Pict Place Shuffle: 情報配置と間接入力による再認式画像認証の改良

吉田 光宏[1,a)]　高田 哲司[1]

概要：暗証番号やパスワードを代表とする知識照合型個人認証は，秘密情報をユーザが記憶保持する必要があり，ユーザにとって負担となっている．そこで改善案の 1 つとして再認式画像認証が提案されているが，これには理論的安全性，認証時間，覗き見攻撃の面で問題が残されている．本研究ではこれらの問題を改善し得る手法として Pict Place Shuffle を提案する．Pict Place Shuffle は，「画像配置」を秘密情報とし，画像を直接選択しない「間接入力」によって秘密情報の入力を行う新たな再認式画像認証である．この手法を用いて被験者実験を行い既存手法との比較を行った結果，Pict Place Shuffle は 3 つの問題点に対する改善策の 1 つとなり得る手法であることを明らかにすることができた．

1. はじめに

暗証番号やパスワードに代表される知識照合型個人認証は，Web サービスや携帯端末の画面ロックとして利用されている．この個人認証手法における問題点は，パスワードや暗証番号といった “秘密情報” をユーザが記憶保持する必要がある点にある．安全な秘密情報を作成し，かつ記憶保持することがこの手法を利用する上で必要となるが，ユーザの多くにとって容易なことではない．よってユーザは，秘密情報を書き留める，記憶できる簡単なパスワードを設定するなど，個人認証を安全に利用する上で望ましくない状況を生む原因になっている．

この問題を改善する方法の 1 つとして再認式画像認証が提案されている．再認式画像認証とは，複数枚の画像を秘密情報とし，認証時には回答候補として提示される画像群の中から秘密情報である画像を選択することで認証操作者がユーザ本人であることを検証する個人認証手法である．この手法の利点は，秘密情報の記憶負担軽減にある．人間には文字列よりも画像を記憶することの方が得意という能力があることが知られている (画像優位性効果 [3])．再認式画像認証の秘密情報は画像であるため，その能力を秘密情報の記憶保持に活用できることから負担軽減になる．もう 1 つは，再認による回答方法により得られる想起支援である．再認式画像認証では認証時に回答候補の画像群が表示され，それらを認識し，秘密情報を選択することで回答を行う．この認識処理を通じて画像を見ることにより，忘れかけていた，または忘れていた秘密情報を思い出す可能性がある．つまり秘密情報の記憶復元を助ける可能性がある．この効果は，空欄の入力フィールドを提示し，回答入力を促す既存の知識照合型個人認証では得られない．ユーザが認証画面から得られる想起支援となるものが無いからである．

しかし，再認式画像認証には以下の問題が残されている．

(1) 安全性: 再認式画像認証は一般に「安全性」が高いとはいえない．ここでいう安全性とは，総当たり攻撃 (Brute-force Attack) に対する安全性を指す．再認式画像認証には認証画面と秘密情報に関して複数のパラメータが存在するため，安全性を一概に議論することはできない．その点をふまえた上で代表的なシステムを例に挙げると，秘密情報が「4 枚の画像」である場合，その安全性は 4 桁数字による暗証番号認証と同等程度であることが多い．

(2) 操作時間: 再認式画像認証における操作時間は短いとは言いがたい．再認式画像認証では認証画面に提示される画像群をユーザが認識し，その中から秘密情報である画像を探し出す時間が必要となる．したがって，純粋に入力操作を行う以外の時間が必要となることから操作時間が長くなる．Stobert らによる評価実験では，48 枚の画像群の中から 5 枚の画像を選択するという再認式画像認証を用いた結果，操作時間は平均 34.61 秒であった [4]．

(3) 覗き見攻撃: 個人認証には覗き見攻撃 (Shoulder Surfing Attack) という脅威が存在する．これは攻撃者が正規利用者の認証行為を覗き見ることで秘密情報を窃

[1] 電気通信大学
[a)] mthrysd.uec@gmail.com

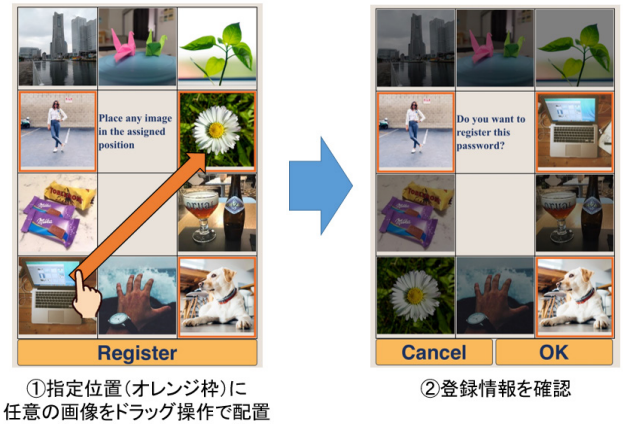

図 1 Pict Place Shuffle における秘密情報登録処理

取する攻撃である．再認式画像認証はこの攻撃に脆弱である．その原因は回答方法にある．再認式画像認証では，秘密情報である画像を直接選択することで回答入力するため，認証行為を第三者が覗き見していれば，秘密情報は第三者に特定されるからである．

そこで本研究は，(1) 認証時のインタフェースを利用した新たな秘密情報を定義するとともに，(2) 回答入力方法を工夫することにより，これらの問題を改善しうる新たな再認式画像認証 “Pict Place Shuffle” を提案する．

2. 提案手法 - Pict Place Shuffle

Pict Place Shuffle では前章で述べた問題点を改善するため，2 つの工夫を行った．1 つは，秘密情報の定義を「複数枚の画像」から「複数枚の画像の配置」に変更したことである．再認式画像認証は，認証時に回答候補である画像群を利用者に提示する．その際，認証システムが回答候補となる画像群を認証画面内になんらかの方法で配置するが，Pict Place Shuffle ではこの配置を秘密情報に応用する．つまり，Pict Place Shuffle における秘密情報は「特定の画像」を認証画面内の「特定の位置」に配置すると定義する．

Pict Place Shuffle における秘密情報の登録処理について説明する (図 1)．なお以降では，秘密情報を「3 枚の画像による画像配置」として話を進める．登録手順は以下の通りである．

(1) ユーザ名を入力する．すると**図 1** 左の画面が表示される．
(2) 秘密情報のうち「画像の配置位置」は認証システムがランダムに決定する．図 1 左の画面におけるオレンジ色の枠でハイライトされている 3 つの配置位置がそれに該当する．
(3) 画面内の 10 枚の画像群から秘密情報にする画像 3 枚を決める．以降，この画像を “パス画像” と呼ぶ．
(4) パス画像 3 枚をそれぞれどの位置に配置するか決める
(5) パス画像を決定した配置位置に Drag 操作で移動する．図 1 左では 1 枚のパス画像を移動している．
(6) 画面下の “Register” ボタンを押す．すると定義した秘密情報の確認画面 (図 1 右) が表示される．設定内容を確認して問題がなければ “OK” ボタンを押す．これで秘密情報が登録完了となる．

上記の操作により，ユーザは「3 枚の画像の配置」を秘密情報として定義したことになる．

もう 1 つの工夫は，2 種類の入力方法を組み合わせて回答を行うことである．2 種類の方法のうちの 1 つは，秘密情報登録処理で説明した Drag 操作による方法である．秘密情報であるパス画像を同じく秘密情報である配置位置に直接移動する操作である．もう 1 つの方法は，認証画面内の画像配置を Shuffle(ランダム再配置) することで入力する方法である．ユーザが画像再配置の操作を行うと，認証画面内の画像群の配置がランダムに変更される．この操作を，パス画像が事前に決定した配置位置に表示されるまで繰り返す．1 枚以上のパス画像が，正解である配置位置に表示されたら，その時点で回答確定とする．Pict Place Shuffle ではこの 2 つの入力方法を組み合わせて認証を行うものとする．以降では，前者の入力方法を “Drag 入力”，後者を “Shuffle 入力” と呼ぶ．

認証操作について説明する (**図 2**)．操作手順は以下の通りである．

(1) ユーザ名を入力する．入力後，図 2 左の画面が表示される．
(2) 秘密情報入力の第一段階として，Shuffle 入力による回答処理を行う．1 枚以上のパス画像が既定の表示位置になったら，認証画面下の “OK” ボタンを押して回答を確定する．図 2 中央の画面では，3 枚のパス画像のうち 1 枚が正しい位置に配置されたため，第一段階の入力完了となっている．
(3) 第二段階として Drag 入力による回答処理を行う．第一段階の回答で配置が未完了なパス画像について，Drag 入力によりすべてのパス画像が既定の位置に表示されるようにする．第一段階の入力終了時 (図 2 中央) では 3 枚の秘密画像のうち 2 枚がまだ既定の位置に配置されていない．よって Drag 入力により 2 枚のパス画像を移動し，最終的に 3 枚のパス画像がすべてを適切な位置に配置する (図 2 右)．
(4) 画面右下の “Login” ボタンを押し，入力を確定する．即座に検証処理が行われ，認証結果が表示される．

このように 2 種類の入力手法を用いて二段階の手順で秘密情報である「画像の配置」を入力し，個人認証を行う．

これら 2 つの工夫により期待される効果について述べる．まずはじめに理論的安全性の向上について述べる．秘密情報が「複数枚の画像配置」に変更されることにより，作成可能な秘密情報のバリエーション数は画像 3 枚の場合，式 (1) のようになる．

図 2　Pict Place Shuffle における回答入力

$$ {}_{10}\mathrm{C}_3 \times {}_{10}\mathrm{P}_3 = 120 \times 720 = 86,400 \qquad (1) $$

式 (1) 内第一項の組み合わせは配置位置のバリエーションであり，第二項の順列は画像の割り当て可能数に相当する．これにより画像 3 枚による秘密情報で 4 桁暗証番号よりも多くのバリエーション数が確保可能になる．よって理論的安全性の改善が可能になる．

次は，回答入力時間の短縮である．再認式画像認証における認証時間には「回答入力操作」と「パス画像の探索」という二つの要素が含まれ，その多くは「パス画像の探索」にかかる時間であると推測する．これに対して提案手法では「パス画像の配置位置」が秘密情報に含まれており，かつこれを応用した Shuffle 入力を導入したことから，「パス画像の探索」に相当する時間を削減しうると著者らは考えている．Pict Place Shuffle における Shuffle 入力では，認証時にパス画像を探すのではなく既定の配置位置のみに注目し，各位置にあるべきパス画像が表示されているかを検証する．もし一枚も適切な位置に表示されていなければ，回答候補画像群の配置をシャッフルし，前述の条件が満たされる配置になるまで繰り返すことになる．したがって，ユーザは回答候補である画像群からパス画像を探す必要がないことから上記効果が期待できると著者らは考えている．

なお回答操作の第二段階である Drag 入力では，従来通りパス画像を探索する必要がある．しかし，その探索領域は第一段階の Shuffle 入力により狭められていると言える．Drag 入力で移動させるべきパス画像は既定の位置以外の場所に存在することが明らかだからである．したがって，Drag 入力による操作時間に悪影響は限定的になると考えている．

最後に覗き見攻撃への対策について述べる．前述した通り覗き見攻撃が可能になる理由は，秘密情報を直接操作するためである．これに対して Pict Place Shuffle は，Shuffle 入力により秘密情報の一部を直接操作することなく回答可能である．したがって，Shuffle 入力により入力された秘密情報は攻撃者に覗き見されていたとしても特定困難である．よって Pict Place Shuffle は，1 回の覗き見攻撃で秘密情報を特定することはできない，という安全性を持つことになる[*1]．また覗き見攻撃による攻撃の成功確率は最悪の場合でも 1/10 となる．この確率値は，Shuffle 入力で 1 枚のパス画像が入力された場合の例となる．

これらの議論から，Pict Place Shuffle は 1 章で述べた 3 つの問題に対する改善策を備えた新たな再認式画像認証である．

表 1　実験参加者の性別・年代分布

	10 代	20 代	30 代	40 代	50 代
男性	0	8	0	1	1
女性	1	0	0	0	1

3. 評価実験と考察

本章では，Pict Place Shuffle の実用性を検証するために行なった少人数による評価実験と，先行研究と実験結果に関する比較議論について述べる．

3.1 評価実験

Pict Place Shuffle の実用性を検証するため，12 名による評価実験を実施した．実験目的は，秘密情報の記憶保持可能性と認証時間を明らかにすることである．実験参加者は所属研究室メンバおよび近親者から募集した．参加者の属性情報は表 1 の通りである．

実験手順は以下の通りである．

[*1] 攻撃主体が「人間」でも「カメラによる録画」でも同じである

表 2　秘密情報の記憶保持可能性に関する実験結果

手順 4 (30 分前後)	手順 5 (一週間後)
100% (12/12)	83% (10/12)

手順 1) 実験説明: 実験手順と Pict Place Shuffle の操作方法について説明を行った．

手順 2) 秘密情報登録: 2 章にて説明した方法にしたがって，参加者に秘密情報を設定させた．設定後には 1 度認証を実施させ，自身の秘密情報で認証に成功することを確認した．

手順 3) 記憶検証のためのタスクとアンケート: 秘密情報の記憶可能性を検証するため，短期記憶の消去を目的としてメンタルローテーションタスクを実施した．実際には文献 [7] にあるタスクを被験者に実施させた．またタスク完了後に人口統計に関するアンケートを実施した．

手順 4) 記憶実験: 上記手順 3) 終了後，Pict Place Shuffle による認証を行わせた．

手順 5) 記憶実験: 上記手順 4) 終了より 1 週間後に，あらためて Pict Place Shuffle による認証行為を実施し，認証成否と認証時間を記録した．なお 2 回までの認証失敗を許容し，3 回連続で認証に失敗したら認証失敗と判定した．

手順 6) 認証時間実験: 手順 4) 終了後に，Pict Place Shuffle での認証行為を 10 回認証成功するまで繰り返し実施させた．終了後，事後アンケートを実施した．

実験結果について述べる．秘密情報の記憶保持可能性については，手順 4 および 5 の認証成否を用いて検証する．認証に成功したら記憶保持できた，失敗したら記憶保持できなかった，として判定し，その結果を集計した．結果は**表 2** の通りである．この結果から，Pict Place Shuffle における秘密情報の記憶可能性について，実用的に利用することが困難な秘密情報ではない，と著者らは考える．

次に認証時間について述べる．手順 6 による実験から 120 回分 (12 名 ×10 回) の認証時間が測定できた．この結果から，平均 11.99(sec)，標準偏差 71.26，ならびに中央値は 10.08(sec) という結果を得た．

3.2　先行研究との比較

本節では，前節の実験で得られた結果，および定性的に得られると考えられる効果について先行研究との比較考察を行う．

まずはじめに再認式画像認証における安全性と認証時間について先行研究との比較を行う．ここでは先行研究事例として Déjà Vu[1] とあわせ絵 [2] を取り上げる．Déjà Vu は，25 枚の回答候補画像の中から 5 枚のパス画像を選択する再認式画像認証である．ただし Déjà Vu では，写真ではなくランダムアートと呼ばれる抽象的な画像を秘密情報に用いている．一方あわせ絵は，36 枚の回答候補画像の中から最大 4 枚の画像を選択する再認式画像認証で，秘密情報には写真を用いた手法となっている．これら 2 手法と Pict Place Shuffle における画像認証の設定値と秘密情報のバリエーション数ならびに平均認証時間をまとめると**表 3** の通りになる．

表 3　秘密情報の記憶保持可能性に関する実験結果

	Déjà Vu	あわせ絵	Pict Place Shuffle
回答候補画像数	25	36	10
パス画像数	5	4	3
秘密情報バリエーション数	53,130	9,999	86,400
平均認証時間 (s)	36.0	24.6	11.99

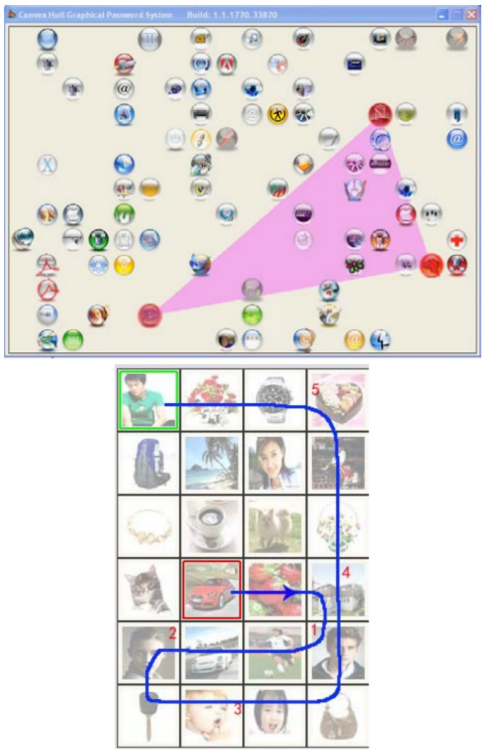

図 3　覗き見攻撃対策の先行研究例 (上: CHC, 下: CDS)

これらの結果から，各認証手法の安全性を秘密情報のバリエーション数の逆数と考えるとすると，Pict Place Shuffle は先行手法よりも少ないパス画像枚数で，3 手法の中で最も高い安全性を実現しているとともに，平均認証時間も他の手法よりも短い手法である，と言える．

次に覗き見攻撃への安全性と認証時間について先行研究との比較考察を行う．ここでは先行研究事例として Convex Hull Click Scheme (CHC)[5] と，Come from DAS and Story (CDS)[6] を取り上げる．どちらも再認式画像認証であるが覗き見攻撃への安全性を確保するため，回答方法に工夫を施した手法となっている．CHC は，パス画像によって生成できる多角形の内部をクリックすることにより間接的に秘密を入力する認証手法である (**図 3** 上)．CDS は，認証システムによって指定される始点と終点を線で結ぶのだ

表 4 覗き見対策手法における比較

	CHC	CDS	Pict Place Shuffle
平均認証時間 (s)	71.66	19.8	11.99

が，その際にパス画像を既定の順番にたどるよう線を描画することで間接的に秘密を入力する手法である (図 3 下)．

これらと Pict Place Shuffle における認証時間を**表 4** に示す．覗き見攻撃に対して確保しうる安全性が 3 手法で異なるため，これらの時間値を単純に比較するべきではない．ただし，それをふまえた上で以下のことが言えると著者らは考える．

(考察 1) CHC は，認証するのに 1 分以上の時間がかかる．よって覗き見攻撃に対する安全性が強く要求される場面以外では実用性に疑問の残る手法だと考える．

(考察 2) CDS の認証時間は実用性に疑問が生じるものではないと言える．ただし，CDS にはユーザの回答操作によって秘密情報が特定される懸念が指摘されている．ユーザは回答時にパス画像に到達するたびに線の描画を一時停止し，次のパス画像を探索するという操作をするからである．この操作だと，パス画像がどの画像かを覗き見している人に伝えてしまうことになるからである．

(考察 3) Pict Place Shuffle は，覗き見攻撃に対する対策となっている 3 手法の中で認証時間は最短であり，実用上の問題はないと考える．しかし，覗き見攻撃に対する安全性という点で考えると，その効果は 3 手法の中で最も限定的な対策と言わざるをえない．Pict Place Shuffle が提供する安全性は「1 回の覗き見に対して安全」であるため，CHC と対極的な位置付けになると言える．つまり安全性が強く要請される場面ならば CHC を採用するべきであり，安全性も必要だが，それよりも利便性が強く要請される場面では Pict Place Shuffle を採用するべき，ということだと考える．

4. おわりに

本論文では，知識照合型個人認証の改良法として提案されている再認式画像認証に注目し，その手法における 3 種の問題点を改善する新たな認証手法 Pict Place Shuffle を提案した．Pict Place Shuffle では，再認式画像認証における認証時のインタフェースに着目した新たな秘密情報を定義し，その秘密情報を活用した Shuffle 入力と呼ぶ回答入力方法を取り入れた二段階入力方法を提案した．この 2 つのアイデアにより，理論的安全性，認証時間，覗き見攻撃対策という問題に対する 1 つの改善策を提案することができたと言える．

またこの提案手法に対して実験参加者による評価実験を実施し，秘密情報の記憶可能性と認証操作時間に関する評価を行なった．さらにその実験結果について先行研究との比較議論を行い，既存の手法とは異なる改善策になりうることを示した．今後の課題としては，実験参加者による大規模の評価実験を行い，期待される効果の検証をあらためて行う．また覗き見攻撃の安全性についても評価実験を行うとともに，Drag 入力に関しても覗き見攻撃に対する安全性を確保しうる別の入力手法について検討する．

参考文献

[1] Dhamija, R. and Perrig, A.: Déjà Vu: a user study using images for authentication, *Proc. the 9th conference on USENIX Security Symposium*, (2000).
[2] 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).
[3] 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)．
[4] Stobert, E. and Biddle, R.: Memory retrieval and graphical passwords, *Proc. the Ninth Symposium on Usable Privacy and Security*(SOUPS'13), (2013).
[5] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, C.J.: Design and evaluation of a shoulder-surfing resistant graphical password scheme, *Proc. the working conference on Advanced visual interfaces*(AVI'06), pp.177-184, ACM(2006).
[6] Gao, H., Ren, Z., Chang, X., Liu, X. and Aickelin, U.: A New Graphical Password Scheme Resistant to Shoulder-Surfing, *Proc. 2010 International Conference on Cyberworlds*, IEEE(2010).
[7] Peters, M., Laeng, B., Latham, K., Jackson, M., Zaiyouna, R. and Richardson, C.: A Redrawn Vandenberg and Kuse Mental Rotations Test: Different Versions and Factors That Affect Performance, *Brain and Cognition*, Vol.28, pp.39-58(1995).