岳人，小池英樹：個人認証システム「あわせ絵」の安全性と利便性に関する評価実験，情報処理学会論文誌，Vol.47, No.8, pp.2602-2612, (2006)．

[13] Davis, D., Monrose, F. and Reiter, K.M.: On User Choice in Graphical Password Schemes, *Proc. the 13th conference on USENIX Security Symposium*, (2004).

[14] 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997-2013, (2005)．

[15] De Angeli, A., Coventry, L., Johnson, G. and Renaud, K.: Is a picture reallyworth a thousand words? Exploring the feasibilityof graphical authentication systems, *International Journal of Human-Computer Studies*, Vol.63, pp.128-152, (2005)

[16] Hayashi, E., Dhamija, R., Christin, N. and Perrig, A.: Use Your Illusion: secure authentication usable anywhere, *Proc. the 4th symposium on Usable privacy and security (SOUPS)*, (2008).

[17] Nasrullah Al-Ameen, M., Wright, M. and Scielzo, S.: Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues, *Proc. the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*, pp.2315-324, ACM (2015).

[18] Christina, K., Christos, F., Marios, B., George, S., and Nikolaos, A.: A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication, *International Journal of Human–Computer Interaction*, Vol.35, pp.1800-1812, (2019).

[19] Yahoo クラウドソーシング，入手先 ⟨https://crowdsourcing.yahoo.co.jp/⟩ (参照 2020.08.10)．