L-015

画像の劣化を用いた認証システムの開発と検証
Development and evaluation of the authentication system with image degradation

中野翔太 †
Shota Nakano

小林孝史 ‡
Takashi Kobayashi

1. 背景

World Wide Web の発達によって，インターネットを介して，世界中で数多くの Web サービスが提供されるようになったが，そのサービスを利用するために必要なものとしてユーザアカウントがある．そのユーザアカウントの多くはメールアドレスとパスワードによってそのサービスを利用するための真正性を保証している．また，現代のインターネットにおいて一人のユーザが一つだけのアカウントを持っていることは少なく，ユーザは複数のアカウントを使い分け，複数のパスワードを管理していることになる．真正性を確保し続けるためにはユーザアカウントが乗っ取られないための対策が必要であり，その対策のうち最も有効な手段が，サービスごとに利用するパスワードを異なるものにすることである．

しかし，人間の記憶力には限界があり，数多くのサービスですべて異なるパスワードにすることは現実的ではない．パスワードの忘却を防止するためにパスワードのメモを取る行為は攻撃者にとっての格好の的になり，アカウントハックの標的になりやすくなる．そのため，ほぼ必然的にパスワードの使いまわしが発生する．ゆえに，ユーザアカウントが悪意のある第三者に乗っ取られたとき，同一のパスワードで利用者のアカウントの多くを乗っ取ることができ，被害は大きくなりがちであり，パスワード以外の認証方式について数多くの検討がなされているが，パスワードの運用の容易さから，依然パスワードが多く利用されている．そこで本研究では，コンピュータについての高度な知識を有していないユーザでも利用でき，なおかつ人間が記憶しやすい「画像」を鍵とした安全な認証方式を提案する．

1.1. 目的

現在ではパスワードによる認証が認証方式の大半を占めている．しかし，利用者にとって重要なサービスにおいても簡易なパスワードを許可するようなサービスも多く存在している．そのため，パスワードによる認証を突破できた場合の利用者への被害も深刻になる．

また，現代の計算機の高性能化によって，比較的短時間でパスワードの解析が行えるようになった．そのため，パスワードのハッシュを保存するファイルが漏えいした場合に，昔よりも短時間でパスワードの解析が行える状況にあり，パスワードを頻繁に変更しなければ，アカウント乗っ取りの被害に遭うことが予想される．しかし，パスワードを頻繁に変更することやサービスごとにパスワードを変更することが難しいのは前章で述べたとおりである．

†関西大学大学院 総合情報学研究科 知識情報学専攻
‡関西大学 総合情報学部 准教授

そのため今回の提案手法ではパスワードの代替としての認証方法を提案するものであり，パスワードよりも攻撃者に解析されにくく，なおかつ利用者にとって記憶しやすく，さらに鍵の利用頻度を視覚的に判断でき，変更のタイミングをとらえやすいものを考えた．

2. 関連研究

小島の研究 [1] では，パス画像と囮画像を配置し，その中からパス画像を見つけ出して認証を行う方法を検討した．この手法の特徴として，パス画像をより効率的に探索するため「あみだくじ」を利用し，パス画像を見つけ出すことで，覗き見耐性を高めた．

このシステムはパス画像と囮画像が混合された画像群の中から 1 枚のパス画像を見つけ出し，認証を行うが，これを複数のシステムで利用することを考えた場合，大量の画像群の中から一枚の画像を見つけ出す必要があるため，記憶負荷が大きくなることが考えられる．

この研究の目的は記憶負荷を軽減することであり，同程度の認証強度を持つパスワードと比較すると， パスワードよりも記憶負荷を軽減させることを実現した．

3. 提案手法

コンピュータ上の静止画表現として，画像ファイルがある．画像ファイルは，各画素 (ピクセル/pixel) に RGB(Red，Green，Blue) やそれに加えて透明度を示すアルファ値などの情報を持つことができる．また，画像ファイルのサイズを圧縮するために近隣のピクセルの情報との差分を持たせることもできる．画像ファイルはそのピクセル情報を書き換えることによって，その画像を編集することが可能である．提案手法では画像ファイルを利用する．画像を劣化させ，その劣化した画像を認証の鍵 (以下，鍵画像) とする．図 1に提案手法のねらいを示す．画像はファイルであるため，オンラインストレージサービスなどファイルの同期を行うことで，複数の端末でも認証が利用できる．

また提案手法はファイルをアップロードすることが可能な Web ブラウザから利用できるようにし，幅広く提案手法を利用できるようにしたいと考えた．

3.1. 画像の劣化について

提案手法では認証を行うたびに画像を劣化させる．画像の劣化とは，画像が不可逆に変化し，元の状態に戻すことが困難であるものを指す．

3.1.1. 劣化に用いるフィルタについて

画像の劣化を行う際に，その画像にどのような劣化処理を施すかが問題になる．ここでは画像をどのように劣化させるかを「フィルタ」と呼ぶ．今回は HSB フィルタ，ぼかしフィルタ 2 種，ノイズフィルタを利用した．

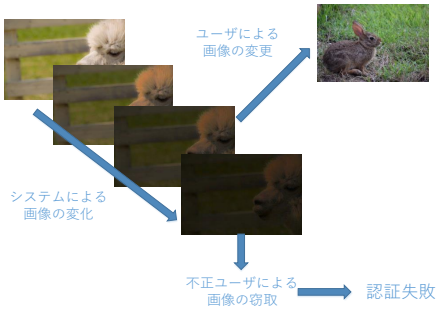

図 1: 提案手法のねらい

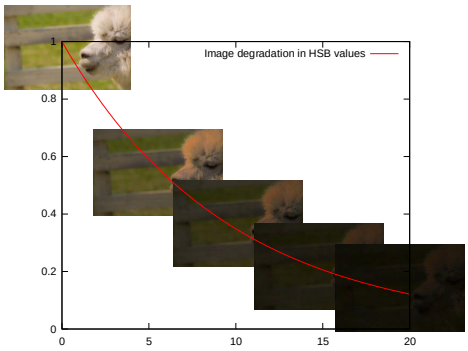

図 2: HSB フィルタによる画像劣化例 (画像劣化グラフ)

HSB フィルタ　画像の HSB 値を減らすフィルタである．HSB 値とは Hue，Saturation，Brightness(色相，彩度，輝度) を表すもので，RGB 値より人間にとって直感的にわかりやすい色表現である．認証のたびに画像の HSB 値を減らし，画像をだんだんと暗くさせる．今回は画像の各画素に対して HSB 各値について 0.9 倍することにした．図 2に画像の劣化を行った際の画像の HSB 値を示すグラフを示し，実際に画像がどのように劣化していくかを図3に示す．

ぼかしフィルタ　画像にランダムなぼかし効果を与える．ぼかしフィルタにはその効果がわかりやすいものと分かりにくいものの二種類を使用した．図5，6が適用例である．

ノイズフィルタ　画像にランダムなノイズを発生させる．図7が適用例である．

3.2. 可用性の検討

提案手法は，ファイルをアップロードすることが可能な Web ブラウザから利用でき，高い可用性を実現することを目標とした．その際，劣化した画像をどのように利用者が複数の端末で利用するかが問題となった．オンラインストレージサービスを利用したファイル同期を利用して，異なる計算機環境でのファイル同期を実現した．オンラインストレージサービスを利用するためにはその端末に専用のソフトウェアをインストールする必要があり，また，その端末にソフトウェアを

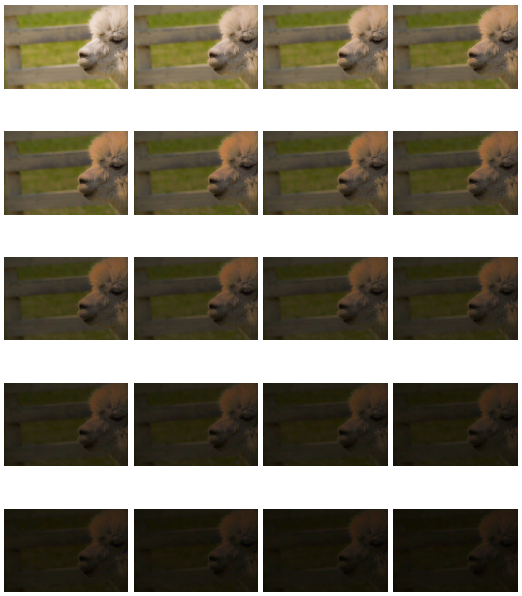

図 3: HSB フィルタによる画像劣化例 (連続的提示)

インストールするだけでは利用できず，その端末においてオンラインストレージサービスを利用するための認証が発生し，その端末を信頼するかどうかを利用者に尋ねるため，利用者が信頼した端末だけでファイル同期が行われることになる．そのストレージにファイルを鍵画像ファイルを配置することによって，利用者は信頼した端末上であればこの認証システムを利用することができる．また，オンラインストレージサービスの可用性は非常に高く，可用性を示す基本的な指標である稼働率は，多くのサービスで軒並み 99.9%と非常に高い．これは，オンラインストレージサービスが大規模な冗長化機能を備えているためである．

3.3. 認証強度の検討

提案手法の認証強度について考える．総当たり攻撃に対するパスワードのパターン数は 利用できる文字種×長さ となるが，画像認証の場合，ピクセル数(縦×横)×ビット深度 となり，パスワードよりも非常に大きくなる．ファイル数によって認証強度を検討する場合，ある時点でのファイル数がそのまま認証強度になる．暗証番号などの選択できるパターン数が少なく，認証失敗率が低い認証システムでは，少ない認証失敗回数で異常な認証試行であることがわかる．それと同様に，選択できる画像ファイル数自体はパスワードの総組み合わせ数より少なく，人間の画像に関する記憶能力の高さを考えると，暗証番号と同様に少ない認証失敗回数で認証の異常を検知することができる．異常な認証が行われている場合，利用者に通知したり，そのユーザ ID をロックしたりなどと様々なことが考えられる．

パスワードは利用期間が長くなればなるほど，窃取される恐れが高くなるが，提案手法は鍵情報が認証のたびに変化するため，パスワードのように全く同じ認証情報が長期間利用されることがないため，窃取に対する耐性もある．

提案手法は利用するサービスが増えるほど，鍵画像，鍵画像だったもの，関係のない画像が増加し，強度が増す．対するパスワードは利用するサービスが増えるほど管理すべきパスワードが増加し，記憶負荷が高まることによってパスワードの使いまわし，記録が発生し，インシデントの原因になり，結果として認証としての強度が低くなる．

提案手法は所持物による認証に近いものである．この認証方式を補強するものとして知識認証であるパスワードを利用することで，より強固な認証方式になるが，本論文では画像のみを取り扱う．

3.4. 鍵画像の漏えいに対する対処

鍵画像が何らかの方法によって窃取，漏えいしてしまった場合，提案手法では認証のたびに鍵画像が変化するため，窃取した後，正規の認証を行うことができれば，鍵画像は更新され，窃取された画像は鍵画像ではなくなるため認証には利用できなくなる．この変化する鍵画像の特性は，コンピュータ内のストレージに鍵を格納する，パスワードなしの非対称鍵認証より優れているものであると考える．また，正規の認証を行う前に不正利用者が認証を行った場合，パスワードと同様に正規利用者は新しく鍵画像を作成する必要がある．

3.5. システムの開発について

本提案手法が実際にシステムに利用することができるかどうかを検証するために，認証システムを開発した．この認証システムは Ruby on Rails 4.0 を Web アプリケーションフレームワークとして利用した．数多の採用実績がある Ruby on Rails を利用することで高い移植性を期待できるためである．

また画像にフィルタをかける際に，画像編集をコマンドラインで行うことができるソフトウェアである ImageMagick を利用し，それを Ruby で利用できるラッパーライブラリである RMagick を利用した．

現在，Internet Explorer や Mozilla Firefox などの複数のブラウザがあり，そのレンダリングエンジンの違いによって，HTML や CSS，Javascript の解釈が異なり，ブラウザごとに表示の違いが現れる．ブラウザ間の表示誤差をなるべく小さくするために CSS フレームワークである Twitter Bootstrap[2] を利用した．

3.5.1.RMagick について

RMagick[3] とは ImageMagick を Ruby で利用するためのラッパーライブラリである．
ImageMagick は画像編集をコマンドラインやプログラム上で行うためのツールおよび API のことで，RMagick を用いることで Ruby プログラム上で画像を簡単に編集することができる．図 4，5，6，7は左から，メソッド適用前，メソッド 1 回適用後，メソッド 10 回適用後の順に並んでいる．

4. 評価実験

提案手法の有効性を検証するために，まず，現代的な環境を想定し，実験することを決定した．

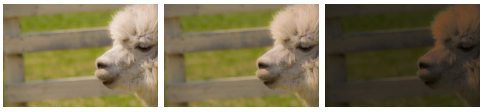

図 4: HSB フィルタ適用前後の画像

図 5: ぼかしフィルタ 1 適用前後の画像

実験では 4 つのユーザ ID とパスワード (8 文字以上英数字記号混合必須) を被験者に記憶させ，また同様に 4 つのユーザ ID と鍵画像を記憶させ，合計 8 つの認証情報を被験者は記憶する．これらの認証情報を 5 日間開けて，再生テストを行い，これを 4 回繰り返す．また，パスワードが漏えいしたという前提で，実験の 2 回目が終了した時点でパスワード 2 種類を変更させる．認証後に各認証方法について，利用者が認証情報を容易に想起することができたかどうかを利用者の主観で評価させる．

実験では被験者の操作時刻と認証状態 (開始，失敗，忘失，成功)，認証種別 (パスワード，画像) を記録した．今回の実験は以下に示す手順で実行される．

4.1. 認証情報登録フェーズ

認証実験を行う際に，鍵情報をシステムに登録する必要がある．

1. システムを利用する際，登録画面が表示され，ブラウザのファイルアップロード機能を利用し，画像を選択する．
2. 鍵画像がシステムに登録される．その際，システムから新しい鍵画像へのリンクが表示されるため，その新しい鍵画像を上書き保存する．

4.2. 認証フェーズ

登録された認証情報を用いて認証を行う．

図8に示す画面が認証画面である．ここに被験者が記憶している認証情報を入力する．

認証に成功した場合，認証が成功したというメッセージが画面に表示され，システムは鍵画像の更新を行う．その際，登録画面と同様にシステムから新しい鍵画像へのリンクが表示されるため，その新しい鍵画像を上書き保存する．

また，認証に失敗した場合は，再度認証を要求する．その際,「認証に失敗した」というログが記録される．

5. 実験結果

今回の実験では 20 歳から 24 歳の学生 19 人の協力を得ることができた．パスワード 4 種類の認証失敗回数と，画像認証の認証失敗回数を表 1に示す．また，各種

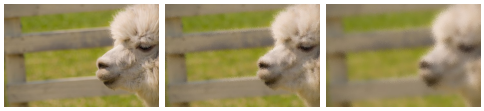

図 6: ぼかしフィルタ 2 適用前後の画像

図 7: ノイズフィルタ適用前後の画像

法ごとの認証試行 1 回あたりの所要時間，認証試行回数，認証失敗回数，認証情報忘失回数，試行回数における失敗回数の割合を表 2に示す.

5.1. 認証に関するアンケート調査の分析

提案手法の有効性を検証するため，被験者にアンケート調査を行った.

5.1.1. パスワードについてのアンケート結果

そもそも，利用者がパスワードを使いまわしている，もしくはパスワードをしばしば忘れることがなければ，本システムの優位性があるとは言えない．よって，被験者にパスワードをよく忘れるか，パスワードを使いまわしているか，パスワードは定期的に変更しているか，複数種類のパスワードを記憶することは苦痛であるか，パスワード漏えいの際，パスワードを変更するかどうかを調査した.

表3〜7より，利用者はパスワードを使いまわしており，パスワードを複数種類記憶することは苦痛であると感じ，パスワードが漏えいした場合にはパスワードを変更するが，サービスの価値によっては変更しないことがあるということがわかった.

5.1.2. 画像についてのアンケート調査の結果

提案手法は利用者が画像を保持していることが認証を行うための条件になる．そのため，利用者が画像を収集することに積極的であるかどうかを調査した．表8によると，過半数が画像を積極的に収集していることがわかる．そのため，提案手法で用いる画像は利用者側で用意することが可能であるケースが多いことが考えられる.

5.2. 実験後アンケートの分析

実験では，認証完了後にアンケートを行った．その結果を以下に示す.

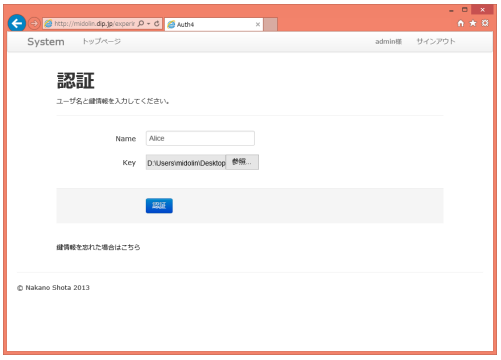

図 8: 認証画面

表 1: 実験結果の比較

手法	パスワード	提案手法
試行回数	571	471
失敗回数	280	152
忘失数	70	23
平均所要時間 (秒)	17.03	29.66

5.2.1. パスワード認証の実験後アンケートの結果

パスワード認証を行った後に，そのパスワードを正確に記憶し，それを思い出すことができたかどうかを質問した．表9より，被験者は 4 種類のパスワードを正確にで記憶できていると考えていることがわかる.

5.2.2. 提案手法の実験後アンケートの結果

画像認証を行った後に，劣化した画像はすぐに見つけることができたか，画像の劣化に対して嫌悪感があったか，手法についての感想，意見を質問した．表10の結果から，鍵画像はすぐに見つけることができているとわかる．また，11の結果から，提案手法全体としてみると，画像の劣化に対して嫌悪感は大きくないことがわかる.

5.2.3. フィルタごとの結果の比較

各フィルタごとの結果について検討する．なお，表 12，13，14，15 の質問項目は表10，11と同じもので，それを各フィルタごとに集計したものである.

HSB フィルタ　HSB フィルタの実験後アンケート結果は表 12のようになった．このフィルタでは，画像の劣化に気付かないとの意見が複数あった.

ぼかしフィルタ 1　ぼかしフィルタ 1 の実験後アンケート結果は表13のようになった．このフィルタでも同様に，画像の劣化に気付かないという意見があり，画像の劣化に気付いたとの意見はごく少数だった.

表 2: 実験結果の詳細

手法	所要時間 (秒)	試行回数	失敗回数	忘失回数	失敗の割合
パスワード 1	17.06	187	105	18	0.5615
パスワード 2	15.57	139	71	15	0.5108
パスワード 3	21.01	132	61	16	0.4621
パスワード 4	14.50	113	43	21	0.3805
HSB フィルタ (図 4)	29.91	158	57	7	0.3608
ぼかしフィルタ 1(図5)	27.63	117	47	5	0.4017
ぼかしフィルタ 2(図6)	35.99	107	30	5	0.2804
ノイズフィルタ (図7)	25.13	89	18	6	0.2022

表 3: 設問「パスワードをよく忘れますか」に対する回答

回答	回答数
非常によく忘れる 1	1
2	6
3	6
4	6
忘れたことはない 5	2

表 4: 設問「あなたはパスワードを使いまわしていますか」に対する回答

回答	回答数
ほとんど使いまわしている 1	7
2	7
3	4
4	2
使いまわしていない 5	1

ぼかしフィルタ 2　ぼかしフィルタ 2 の実験後アンケート結果は表 14のようになった．上述の 2 種類のフィルタと比較して，被験者は嫌悪感を示していることがわかる．このフィルタでは，画像の劣化に気付いた被験者が少なからず存在していた．

ノイズフィルタ　ノイズフィルタの実験後アンケート結果は表15のようになった．上の 3 つのフィルタと比較して，被験者の嫌悪感の差は大きく出たが，鍵画像をより早く発見できるようになったと回答していることがわかる．このフィルタはほかのフィルタとは異なり，被験者の多くが画像の劣化に気付いていた．

5.3. 実験結果の分析

実験結果から提案手法の認証失敗回数がパスワード認証の認証失敗回数よりも少ないことがわかる．さらに，認証失敗回数，認証情報忘失数は半分程度になっていることが確認できる．また，平均認証所要時間は 17.03 秒から 29.66 秒と長くなっていることがわかる．

フィルタごとに検証した結果，ノイズフィルタは利用者が鍵画像を発見しやすくなるが，フィルタに対する嫌悪感は大きくなる結果になった．

被験者の実験全体の意見として，ユーザ ID を間違えて記憶した状態で認証に何度も失敗したとの意見があった．

表 5: 設問「パスワードは定期的に変更していますか」に対する回答

回答	回答数
3 か月に 1 回は変更している	1
1 年に 1 回は変更している	2
不定期に変更している	12
変更していない	6

表 6: 設問「複数種類のパスワードを記憶することを苦痛に感じますか」に対する回答

回答	回答数
とても苦痛である 1	4
2	10
3	4
4	3
苦痛ではない 5	0

6. 議論

前章の実験結果より，認証失敗回数を比較した結果，パスワードよりも提案手法を利用したほうが認証失敗回数が少ないため，提案手法はパスワードよりも記憶に残りやすいことがわかる．

また，画像認証における各フィルタごとの嫌悪感の調査の結果，インパルスノイズを付加する手法がもっとも嫌悪感があり，被験者にもフィルタに戸惑ったという結果が得られ，インパルスノイズはフィルタはわかりやすいがポジティブな反応ではなかった．その他のフィルタについてはどれも変化がわかりにくいという結果だった．

6.1. 考察

今回の実験から，提案手法の有効性が示されたが，複数の鍵画像を記憶する際にこの認証手法は有効であると考える．

6.2. 実験から得られた情報

今回の実験では，画像を被験者に選択させる際に，画像をサムネイル表示した状態で選択させた．その際，サムネイルの大きさによっては画像の変化がわかりにく

表 7: 設問「利用しているサービスのパスワードが漏えいした際にパスワードを変更しますか」に対する回答

回答	回答数
使用しているサービスの価値による	7
変更する	14
変更しない	0

表 8: 設問「画像や写真を収集する趣味はありますか」に対する回答

回答	回答数
N/A	2
ある	11
ない	8

い，もしくはわからないという状況を確認できた．

これは，覗き見耐性を検討する場合に良い結果であると考える．まず，画像の劣化状態が覗き見てはっきりと分かる場合，画像の一覧を覗き見るだけで，鍵画像をすばやく見つけることができてしまい，攻撃に対する問題点になり得る．しかし，サムネイル表示の状態で画像の劣化がわかりにくいのであれば，画像の一覧を覗き見ただけでは鍵画像を見つけ出すのは困難になる．

6.3. 提案手法を繰り返し利用した場合

提案手法を繰り返して利用した場合，画像を格納しているディレクトリにはさまざまな鍵画像が保存されることになる．この鍵画像は使用中のものもあれば，鍵画像として利用しなくなったものも存在する．その際，攻撃者は複数の使用済み鍵画像を含む画像群からどれが正しい鍵画像であるのかを認識するのは難しくなる．総当たりで攻撃をする場合にも，提案手法はパスワードと比較して少ない認証回数で成功するため，パスワードよりも少ない回数でアカウントのロックを設定することが可能である．

7. 課題

今回の提案手法を検証するにあたって発覚した問題について今後の課題として以下に記す．

7.1. ファイルの更新日時問題

本認証システムではファイルを書き換えることからファイルの更新日時が変化する．そのため，ほとんどの OS では，ファイルの並び替え機能によりファイルを更新日時順に並べ替えることが可能である．それにより，ファイルの上書きが発生したファイルは更新日時が最も新しいものになっているため，並び替えた先頭か末尾にあることになる．

この問題への対策として考えられるものとして，ファイルを ZIP ファイルで利用者に送信し，利用者はその ZIP ファイルから展開した鍵画像を，画像を保管しているディレクトリに保存する．

しかし，これは利便性の面で問題がある．

最近のモダンな Web ブラウザでは，ブラウザ上からローカルストレージにあるファイルを直接編集することができる．その機能を利用してファイルを書き換える．ブラウザのコントロールが不正に攻撃者に奪われた際にファイルシステム，すなわちコンピュータ自身が乗っ取られてしまうリスクが非常に大きい．

Mozilla Firefox や Google Chrome などのブラウザには拡張機能 (エクステンション，アドオンなど) を付加し，ブラウザの機能を増やすことができる仕組みがある．このアプローチの問題は上述のファイルシステムに直接アクセスできる問題に加えて，エクステンションを利用できるブラウザであることがシステムを利用するための条件になってしまう．

表 9: 設問「あなたはパスワードを正確に記憶し，思い出すことができていましたか」の回答

回答		回答数	割合
正確に記憶し，容易に思い出すことができた	1	89	0.47
	2	59	0.31
	3	20	0.11
	4	19	0.10
思い出すことは不可能だった	5	1	0.01

表 10: 設問「劣化した鍵画像はすぐに見つけることができましたか」の回答

回答	回答数	割合
すぐ見つけた 1	140	0.63
2	59	0.27
3	11	0.05
4	7	0.03
とても時間がかかった 5	5	0.02

7.2. 画像選択における問題

今回の実験では画像の選択にサムネイル表示を利用するようにした．このサムネイルキャッシュが画像を選択する際に更新されていない問題が発生した．

また，画像を選択する際，画像についているファイル名で覚えてしまうといった被験者の声もあった．

一部の被験者は図9のように一つの鍵画像を決定後，それ以降の鍵画像を前の鍵画像の左隣にする行動が見られた．

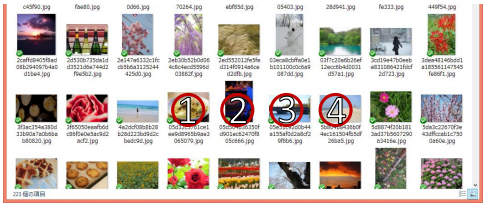

図 9: 相対位置で記憶してしまう問題

フィルタのかかり具合を認証頻度と要求するセキュリティレベルによって設定するが，どの程度の強さのフィルタまで，人間は同じ画像として変化前後の画像

表 11: 設問「画像の劣化に対して嫌悪感を感じましたか」の回答

回答	回答数	割合
強く感じた 1	22	0.10
2	29	0.13
3	22	0.10
4	53	0.24
全く感じない 5	96	0.43

表 12: HSB フィルタの実験アンケート結果

質問項目	1	2	3	4	5
すぐ見つけられたか	33	17	3	3	0
嫌悪感はあったか	3	2	4	11	36

を認識することができるのかを検証する必要がある．

利用者が新しい鍵画像ファイルをダウンロードし忘れる問題が被験者の話からわかった．この問題は認証完了後に画像の自動ダウンロードが開始されるように設定を行うことで解決することが可能である．

画像は，その情報がいつ，どのような状況であるのかを視覚的にわかりやすく表現する媒体である．つまり，画像にはピクセルの情報のほかにその画像自身が持っている意味が込められている．その画像自身が持っている意味によって記憶成績が変化すると考えられる．

7.3. おわりに

提案手法を用いることで，利用者はパスワードよりも多くの認証情報を記憶することができた．いろいろと問題はあるが，パスワードにとって代わる新しい認証方式として普及することを期待したい．

参考文献

[1] 小島悠子，山本匠，西垣正勝，“覗き見攻撃耐性と利便性を有する画像認証方式に関する一検討,” 情報処理学会研究報告，pp.91-96，2009.

[2] “Twitter bootstrap,” http://getbootstrap.com/, 2014 年 2 月 3 日 確認.

[3] “Rmagick 2.12.0 user’s guide and reference,” http://www.imagemagick.org/RMagick/doc/, 2014 年 2 月 3 日 確認.

[4] 稲村 雄 Richard E.Smith，認証技術: パスワートから公開鍵まで，オーム社，2003.

[5] David Heinemerer Hansson 前田 修吾 Sam Ruby, Rails によるアジャイル Web アプリケーション開発 第 4 版，オーム社，2011.

表 13: ぼかしフィルタ 1 の実験アンケート結果

質問項目	1	2	3	4	5
すぐ見つけられたか	32	17	3	2	1
嫌悪感はあったか	1	2	5	18	30

表 14: ぼかしフィルタ 2 の実験アンケート結果

質問項目	1	2	3	4	5
すぐ見つけられたか	35	10	4	1	3
嫌悪感はあったか	5	8	8	14	18

表 15: ノイズフィルタの実験アンケート結果

質問項目	1	2	3	4	5
すぐ見つけられたか	40	15	1	1	1
嫌悪感はあったか	14	17	5	10	12