L-023

携帯電話を用いたランダム画像個人認証方式について
Personal Identification Using Random Images for Mobile Phones

瀬野尾 純† 加藤 貴司† ベッド B. ビスタ† 高田 豊雄†
Jun Senoo Takashi Katoh Bhed Bahadur Bista Toyoo Takata

1. はじめに

現在、個人認証方式の主流となっているのは、汎用性と利便性の高さから、文字や記号、数字を組み合わせたパスワード・暗証番号を利用したものである。しかし、人間にとっては、長い文字記号列を正確に覚えることは負荷が高いため、誕生日、電話番号などの短くわかりやすい (他人に推測されやすい) パスワードや暗証番号を使ってしまったり、パスワードをメモ書きで管理してしまうなど、ずさんなパスワード作成・管理をしてしまう事が多い。

そこで本稿では、近年、人々の生活において欠かせないものになっている携帯電話を対象として、ユーザのパスワード管理 (記憶) における負担を減らすことでずさんなパスワード管理を抑制し、ショルダーハッキングが困難な個人認証方式を実現することを目的とする。そのため、本稿では、ランダム画像による個人認証を用い、さらにそのランダム画像に、表示位置に関する情報を付与することを提案する。

2. ランダム画像個人認証と携帯電話への導入における問題点

ランダム画像個人認証とは、パスワードとして、文字や記号の代わりに、コンピュータで自動的に生成されるランダムな画像を用いる個人認証方式である。この方式では、認証時に提示される複数の画像から、自身のパスワード画像を再認し入力することにより認証を行う。この個人認証方式は、パスワード認証の欠点の克服を目標としており、文字や記号の列に比べてイメージの方が以前見た情報を再び認識する時の負担が少ない事に基づいている [1][2][3]。パスワード画像には、コンピュータで自動的に生成される、特別な意味を持たないランダムなイメージを使用する。このことにより、紙等への書き留めによるパスワードの管理を抑制し、ユーザの趣味趣向や個人情報に基づいたパスワード推測攻撃への脅威を減らすことを可能にしている。

このランダム画像認証を利用したシステムとして、PC 上で実現されている Déjà Vu[4] がある。Déjà Vu では、25 枚のランダム画像から 5 枚のパスワード画像を選択することで認証を実現している。このシステムを用いて行ったユーザテストでは、Déjà Vu、パスワード、PIN、写真による画像認証の 4 つの認証方式を比較した結果、画像を使った認証方式が一番時間が経っても忘れにくいことが示されている。

しかし、現在 PC 上において実装されているランダム画像個人認証を行うためには、画像の表示サイズとランダム画像の認識のトレードオフの問題を解決しなければならない。パスワード画像として用いるランダム画像は、携帯電話の液晶画面上において多くの画像を表示しないと簡単に破られてしまい、セキュリティの低下の原因になってしまう。逆に、多くの画像を表示しようとすると、ユーザのランダム画像の再認が困難になってしまい、ユーザビリティが低下してしまう。加えて、どこでも使えるという携帯電話の特徴により、覗き見によるパスワード漏洩などのショルダーハッキング攻撃を受けやすくなってしまうという問題がある。

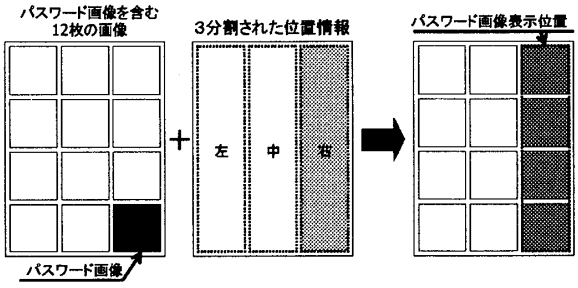

図 1: 位置情報を含む画像表示方法の例

3. 位置情報を用いたランダム画像個人認証の提案

3.1 認証方式

携帯電話上でランダム画像個人認証を実現する際には、携帯電話の限られた画面サイズの中で、適切な枚数のランダム画像を表示し、特別な意味をもたないランダム画像に対し、いかに再認へと導くかが重要である。そこで本稿では、パスワード画像を再認するためのユーザの負担を軽減するために、画面を分割し、その位置情報と、パスワード画像を含むランダム画像を組み合わせる個人認証方式を提案する。例えば、図 1 のように縦 4 枚、横 3 枚の計 12 枚の画像からパスワード画像を選択する場合、パスワード画像を含む 12 枚の画像は、表示画面において左・中央・右の 3 つの場所に分割され、画像を表示する際は毎回その 3 つに分けられた場所の中でランダムに表示される。ユーザは、パスワード画像とその位置情報を覚えることにより、位置情報による絞込みができるため、特別な意味の無いランダム画像でも認証時の再認が容易になる。また、そのほかの分割方法として、横 4 行に分割したり、画像の表示枚数が 16 枚 (4 行 ×4 列) の場合には、左上・右上・左下・右下の四方で分割する方法などがある。このように、分割方法をユーザ自身が定義することで更なる効果が期待できる。

3.2 登録・認証手順

提案する認証方式におけるパスワード画像登録、及び認証手順は次の通りである。

†岩手県立大学 ソフトウェア情報学部

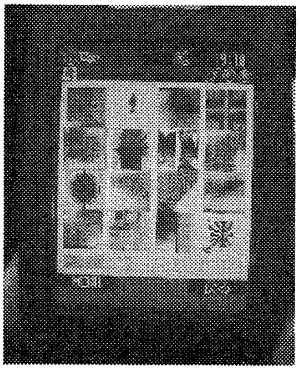

図 2: 認証画面 (FOMA F900iT)

登録フェーズ アプリケーションにおける初回起動時またはパスワード変更時には、次の手順でパスワード画像が登録される。1) アプリケーションの初回起動時やパスワード画像変更時において、サーバからパスワード画像をダウンロードする。2) ダウンロードしたランダム画像をアプリケーションに記憶する。3) ユーザはアプリケーションに記憶されたランダム画像から、パスワード画像として用いたい画像を、認証に必要な枚数選択する。4) ID(機種固有番号) と選択された画像情報をサーバに登録する。

認証フェーズ アプリケーションにおけるユーザの認証は、次の手順で行われる。1) アプリケーションは、ユーザのパスワード画像を含む複数枚のランダム画像を読み込み、位置情報に基づいた場所にランダムに表示する。2) ユーザが、表示されたランダム画像の中から、自身のパスワード画像を、認証に必要な枚数分選択する。3) ユーザが正しいパスワード画像を選択することができれば、正規ユーザとして認証する。

4. 実装及び評価

本提案方式における、ユーザビリティ評価とショルダーハッキングに対する耐性評価のために、システムの実装を行った。本システムの実装には、NTT DoCoMo iαppli Development Kit for DoJa 3.5* 及び Java version 1.4.2 を使用した。クライアントは NTT ドコモの FOMA F900iT を使用した (図 2)。

本実験では実機を用い 1) ユーザビリティ 及び 2) ショルダーハッキングに対する耐性に関する評価を行った。なお、被験者は、日頃、携帯電話を持っており、不自由無く操作を行える本学の学生である。

ユーザビリティの評価 本提案方式のユーザビリティを評価するために、以下の実験を行った。

被験者は自分が安全だと思うパスワードを自身で選択する。登録直後の認証は、充分練習を行った後に行う。2 回目の認証は、1 日以上経過した後に行う。これらの操作は、ランダム画像認証の場合、入力はすべて方向キーと決定キーで行う。被験者は 10 名である。

*http://www.nttdocomo.co.jp/

評価項目は 1) 被験者が認証開始からパスワードを入力し終わるまでの認証に要する時間, 2) パスワード登録直後と 1 日以上経過した後の認証失敗率 である。これらに対し、提案手法 (位置情報を付与した、縦 4 枚、横 4 枚の 16 枚から 4 枚選択するランダム画像認証) と、縦 4 枚、横 4 枚の 16 枚から 4 枚選択するランダム画像認証、縦 3 枚、横 3 枚の 9 枚から 4 枚選択するランダム画像認証 (携帯電話の画像認証で多く用いられている表示枚数)、パスワード認証 (4 桁の数字を使用) のそれぞれとの比較を行った。

結果 及び 評価 表 1 は、本提案方式を含む 4 つの個人認証方式のユーザビリティを比較した実験結果である。この表より、登録直後と時間が経過した後の認証時間を比べると、パスワード認証方式では、時間の経過による差はあまりないが、認証行為自体に時間が多くかかってしまっていることが分かる。ランダム画像認証方式では、画像を再認しなければならないため、多少時間が増えているが、認証に要する時間は、パスワード認証方式と比べて、短くなっている。

また、時間が経過した後の 4 つの認証方式の認証失敗率は、パスワード認証方式と位置情報の無い表示枚数 16 枚のランダム画像個人認証方式で、それぞれ 2 回の認証失敗があったのに対して、表示枚数の少ない表示枚数 9 枚のランダム画像認証方式と本提案方式 (位置情報のある表示枚数 16 枚のランダム画像認証方式) では、認証失敗は 0 回であった。これは、表示枚数 16 枚の時の小さな画像でも、位置情報を付加することにより、ユーザがランダム画像を再認しやすくなり、認証の失敗が減少したことによるものと考えられる。

加えて、3 つのランダム画像認証方式を比較すると、いずれも登録直後の認証に要する時間では大きな差は無いが、時間が経過した後の認証に要する時間では、本提案方式が、表示枚数が枚数が多いのにもかかわらず、少ない時間で認証に成功している。これは、特別な意味を持たないランダム画像でも、位置情報を付与することにより、認知的な負荷を低減できていることによるものと考えられる。

これらの結果から、本提案手法は、高いユーザビリティを持つと言える。

ショルダーハッキングに対する耐性の評価 次に、ショルダーハッキングに対する耐性評価として、2 種類の認証方式に対する実験を行った。具体的には、正規ユーザが認証を成功させるところを、攻撃者が有利な条件で覗き見た場合、なりすましまでに必要な覗き見回数を調べた。

実験の手順は以下の通りである。1) 正規ユーザが認証を行う。2) 攻撃者は隣または後ろにいて、1) の様子を、覗き見する。3) 攻撃者は、2) の直後に、正規ユーザになりすまして認証を行う。4) 認証に失敗した場合、1) から 3) の手順を繰り返す。5) 4 回のなりすましの試行でも成功出来なければ実験を終える。

ここで覗き見を 4 回までとしているのは、本提案方式では選択画像が 4 枚であり、攻撃者が 1 度の覗き見で 1 枚の画像を確実に覚えることができれば、4 度の覗き見でなりすましを成功させられるからである。

比較する認証方式は、本手法 (位置情報を付与した、

表 1: 認証成功時の平均入力時間 及び 認証失敗率

	認証成功時の平均入力時間 (秒)		認証失敗率	
	登録直後	1 日以上経過後	登録直後	1 日以上経過後
本提案方式 (位置情報有り、表示枚数 16 枚)	5.9	10.1	0	0
表示枚数 16 枚	6.5	10.9	0	20% (2/10)
表示枚数 9 枚	5.5	11.7	0	0
パスワード認証	11.9	12.3	0	20% (2/10)

表 2: なりすましの成功回数

	成功回数
提案手法 (16 枚)	7/15 回 (47%)
表示枚数 9 枚	14/15 回 (93%)

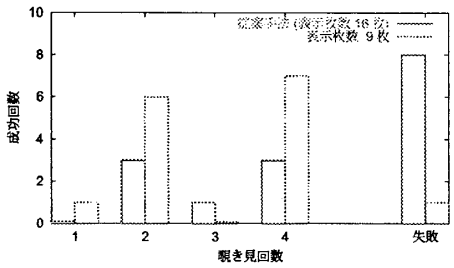

図 3: なりすますことが出来た覗き見回数

縦 4 枚、横 4 枚の 16 枚から 4 枚選択するランダム画像認証) と、縦 3 枚, 横 3 枚の 9 枚から 4 枚選択するランダム画像認証 (携帯電話の画像認証で多く用いられている表示枚数) である。

実験条件は次の通りである。1) 攻撃者は、後ろや隣などの覗き見しやすい有利な位置で認証を覗き見ることが出来る。2) 攻撃者は事前に表示枚数、位置情報の有無について知ることができる。3) 入力はすべて方向キーと決定キーで行う。4) 被験者である攻撃者は 5 名であり、それぞれの被験者は、正規ユーザの認証の覗き見を、異なる 3 種類のパスワード画像に対して行う。

結果 及び 評価 表 2 は 4 回以内になりすますことが出来た回数であり、図 3 はなりすますことが出来た覗き見回数のグラフである。

本実験のように攻撃者に有利な条件であり、選択画像が 4 枚であった場合には、攻撃者が 1 度の覗き見で 1 枚の画像を確実に覚えれば、4 度の覗き見でなりすましが成功してしまう。実験の結果から、表示枚数 9 枚の場合には 1 度に複数枚の画像を覚えられてしまい、早い段階でなりすまされてしまっているが、表示枚数 16 枚の方では 4 度の覗き見でもなりすましされにくくなっていることが分かる。

実験後、被験者 (攻撃者) から聞き取り調査を行ったところ、表示画像が 16 枚より 9 枚表示された方がカーソル移動にあまり変化がなく、指の動きでパスワード画像が推測しやすいというコメントが多くあった。一方、表示枚数が 16 枚の場合の位置情報については、認証を行っている短時間にどのような法則の位置情報で表示されているかまでは推測できないとのコメントがあった。

以上から、ランダム画像個人認証における覗き見の対策として、(1) 多くの画像を表示させることにより、正規ユーザ以外に画像を認識出来ないようにすること、(2) 攻撃者に表示方法の規則を推測されやすいパスワード画像表示 (カーソルの移動量が少ないなど) を防ぐための表示方法、が有効であることが分かる。本提案方式は、表示枚数を 16 枚としており、そのためカーソルの動きも多くなるため、覗き見を防ぐ手法として、有効であると言える。

5. まとめ

本稿では、携帯電話において、ランダム画像個人認証を用いることにより、パスワード個人認証の安易なパスワードの作成・管理の問題を克服し、また、画像表示方法に位置情報を持たせることにより、ユーザの画像を再認する負担を軽減する個人認証方式を提案した。ついで、本提案手法を実装し、実験により本提案手法の有効性を確認した。実験結果から、位置情報を用いることにより、既存の画像認証よりも画像のサイズを小さくしても、ユーザのパスワード管理の負担を軽減すること可能になった。そのため、画像や指の動きの覗き見によるショルダーハッキング攻撃に対しても、攻撃者が画像や指の動きを認識しにくくなっていることがわかった。

今後の課題としては、通信コストのためにクライアント側での画像作成の実現や、ユーザの記憶に残りやすいパスワード画像の作成などが挙げられる。

参考文献

[1] 原田篤史, 漁田武雄, 西垣正勝. モザイク画像認証の提案とその実用可能性. コンピュータセキュリティシンポジウム 2004, pp. 385–390, 2004.

[2] 高田哲司. あわせ絵: 写真を用いた携帯端末での個人認証方式. インターネットコンファレンス 2003, 2003.

[3] Real User Corporation. Passfaces. http://www.realuser.com/cgi-bin/ru.exe/_/homepages/index.htm.

[4] R. Dhamija and A. Perrig. Déjà vu: A user study using images for authentication. In *Proc. Ninth USENIX Security Symp.*, 2000.