

アイコンとフリック入力を用いた覗き見耐性を持つ 認証方式の検討

和斉 薫¹ 菅井 文郎² 喜多 義弘³ 朴 美娘³ 岡崎 直宣¹

概要：モバイル端末内の情報の漏えいを防ぐため、画面ロック及び画面ロック解除認証が広く利用されているが、覗き見耐性と高いユーザビリティを同時に実現している認証方式は実用化されていない。アイコンとタップ入力を用いたモバイル端末向けの認証方式である Secret Tap 方式は高い覗き見耐性を持つが、偶然に認証を成功する確率を十分な強度にするためには、一連の認証において、タップ入力の回数を多くする必要があり、ユーザビリティが低下する問題がある。

本研究では、Secret Tap 方式をフリック入力を用いて拡張した Secret Flick 方式を提案する。認証中の 1 回の入力においての偶然に認証を突破される確率を低くし、入力回数を少なくすることでユーザビリティを向上させることを目指す。

キーワード：モバイル端末、覗き見攻撃、個人認証

An Examination of Icon-based User Authentication Method Using Flick Input for Mobile Terminals

KAORU WASAI¹ FUMIO SUGAI² YOSHIHIRO KITA³ MI RANGPARK³ NAONOBU OKAZAKI¹

Abstract: Some authentication methods that lock and unlock the screen are widely used in order to prevent from information be stolen. However, there is no method suitable for mobile terminals that have both shoulder-surfing resistant and high usability. "Secret Tap" method uses icon and tap input and has high shoulder-surfing resistant. However, in order to have sufficiently low probability for breaking the authentication by accident, it needs many times of tap input in an authentication. In this paper, we propose a new authentication method called "Secret Flick" method that extends the Secret Tap method with "flick" input. The proposed method achieves high usability by less number of inputs.

Keywords: mobile terminals, shoulder-surfing attack, personal authentication

1. はじめに

近年、スマートフォンや Android などのモバイル端末が広く普及してきている。多くのモバイル端末の中には個人情報等の重要な情報が格納されており、情報の流出を防ぐため、PIN(Personal Identification Number)等の画面の操

作ロック及び個人認証方式を利用した画面ロック解除認証が必要になる。しかし、既存の多くの認証方式では、人の目にさらされた環境でロック解除を行うと第三者に認証情報がばれてしまう可能性が大きいという問題がある。さらに、多くのモバイル端末はキーボードを搭載しておらず、タッチパネル液晶といくつかのボタンのみが標準の入力デバイスとして搭載されている。そのため、モバイル端末において既存の認証方式を使用するとユーザビリティが低下してしまう可能性がある。そこで、モバイル端末を対象とした高いユーザビリティと覗き見耐性を備えた認証方式が

¹ 宮崎大学工学部
University of Miyazaki

² 宮崎大学大学院工学研究科
University of Miyazaki

³ 神奈川工科大学
Kanagawa Institute of Technology

急務である。

Secret Tap 方式 [1] は、画面上のアイコンをタップ入力するという簡単な操作で高いユーザビリティを有し、視き見耐性を備えた認証方式である。しかし、この方式では、偶然に認証を突破される確率を十分に低くするためには、1 回の認証に行う際のタップ入力の回数が多くなり、ユーザビリティが低くなってしまう。

そこで、1 回の認証での偶然に認証突破される確率を低くし、入力回数を少なくすることでユーザビリティの向上を目指す。本研究では Secret Tap 方式の入力方法としてフリック入力を追加した認証手法 Secret Flick の提案および評価を行う。

2. 関連研究

2.1 画面ロック

現在、デスクトップ端末、モバイル端末を問わず画面ロックを利用したセキュリティが広く普及している。画面ロックは、端末を操作できる状態からユーザが任意に、または、あらかじめ設定した時間内にマウスやキーボードなどの入力があった場合などに、端末の操作をできない状態にする機能である。この画面ロックを解除するためには設定しているパスワードや暗証番号などを用いた個人認証が必要となる。画面ロックは、デスクトップ端末では席を外している間に、モバイル端末では紛失、盗難の際に、端末内の情報の盗難、改ざんを防ぐ目的がある。モバイル端末はデスクトップ端末と違い、席に座っている間は常に画面ロックが解除されている。かばんの中やポケットに身に着けているなどの状態でも画面ロックをかける。このため、メール、電話などモバイル端末の機能を使用する毎に画面ロックを解除する必要がある。モバイル端末はデスクトップ端末と比較して画面ロックの解除認証の頻度が非常に多くなってしまう。そこで、画面ロック解除認証においてモバイル端末はデスクトップ端末よりもユーザビリティについて配慮する必要がある。

2.2 視き見攻撃

視き見攻撃とは、ユーザの認証操作を視き見することで認証情報を盗む攻撃である。この攻撃を防ぐ簡単な対策としては、ユーザが他人に認証操作を見られないように注意することが考えられる。しかし、混雑した電車やエレベーターの中などでは人の目を避けることが難しい場面もある。そのため、他人に認証操作を見られても認証情報が露呈することがない視き見耐性を持つ認証方式が必要である。

視き見攻撃は何を使用するかで大きく二つに分類できる。一つは「人の記憶を使い認証動作を視き見る攻撃」（以下、人による視き見攻撃）であり、もう一つは「カメラなどの録画機器を使い認証動作を記録し解析する攻撃」（以下、録画攻撃）である。人による視き見攻撃において人は

記憶力、処理能力に限界がある。そのため、ある程度認証方式を複雑にすると、第三者が一連の操作をすべて記憶することが困難になる。したがって、人による視き見攻撃に対する十分な耐性を持たせることが可能である。

一方、録画攻撃は認証画面、認証操作をすべてまたは一部を記録し、コンピュータを用いた解析が可能であり、記憶能力と処理能力には限界がない。そのため、録画攻撃に対する耐性（以下録画耐性と呼ぶ）を持たせることは人による視き見攻撃よりも複雑な認証方式が必要になる。

さらに複数回の録画攻撃に耐性を持たせた場合、冗長にしなければならない情報量が増えてしまう。そのため、認証手続きが複雑になり、頻繁に認証を行う画面ロック解除において、ユーザビリティを著しく損ねる。

また、偶然に録画機器にユーザの認証操作が映りこむことはあるが、同じ録画機器に複数回認証操作が映りこんでしまう可能性は低いと考える。しかし、偶然に録画機器に写りこんで秘密情報が露呈してしまうことは防がなければならない。そこで、本研究では、1 回の録画攻撃に対しては耐性を持つことを目標とする。

3. 既存手法

本章では、モバイル端末で現在用いられている認証方式と視き見耐性を持つ認証方式を紹介する。

3.1 Android Password Pattern [2]

モバイル端末向けの個人認証方式であり、4 節点以上のパターンを指でなぞることで認証を行う。この方式は、認証操作を見られると第三者にパターンが露呈してしまうため、視き見耐性がない。さらに、画面になぞった跡がつくという問題点があると考えられている。

3.2 Convex Hull Click Scheme(CHC)[3]

画像パスワードによる認証であり、表示される正解のアイコンで作られる凸包形内のアイコンを選択することで認証を行う。直接正解のアイコンを選択しないため、視き見耐性を有している。しかし、モバイル端末のような小さい画面の場合、表示されるアイコンが少なくなる。ゆえに、表示される凸包形内のアイコンが少なくなるため、第三者に推測されやすくなってしまう。さらに、複数の正解のアイコンを探さないといけないのでユーザビリティが低下してしまう。よって、この方式は高いユーザビリティが必要であるモバイル端末には向かない。

3.3 Secret Tap 方式 [1]

この方式は、モバイル端末を対象にし、高いユーザビリティと視き見耐性を持つ個人認証方式である。事前に、秘密情報となる複数の正解アイコン（以下、登録アイコン）と入力回数、シフト量を設定する。この方式の認証画面を

図1に示す。認証画面には、登録アイコンが1つとダミーのアイコンが4×4マスにランダムに表示される。認証画面を2×2ずつ4つに分け、それぞれ第1象限から第4象限とし、登録アイコンが表示されている象限から反時計回りに、事前に設定したシフト量分ずらした象限内の任意のアイコンをタップする。ここでシフト量とは、図1のように登録アイコンが表示されている象限から、反時計回りに、どれだけずれた象限のアイコンをタップして認証するかを決める値である。タップするとアイコンがシャッフルされて再び表示される。この操作を設定した入力回数繰り返して認証を行う。シフト量を秘密情報として設定することによって、どの象限に登録アイコンが表示されているかを隠蔽することが可能となり、覗き見耐性を向上させることができる。さらに、設定した登録アイコンが表示されている象限をタップする事を回避することで、登録アイコンを直接タップしてしまうことを防ぐことが可能となる。また、この方式では登録アイコンの出現確率を一連の認証操作を通して均一になるようにしている。これは、認証中に同じアイコンが何度も出現して第三者にばれてしまうことを防ぐ目的がある。入力回数よりも登録アイコン数が多い場合、十分な数のアイコンを用意する事ができれば、一回の録画耐性について十分な強度を確保することが可能である。

しかし、Secret Tap方式では各1回の認証において、偶然に認証を突破される確率が1/4であり、10進数のPIN数字4桁相当の強度にするためには入力回数を7回にする必要がある。PINやAndroid password patternと比較しても入力回数が多くユーザビリティが低下してしまう。入力回数が増加するにつれて入力時間が増加するため、ユーザビリティが低下することが考えられる。また、入力回数が増えた場合、設定した登録アイコンが入力回数より少ないと何回も同じ登録アイコンが出現してしまい覗き見耐性が下がってしまう。

この方式には2つのトレードオフが存在する。1つは、覗き見攻撃に対する耐性とユーザビリティの間のトレードオフである(トレードオフ1)。覗き見耐性、録画耐性を持たせるには、認証方法を複雑にする必要がある。そのため、認証方式のユーザビリティが低下してしまう。逆に、高いユーザビリティを持たせた認証方式は認証操作が簡単なものになってしまうため、覗き見耐性が低下してしまう。

もう1つは、録画耐性と1回の認証における偶然に認証を突破される確率の間の関係である(トレードオフ2)。Secret Tap方式では、表示されるアイコンの数は16個であり、これを4つのグループに分けている。録画耐性は1回の入力で第三者に正解のアイコンを推測される数が多いほど高くなる。したがって、録画耐性はグループ内のアイコンの数に依存し、録画耐性を上げるためには、グループ内のアイコンの数を増やす必要がある。しかし、グループ内のアイコンを増やすとグループの数が減ってしまう。

また、偶然に認証を突破される確率を低くするには、入力総当たり数が増えるほど低くなる。したがって、偶然に認証を突破される確率は、グループの数に依存し、低くするためには、グループの数を増やす必要がある。しかし、グループの数を増やすとグループ内のアイコンの数が減ってしまう。

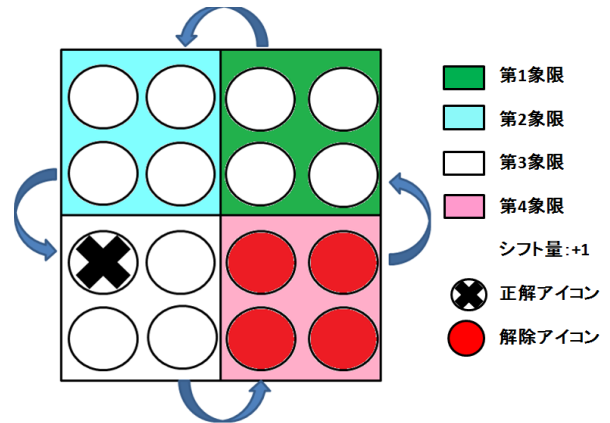


図1 Secret Tap方式の認証画面 [1]
Fig. 1 Authentication screen of Secret Tap

4. 提案手法

4.1 目的

Secret Tap方式は、画面のアイコンをタップするという簡単な操作で高いユーザビリティを有し、覗き見耐性を持つ認証方式を実現している。さらに、モバイル端末の小さい画面でも使用可能である。既存手法には覗き見耐性を持つ認証方式はあるが、モバイル端末を対象とし、高いユーザビリティを有した認証方式は少ない。そこで、本論文では、Secret Tap方式を基に1回の偶然に突破される確率を低くし、入力回数を少なくすることでユーザビリティの向上を目的とした新しい認証方式を提案する。

しかし、Secret Tap方式は3.3節で述べたような問題点がある。そこで、本論文では、PINと同じ強度を備えた上で、ユーザビリティを向上させるために、Secret Tap方式にタッチパネル液晶のフリック入力を導入したSecret Flick方式を提案する。

4.2 設計方針

(1) 覗き見攻撃に対する耐性

同じ人に何回認証動作を見られても認証情報が露呈することはない強度を持つこと。認証入力時に既出の登録アイコンが再出現しないことを目標にする。

(2) 録画攻撃に対する耐性

一回の録画攻撃に対して耐性を持つこと。複数回の録

画攻撃に耐性を持たせると冗長にしなければならない情報量が増えてしまう。そのため、認証手続きが複雑になり、頻繁に認証を行う画面ロック解除において、ユーザビリティを著しく損ねユーザに受け入れられないと考える。しかし、偶然に録画機器に写りこんでしまうなどのリスクを回避することは必要であると考えたため、一回の録画攻撃に対しては耐性を持つことを目標とした。

(3) 偶然に認証に成功する確率

10進数のPIN4桁に相当する強度を持つこと。これは、現在広く普及しているATMにおいて10進数のPIN4桁が利用されていることを考慮した。なお、brute-force攻撃に対しては認証の試行回数に制限を設けるなどの方法を併用することで対策が可能なのでここでは特に考慮しない。

(4) ユーザビリティ

覗き見耐性を持つ認証方式として、ユーザに受け入れられるユーザビリティを持つこと。提案手法において、ユーザに負担がかからないと想定する入力回数をPIN4桁の入力回数である4回程度と仮定する。この入力回数で十分な認証強度を実現することを目標とした。また、モバイル端末は操作を片手で行うことが多く、認証は両手よりも片手でできた方がユーザビリティが向上すると考え、認証動作を片手だけで行えることを目標とした。提案方式はアイコンを用いるが、スマートフォンの約4.0インチの大きさのタッチパネル液晶でも快適に認証を行えることを目標とした。

4.3 Secret Flick 方式の認証手順

事前に秘密情報となる複数の登録アイコン、シフト量、入力回数、登録アイコンごとにフリック方向を設定しておく。本方式の認証画面を図2に示す。

ここで、登録アイコンを設定したシフト量分だけ反時計回りに移動した事象を正解事象と呼ぶ。本方式では、正解象限において表示されるアイコンに設定したタップまたはフリック入力をする。この操作を設定した入力回数繰り返す、すべて正確に入力できた場合に認証が完了する。図2で認証例を説明する。シフト量を+1、アイコンにフリック入力の右方向を設定したとする。この場合、登録アイコンが第3象限にある。シフト量が+1なので第3象限から反時計回りに1つずらした第4象限が正解象限になる。正解象限内のアイコンにおいて、登録アイコンに設定している右向きのフリック入力をする事で1回の認証が成功となる。この認証操作を入力回数繰り返す。

入力方法を増やすことにより、1回の認証の偶然に認証を突破される確率をSecret Tap方式の1/4から1/20まで下げることが可能である。さらに、10進数PIN4桁以上の強度にする場合、入力回数を7回から4回まで下げるこ

が可能である。

3.3節で述べたトレードオフ2に関してこの方式は、入力1回の偶然に認証を突破される確率を下げるためには、録画耐性が下がるのが危惧される。しかし、画面に表示されない認証情報であるフリックという入力方法を増やすことでこの問題を回避することができる。

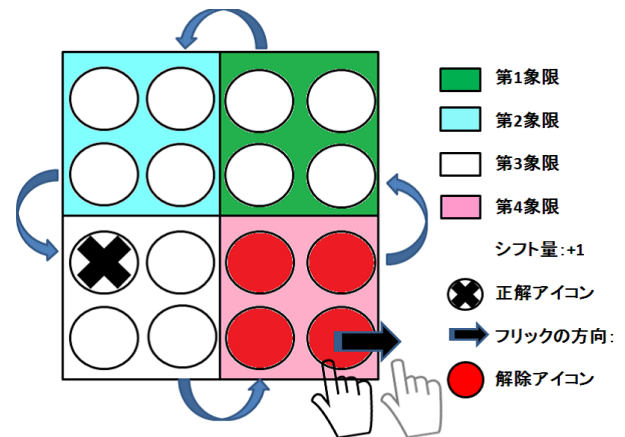


図2 Secret Flick 方式の認証画面の模式図

Fig. 2 Schematic diagram of the authentication screen of Secret Flick

5. 実装

5.1 実装環境

各提案手法はJavaでAndroid SDKを用い、統合開発環境Eclipseを使い、Android端末上に実装した。

5.2 アプリケーション

アプリケーションに実装した各提案手法の認証画面を図3に示す。この認証画面において入力回数入力すると、認証に成功したか失敗したかと認証にかかった時間を表示する。設定画面においては、図4の1のエリアでSecret Flick方式とSecret Tap方式の切り替えられるようにした。さらに、同図の3のエリアで入力回数の設定、アイコンの一覧表をタップして正解となるアイコンを設定できるようにした。選択後、同図の2の箇所に現在選択されているアイコンがリストとして表示される。アイコンごとの入力方法の設定は、この箇所のアイコンをロングタップし、フリックの方向を選択することで設定する。

6. 評価および考察

6.1 偶然に認証に成功する確率について

提案手法とSecret Tap方式、10進数PIN4桁の偶然に認証に成功する確率を表1に示す。同表において、10進数の4桁のPINに相当する強度を各手法で実現するときの入力回数を太字で示している。偶然に認証に成功する確



図 3 Secret Flick 方式の認証画面

Fig. 3 Authentication screen of Secret Flick

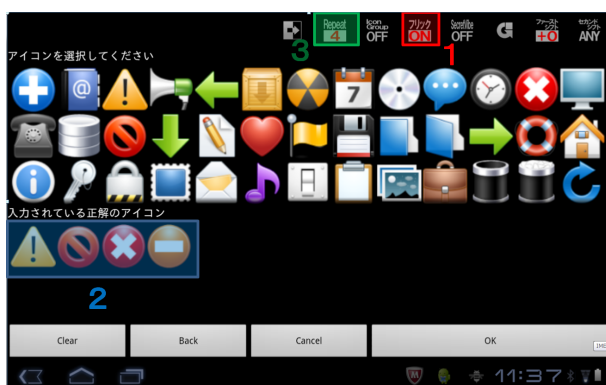


図 4 Secret Flick 方式の登録アイコン設定画面

Fig. 4 Password icon setting screen of Secret Flick

率は、入力が n 回の場合、Secret Tap 方式が $1/4^n$ 、Secret Flick 方式では $1/20^n$ となる。Secret Tap 方式では、7 回繰り返した場合に $1/16384$ となり、4 桁の 10 進数 PIN に相当する強度を超える。しかし、入力回数が 7 回であるので、ユーザビリティの観点から許容できないと実用的ではない。Secret Flick 方式では、3 回繰り返した場合 $1/8000$ となり、多少 10 進数 PIN に相当する強度に満たないが近い値になる。これは、ユーザがセキュリティの観点から許容できるならば、PIN の入力回数よりも 1 回少なく認証を行うことが可能である。4 回繰り返した場合には $1/160000$ となり、4 桁の 10 進数 PIN と同じ入力回数で 4 桁の 10 進数 PIN に相当する強度を大きく上回る。

6.2 覗き見耐性について

提案手法が実際に覗き見攻撃に対する耐性を有しているか評価する目的で実験を行った。被験者は、宮崎大学工学部情報システム工学科に所属する学生 11 人である。提案手法を十分説明した後、実際に使用してもらい、理解してもらった上で被験者の目の前で 10 回ゆっくり繰り返した認証を 2 回行い、秘密情報を推測してもらった。

実験の結果、提案手法の実際の認証情報と被験者が推測した認証情報が一致したのは 1 回で正答率は 4.5% であっ

表 1 既存手法と提案手法の偶然認証に成功する確率の比較

Table 1 Comparison of proposed methods and existing methods for the probability of success by accident

	3 回	4 回	5 回
Secret Tap	1/64	1/256	1/1024
Secret Flick	1/8000	1/160000	1/320000
10 進数 PIN	1/1000	1/10000	10^{-5}
	6 回	7 回	n 回
Secret Tap	1/4096	1/16384	4^{-n}
Secret Flick	1/16400000	1/128000000	20^{-n}
10 進数 PIN	10^{-6}	10^{-7}	10^{-n}

た。推測されてしまった原因は、設定した登録アイコンが視覚的に関連付けたものであり、そのアイコンが各認証に 1 個ずつ出現してしまったためだと考える。そのため、視覚的に関連付けられたアイコンが 1 個ずつ表示されないことで改善できると考える。

提案手法について設定する登録アイコン次第で十分な覗き見耐性を有していることが確認できた。

6.3 ユーザビリティについて

提案手法がユーザに受け入れられるユーザビリティを有しているかを評価する目的でアンケートを行った。被験者は上記と同じで行った。Secret Tap 方式と提案手法の説明を行い、実際に使ってもらい、評価実験を行った後でアンケートに答えてもらう形式で行った。提案手法についてとそれぞれの手法について SD(Semantic Differential) 法を用い主観的な印象度、許容できる入力回数 (桁数) を答えてもらった。SD 法を用いて取得した各項目の印象語と得点の対応関係を表 2 に示す。

表 2 各手法の印象に関する測定項目と得点

Table 2 Measurement items and scores on the impression of each method

測定項目	印象語と得点
理解のしやすさ	難しい 1 点 $\leftrightarrow$ 5 点 容易
使いやすさ	使いにくい 1 点 $\leftrightarrow$ 5 点 使いやすい
覚えやすさ	覚えにくい 1 点 $\leftrightarrow$ 5 点 覚えやすい
覗き見耐性があることで安心と感じたか	安心でない 1 点 $\leftrightarrow$ 5 点 安心
偶然認証について安心と感じたか	安心でない 1 点 $\leftrightarrow$ 5 点 安心
使いたいと思うか	使いたくない 1 点 $\leftrightarrow$ 5 点 使いたい

表 3 SD 法による各認証方式の印象度の結果

Table 3 Results of the questionnaire using semantic differential method

	理解のしやすさ	使いやすさ	覚えやすさ	(覗き見耐性) 安心さ	(偶然認証) 安心さ	使いたいと思うか	許容回数
Secret Tap	4.1(0.8)	4.2(0.4)	3.8(1.0)	4.5(0.7)	2.7(1.1)	4.3(0.7)	4.4(0.9)
提案手法 Secret Flick	4.3(0.9)	3.7(0.9)	3.3(1.1)	4.6(0.7)	4.7(0.5)	4.2(0.8)	3.8(0.4)

SD 法によるアンケート結果を表 3 に示す。表内の括弧内の値は標準偏差である。アンケート結果では、Secret Tap 方式と Secret Flick 方式を比較して「使い易さ」と「覚えやすさ」、「偶然認証の安心さ」以外の項目がさほど変わらな

い値となった。Secret Flick 方式は、偶然に認証についての「安心さ」の項目で Secret Tap 方式を大きく上回った。しかし、Secret Flick 方式は、Secret Tap 方式に認証操作、秘密情報を追加した方式であるため、そのことが「使い易さ」と「覚えやすさ」の項目の値が低くなってしまった理由だと考える。また、許容回数において Secret Tap 方式は 4.4 回、Secret Flick 方式は 3.8 回という結果となった。この許容回数において、Secret Tap 方式の偶然に突破される確率は十分な強度を持たず、Secret Flick では十分な強度を持つ。そのため、提案手法は、実現可能なユーザビリティで安全性を確保できている。使い易さと覚えやすさの項目の値以外はさほど変わらないため、Secret Flick 方式は、Secret Tap 方式の良さは維持していると考ええる。また、提案手法について入力回数を減らすことは使い易くなり、PIN 以上の強度にした場合の入力回数の場合、Secret Flick 方式の方が使い易いと 11 人中 9 人が回答した。この結果から、Secret Flick 方式は記憶負荷が増加するが、入力回数を減らすことでユーザビリティが向上しているといえる。

7. まとめ

本論文では、覗き見耐性を持つ従来の認証方式の安全性を確保しつつ、入力回数を減らすことでユーザビリティを考慮した Secret Flick 方式を提案した。評価実験により、実現可能な入力回数において安全性を確保していることがわかった。しかし、新たな秘密情報を追加したため、記憶負荷の増加が課題となる。今後は、複数回の録画攻撃や記憶負荷を考慮した改良方式を検討していきたい。

参考文献

- [1] 菅井文郎, 油田健太郎, 山場久昭, 朴美娘, 岡崎直宣, “アイコンとタッチパネル液晶を用いた覗き見耐性を持つ認証方式の提案”, マルチメディア, 分散, 協調とモバイル (DICO2012) シンポジウム, pp.2402-2409(2012).
- [2] Google, Android-open source project, <http://source.android.com/>
- [3] S.Wiedenbeck, J.Waters, L.Sobrado, and J.Birget, “Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme”, in International Working Conference on Advanced Visual Interfaces(AVI), May 2006.