社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (64)
2007－CSEC－ 36 (64)
2007／3／2

間違い探しを利用したワンタイム・パスワード型画像認証の提案

小島 悠子*, 山本 匠**, 西垣 正勝***
*静岡大学情報学部 〒432-8011 静岡県浜松市城北 3-5-1
**静岡大学大学院情報学研究科 〒432-8011 静岡県浜松市城北 3-5-1
***静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市城北 3-5-1
E-mail: nisigaki@inf.shizuoka.ac.jp

あらまし
我々は，人間の有する「経験を活用する能力の高さ」をユーザ認証に応用する試みとして，「ウォーリーを探せ」をコンセプトとした画像認証方式を提案している．しかし本方式は，毎回の認証時に正解キャラクタを直接クリックすることにより認証を行う方式となっているため，認証行為を覗き見られると，認証システムそのものの安全性が消失してしまうという問題を残していた．そこで本稿では，本方式に「間違い探し」のコンセプトを融合させることによって，認証方式のワンタイム化を図る．本稿では，本方式の有効性を基礎実験により評価する．

Proposal of an Image-Based One-Time Authentication Scheme Using "Spot the difference"

Yuko Kojima*, Takumi Yamamoto**, Masakatsu Nishigaki***
* Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
** Graduate School of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
*** Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract
We have proposed an image-based user authentication system which is inspired by "Where's Waldo?". The system is using human characteristics; the second trial is easier than the first trial. However, the system has a drawback that by observing the legitimate users' authentication trial, it is very easy for illegal users to steal the authentication information, since legitimate user directly clicks on the place of the authentic character to complete authentication. Therefore this paper tries to enhance our authentication system by introducing a concept of "Spot the difference" so that the system can achieve one-time-password-type authentication. In this paper, the availability of the modified system is evaluated through basic experiments.

1. 背景

現行のユーザ認証方式は，汎用性と利便性の高さからパスワード方式が主流となっているが，人間にとって長くランダムな文字列を記憶することは容易ではない．そのため，近年，人間の記憶負荷を軽減する様々な認証方式が提案されてきている．人間の得意な画像認識能力を利用して記憶負荷を軽減させる画像認証方式[1,2]や自身のエピソードとパスワード情報を関連付けることで想起を容易にさせる認証方式[3]などがその好例である．著者らのグループも，人間の得意な画像の認識・識別能力に加え，過去に解いたことのある問題に再度直面した際に以前より速く解くことができるという「人間の経験を活用する能力の高さ」を利用した認証方式[4]を既に提案している．

本方式の詳細は2章で述べるが，文献[4]にて実施された基礎実験にて，問題を解いた経験を有する正規ユーザと経験を持たない攻撃者を，認証時間の差で切り分けることが十分可能であるという結果が得られている．しかし本方式は，毎回の認証時に問題の答えを直

接クリックするため，認証行為を覗き見されてしまうと，認証システムそのものの安全性が消失してしまうという問題を残していた．

そこで本稿では，本方式に「間違い探し」のコンセプトを融合させることによって，認証方式のワンタイム化を図る．提案方式の詳細は3章で述べる．そして，提案方式のプロトタイプシステムを実装し，基礎実験によって有効性の検証を行った結果を4章に示す．最後に5章で本稿をまとめる．

2. 経験による想起の容易さを利用した認証方式

本章では，我々が既に提案している「経験による想起の容易さを利用した認証方式[4]（以下，既存方式）」の説明を行う．既存方式は，多数の紛らわしい人物たちの中から，ある特定の人物を探し出すというパズル絵本の「ウォーリーを探せ」[5]より着想を得ている．

既存方式の登録フェーズでは，ユーザはある特定のキャラクタを選び，これを正解キャラクタとして登録する．認証システムは，多数のキャラクタをランダムな位置に配置した画面（図1）を生成して，ユーザに提示する．この画面の中のどこかに正解キャラクタが隠れている．ユーザは，正解キャラクタを多数の類似したキャラクタ群の中から選びだすというパズル問題を解いておく．認証フェーズでは，登録フェーズと全く同じ画面（図1）が提示される．制限時間以内にこのパズル問題を解くことができた場合に(正解キャラクタの位置を回答できれば)本人として認証される．

正規ユーザは登録フェーズにおいて一度パズルを解いた経験があるため，認証フェーズで素早く正解キャラクタを探し出し，その位置を回答することができる．正規ユーザ以外は，たとえ正解キャラクタを推測できたとしても，初見でパズル問題を制限時間内に解くことは困難である．このように既存方式では，「パズル問題を解いたことがあるか否か」という経験の差を利用して本人認証が実現されている．具体的には，この「経験」の有無による回答時間の差で正規ユーザと攻撃者を切り分けている．

文献[4]の基礎実験より，正解キャラクタを見つけるまでの所要時間は，登録フェーズ（パズル問題を初めて解く場合）よりも認証フェーズ（過去に解いたことのあるパズル問題を再び解く場合）のほうが十分に短いことが確かめられている．また，登録フェーズから2週間が経過した時点においても，この結果に変わりはなかった．

しかし既存方式は，毎回の認証時に正解キャラクタを直接クリックすることにより認証を行う方式となっているため，認証行為を覗き見されてしまうと，正解キャラクタとその位置が漏洩する危険性があり，認証システムそのものの安全性が消失しかねないという問題を有している．

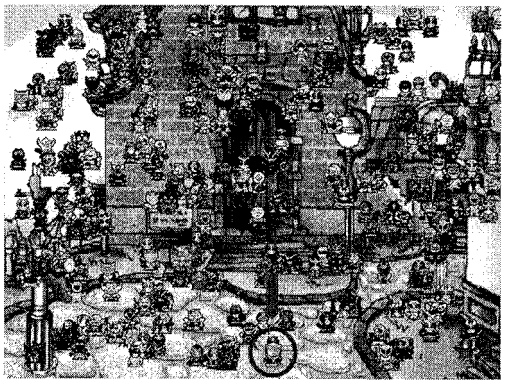

図1　既存方式の認証画面

3. 提案方式

3.1 アプローチ

既存方式では，常に同じ位置にある正解キャラクタを直接クリックするため，覗き見攻撃に脆弱であるという問題を残していた．そこで提案方式では，入力をワンタイム化することによりこの問題の解決を試みる．

具体的には，既存方式に「間違い探し」のコンセプトを融合する．登録フェーズでは，ユーザに複数のキャラクタを記憶してもらった上で，それら登録キャラクタが配置された絵を作成してもらう．認証フェーズにおいては，登録時に作成した絵とその鏡像の絵☆を左右に並べてユーザに提示する．その際，鏡像の絵の中の一部のキャラクタに間違いを混入する．ここで「間違い」とは，鏡像の絵におけるキャラクタのポーズや色を変化させること，またはキャラクタ自体を変化させることを意味する．間違いが混入されたキャラクタに対しては，左右の絵において対応するキャラクタが「非

☆ 2つの絵を同じ向きに並べた間違い探しの場合，ステレオグラムを見る際と同様に立体視をすれば異なる部分を容易に見つけることができると言われている．そのため，本システムでは，鏡像にした2枚の画像を利用する．

対称」となる．どのキャラクタに間違いを混入させるか，何体のキャラクタに間違いを混入させるかは，認証毎にランダムに変化する．ユーザは，左右の絵における間違い（左右の絵において非対称である登録キャラクタ）の数を答えることによって，認証を行う．絵の中には，ユーザが記憶する登録キャラクタだけでなく，他のキャラクタ（囮キャラクタ）も配置される．囮キャラクタにも登録キャラクタと同じ確率で間違いが混入されるようになっており，これにより，攻撃者から登録キャラクタを隠すことができている．

正規ユーザは，認証時に，自分が記憶している登録キャラクタのみに対して，左右2枚の絵の比較を行うだけでよいため，間違いの数を容易に数え上げることができる．登録の際に認証の練習を何回か繰り返して「経験」を積んでおいてもらうことで，認証フェーズに非対称となっている登録キャラクタを探す作業は正規ユーザにとって更に簡単なものになるであろう．また，その場で左右の絵を見比べれば間違いが分かるので，正規ユーザは登録キャラクタの細部まで記憶する必要はない．このように，本提案方式は人間が得意としている「経験を生かす能力」と「画像をあいまいに記憶する能力」の両方を利用した認証方式になっていると言える．

一方，どれが登録キャラクタなのか知らない不正者は，すべてのキャラクタに対して，そのキャラクタが登録キャラクタであるのか囮キャラクタであるかの推測をした上で，左右の絵の比較をしなければならず，非常に手間がかかることになる．

3.2 認証システムの実装

本提案方式の登録・認証の手順を以下に示す．

● 登録フェーズ

【Step1】ユーザは背景及び幾つかのキャラクタを選択し，背景上の記憶しやすい場所にキャラクタを配置する(図2)．

【Step2】システムはユーザが登録キャラクタを配置した画像に，多数の囮キャラクタをランダムに配置する(図3)．

【Step3】ユーザは納得がいく配置であれば，その画像を登録する．そうでない場合は，Step2をやり直す．

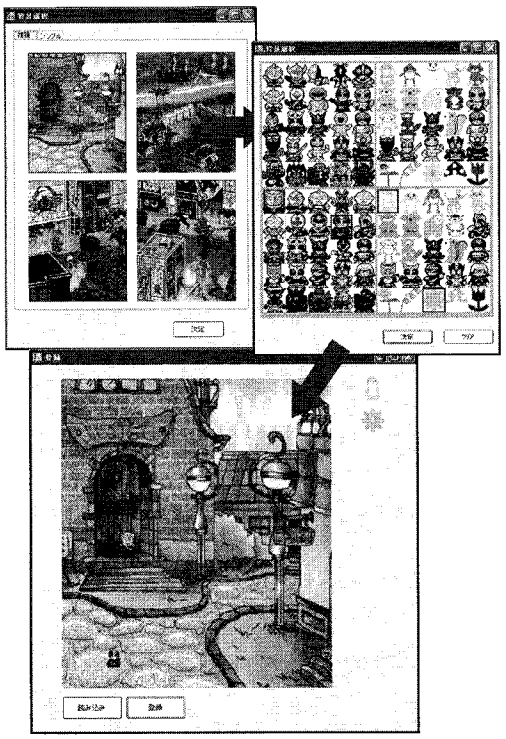

図2　登録手順（背景及び登録キャラクタの選択，登録キャラクタの配置）

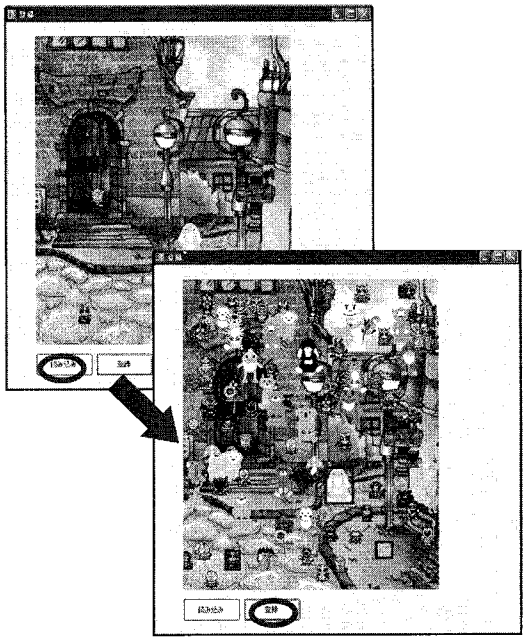

図3　登録手順（囮キャラクタの配置）

● 認証フェーズ

【Step1】システムは登録画像を左側に，登録画像の鏡像画像を右側に並べ，ユーザに表示する．ここで，鏡像画像においては，一部のキャラクタに間違いが混入される．登録キャラクタにも囮キャラクタにも同じように間違いが混入され得る．間違いが混入されるキャラクタは，認証毎にランダムに選ばれる．

【Step2】ユーザは左右の 2 枚の絵を比較し，登録キャラクタの中で間違いが含まれているキャラクタ(左右の画像において非対称になっている登録キャラクタ）の数を数え上げ，これを回答としてシステムに入力する(図 4)．

【Step3】ユーザが正しい数を返答することができれば認証成功とする．

登録するキャラクタの数，登録キャラクタと一緒に表示される囮キャラクタの数，認証フェーズにおける間違い探しの繰り返し回数(ターン数)などは，要求される認証強度に応じて定められる．

4. 基礎実験

提案方式のプロトタイプシステムを実装し，提案方式の有効性を基礎実験を通じて評価する．

4.1 本人認証の実験

被験者は，本学情報系学部の学生 12 名である．ユーザが登録時に自ら選択・配置した登録キャラクタを，一定期間後の認証時においても記憶しており，さらに，容易に間違いを見つけることができるかどうかを検証する．

● 実験方法

本実験システムでは，正規ユーザが記憶すべき登録キャラクタの数を 4 体，登録キャラクタと一緒に表示する囮キャラクタの数を 96 体とし，認証フェーズ（100 体のキャラクタの中に紛れている登録キャラクタの間違いの数を入力する）を 6 ターン行って 1 回の認証とするシステムを構築した．実験に用いたキャラクタの画像はインターネット上で公開されている画像[6]などから収集した．なお，本稿の図中に示した画像は，作者により自由な使用が認められている画像である．

被験者は実験初日（登録フェーズ）に，背景及び登録キャラクタを選択し，登録キャラクタの配置を行う．4 体のキャラクタはそれぞれ異なるものとする．登録キャラクタが配置された後，システムは囮キャラクタを配置し，登録画像を生成する．この時点で，被験者は登録画像の確認を兼ね，認証作業の練習を行う．この作業は被験者の納得がいくまで行うことができる．これにより，被験者は間違い探しの経験を得ることができる．

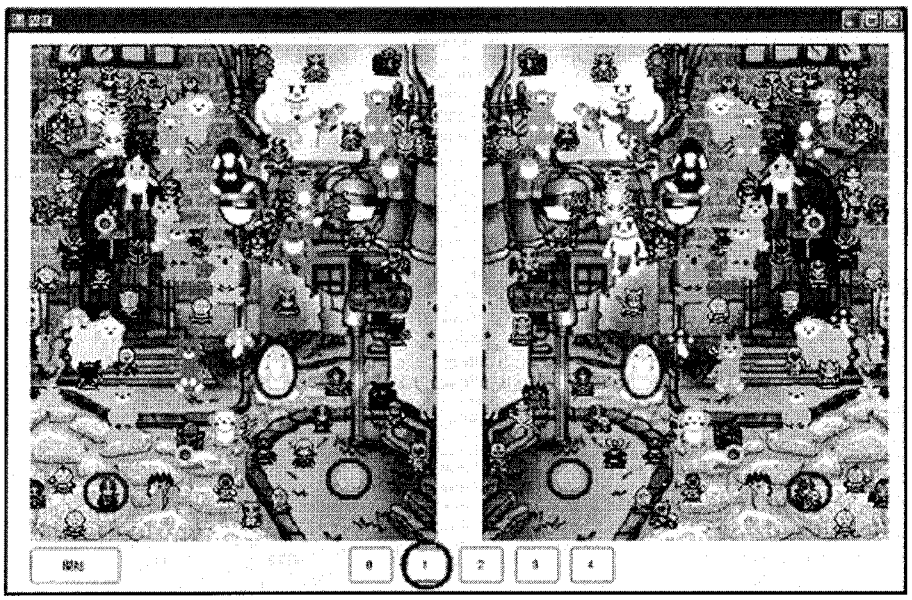

図 4　認証手順

被験者にはその後，登録日の翌日，1 週間後，2 週間後，1 ヵ月後に 5 回ずつ認証を行ってもらう．なお，登録日より後には，被験者は自分の登録キャラクタを確認することはできない．

● 実験結果

実験結果を表 1 に示す．表中，「認証成功率」は 12 名の各被験者につき 5 回ずつ行った認証試行の全体の成功率（1 回の認証において，6 ターンの間違い探し全てに成功した割合）を表し，「入力正答率」とは，各認証試行時に行う 6 ターンの間違い探し（100 体のキャラクタの中に紛れる登録キャラクタの間違いの数を答えるタスク）を独立にとらえ，1 ターンごとの成功率を表したものである．「平均認証時間」は 1 回（6 ターン）の認証に要した時間の平均である．

表 1．本人認証実験の結果

実験日	認証 成功率	入力 正答率	平均認証 時間(s)
翌日	58/60(96.7%)	357/360(99.2%)	30.5
1 週間後	58/60(96.7)	358/360(99.4)	27.3
2 週間後	58/60(96.7)	356/360(98.9)	25.2
1 ヶ月後	59/60(98.3)	359/360(99.7)	26.0

表 1 より，翌日，1 週間後，2 週間後，1 ヵ月後ともほぼ確実に本人認証に成功していることがわかる．認証に失敗したケースも見られたが，失敗した被験者からの聞き取り調査からは，登録キャラクタを忘れていたのではなく，入力ミスによるものであることがわかった．また，このことは，入力正答率の高さからも推測することができる．

平均認証時間に注目すると，前回の認証から長時間経過していたとしても，著しく認証に要する時間が長くなることはなかった．以上の結果から，まだ被験者数は少ないものの，提案方式の利用可能性が示された．ただし，6 回という入力回数は多いと感じた被験者が多かったため，入力回数を削減することが今後の課題である．

4.2 攻撃実験

提案方式における安全性を検証する．今回の実験は特に覗き見攻撃による脅威を調べることが目的である．提案方式は正規ユーザの肩越しに認証行為を直接覗き見るタイプの攻撃については十分な耐性を有しているものと判断し，攻撃者により有利な条件の実験環境になるように設定した．また，正規ユーザ役の実験実施者と攻撃者役の被験者との間に面識がある場合とない場合とに分けて実験を行うことにより，攻撃者が正規ユーザに関する情報を推測し，なりすましを試みる推測攻撃（Educated Guess 攻撃）の脅威も検証した．

● 実験方法

攻撃者役の被験者は，本学情報系学部の学生 11 名である．この 11 名は 4.1 節に示した 1 ヵ月間の本人認証の実験を既に行っており，本認証システムについての知識を十分に持っている．正規ユーザ役の実験実施者は本学情報系学部の学生 1 名（ユーザ A）と他大学の学生 1 名（ユーザ B）である．ユーザ A は被験者と同じ研究室に所属している学生であり，すべての被験者と少なくとも 9 ヵ月間の交流がある．ユーザ B は被験者との面識は無い．実験では 11 名の被験者を 2 つのグループ（5 名と 6 名）に分け，1 つ目のグループは「ユーザ A→ユーザ B」の順序で攻撃実験を行ってもらう．2 つ目のグループはその逆の順で実験を行ってもらう．

実験システムは 4.1 節のものと同じであるが，本実験では実際のシステムを用いるのではなく，認証画面のカラー印刷画像を利用する．すなわち被験者には，実験実施者（ユーザ A およびユーザ B）の 1 回の認証における 6 ターン分の認証画面のカラー印刷画像 6 枚が，実験実施者の回答とともに配布される．また，攻撃を効率的に実施してもらうために，被験者にはクリアファイルとペンを与え，クリアファイルに認証画面のカラー画像を代わる代わる挟み込みながら，クリアファイルに印などを書き込むことによって，6 枚の認証画面の画像比較を簡便に行うことができるよう配慮した．メモ帳の使用も許した．

被験者には実験を開始する前に，本システムにおいては「間違いの数が 0 であるという回答であった場合には左右非対称なキャラクタは全て囮キャラクタと判断でき，回答が 4 であった場合には左右対称なキャラクタは全て囮キャラクタであると判断できるため，登録キャラクタの候補を絞り込むことが可能である」という情報を与えた．その後，6 枚の認証画面のカラー画像および実験実施者の回答，クリアファイル，ペン，メモ帳を同時に渡し，15 分間自由に登録キャラクタを探してもらった．15 分経過後，6 枚の認証画面を回収し，登録画面を印刷したカラー画像を渡す．被験者には，登録画面のカラー画像と 15 分の間にクリアファイルやメモ帳に書き留めた情報とを照らし合わせ，実

験実施者（ユーザAおよびユーザB）の登録キャラクタの組み合わせ(4体)の候補を5通り回答してもらう．

● 実験結果

実験結果を表2に示す．表中，「なりすまし成功率」は，11名の攻撃者の中で登録キャラクタ4体の組み合わせを正確に回答できた人の割合を示す．「推測に成功したキャラクタ数の平均」は，5通りの回答それぞれにおいて平均何体の登録キャラクタを推測することができたかを記したものである．

表2 なりすまし成功率

	ユーザA	ユーザB
被験者との面識	あり	なし
なりすまし成功率	2/11(18.2%)	0/11(0%)
推測に成功したキャラクタ数の平均	1.85体	1.20体

表2より，登録キャラクタ4体の組み合わせを正確に回答できた者は2人だけであった．ただし，実験後にこの2人に聞き取り調査を行ったところ，幾つかの候補にまでは絞り込むことはできたが，登録キャラクタ4体を一意に絞り込めたわけではないということがわかった．

今回の実験では，1回分（6ターン）の認証画面全てを印刷して与えるという攻撃者に非常に有利な条件下でも，なりすまし成功率を20%弱にまで抑えることができている．このことから，提案方式が覗き見攻撃の耐性を有していると考えることができる．

面識の有無による登録キャラクタの推測のし易さに関しては，若干ではあるが，面識のある正規ユーザ役へのなりすまし成功率（ユーザA）の方が面識の無い場合（ユーザB）よりも高くなっている．これは，攻撃者が正規ユーザの情報を，登録キャラクタの推測に活用できたからであると解釈することができる．しかしながら，実験後の聞き取り調査からは，面識の無い正規ユーザ役の被験者が選択した登録キャラクタには，気付くことが難しい（攻撃者役の被験者が，そのキャラクタを背景の一部と見間違えてしまった）ものも含まれていたという意見もあり，今回の結果が推測攻撃の影響を反映したものであると言い切ることはできないという結果であった．

今後は，覗き見攻撃や推測攻撃による脅威の検証だけでなく，登録キャラクタの種類及び配置の仕方が，提案方式の安全性にどのように影響を与えるかということも検討していく必要がある．また，今回は1回（6ターン）分の認証の覗き見を想定した攻撃実験であったが，複数回の認証を覗き見された場合の攻撃耐性についても検証していかなければならない．

5. おわりに

本稿では，経験による想起の容易さを利用した認証方式をベースに，「間違い探し」のコンセプトを導入することにより，認証方式のワンタイム化を実現した．さらに，プロトタイプシステムを実装し，本人認証および覗き見攻撃に関する基礎実験を行い，本方式の有効性を示した．

参考文献

[1] Rachna Dhamija, Adrian Perrig: Déjà Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, pp.45-58, 2002.

[2] Trevor Pering, Murali Sundar, John Light, and Roy Want: Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, Vol 2. No 1, pp.30-36, (Jan 2003).

[3] 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.2002-2012，2002年8月．

[4] 花井將臣，中村逸一，吉田英樹，曽我正和，西垣正勝：経験による想起の容易さを利用した認証方式，情報処理学会研究報告，2004-CSEC-24-34，pp.193-198，2004年3月．

[5] Martin Handford 著，唐沢 則幸 訳：新ウォーリーを探せ！，フレーベル館，2000年

[6] けらちん：ほそ目のCURSOR(キャラクタ素材)，http://earth.endless.ne.jp/users/keira/