モバイル端末における覗き見耐性を持つ認証方式の提案と実装

喜多 義弘† 菅井 文郎‡ 朴 美娘† 岡崎 直宣‡

†神奈川工科大学
243-0292 神奈川県厚木市下荻野 1030
y.kita@ccy.kanagawa-it.ac.jp
mirang@nw.kanagawa-it.ac.jp

‡宮崎大学
889-2192 宮崎県宮崎市学園木花台西 1-1
tf12006@student.miyazaki-u.ac.jp
oka@cs.miyazaki-u.ac.jp

あらまし 近年，スマートフォンなどのモバイル端末が広く普及し，それに伴い，モバイル端末内の個人情報などの漏洩が問題視されている．情報が盗まれることを防ぐため，PIN などを利用した画面ロックの解除認証が広く利用されている．しかし，既存の認証方式では，覗き見や録画に対する耐性がなく，認証情報が他人にばれてしまう危険性がある．そこで本研究では，モバイル端末における覗き見耐性を持つ認証方式を提案する．具体的には，持ち主のみが知り得る認証情報の間接的な入力法則により，覗き見耐性を有しつつ，偶然の認証成功による誤認証への対策を提案する．また，入力をグラフィカルなアイコンのタップ操作で行うことにより，覗き見耐性と高いユーザビリティも同時に実現する．提案手法をモバイル端末上に実装し，実験により評価を行う．

A Proposal and Implementation of Authentication Method for Mobile Terminals

Yoshihiro Kita† Fumio Sugai‡ MiRang Park† Naonobu Okazaki‡

†Kanagawa Institute of Technology
1030 Shimo-Ogino, Atsugi-city, Kanagawa 243-0292, JAPAN
y.kita@ccy.kanagawa-it.ac.jp
mirang@nw.kanagawa-it.ac.jp

‡University of Miyazaki
1-1 Gakuenkibanadai-Nishi, Miyazaki-city, Miyazaki 889-2192, JAPAN
tf12006@student.miyazaki-u.ac.jp
oka@cs.miyazaki-u.ac.jp

Abstract In recent years, mobile terminals such as smartphone come to be widely used. Most of such mobile terminals store many kinds of important data such as personal identifiable information. So, it is necessary to lock and unlock terminals using a personal authentication method such as Personal Identification Number (PIN) in order to prevent stealing data. However, most of existing authentification method have a common problem called “Shoulder-Surfing,” that means inferring authentification information by watching the authentification sequence. In this paper, a new icon-based authentification method is proposed that is simple but sufficiently secure even if other people watch authentification sequences. Proposed method is implemented on a mobile data terminal and evaluated through a series of experiments and questionnaire surveys.

1　はじめに

近年，スマートフォンなどに代表される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など重要な情報が格納されており，情報を盗まれることを防ぐために，画面の操作ロック (以下，画面ロック)，および，PIN(Personal Identification Number) などを利用した画面ロックの解除認証が広く利用されている．しかし，既存の多くの認証方式では，覗き見耐性が実現されておらず，人の目にさらされた環境で画面ロックの解除認証を行うと他人に認証情報がばれてしまう危険性がある．また，多くのモバイル端末は，タッチパネル液晶およびいくつかのボタンのみが標準の入力方法として搭載されている．既存の認証方式は，画面の小さいモバイル端末をターゲットにし，かつ，ユーザビリティについて考慮したものが少ない．そのため，扱いやすい入力方法によるユーザビリティを保ちつつ，覗き見耐性を持つ認証方法の研究開発が求められている．

我々は以前に，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を提案した [1]．この認証方式は，画面上のアイコンをタップして操作するという，扱いやすい入力方式によって高いユーザビリティを有し，覗き見攻撃や 1 回の録画攻撃に対する耐性を備えている．しかし，1 回の認証入力における認証成功の確率が比較的高いため，偶然に認証が成功する可能性も高い．この可能性を低くするには入力回数を多くする必要があるが，入力回数が多くなるとユーザビリティが低くなることが考えられる．

そこで本論文では，偶然に認証が成功すること (以下，確率的誤認証) に対する耐性を高めるために，従来の認証方式に更なる認証条件を追加した認証方式を提案する．そして，提案した認証方式を実装し，従来の方式と定量的に比較し，評価を行う．

2　研究背景

2.1　画面ロックによるセキュリティ

現在，デスクトップ端末や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．画面ロックとは，端末の操作ができる状態からユーザが任意に，または，予め設定した時間内にマウスやキーボードなどの入力がなかった場合に，端末の操作ができない状態にする機能である．

画面ロックの状態から再び端末の操作ができる状態にするためには，パスワード入力などの本人認証が必要になる．これは，デスクトップ端末では席を外している間などに，モバイル端末では端末の置き忘れ，紛失，または，盗難にあった場合などに，端末内の情報の漏洩や改ざんを防ぐ目的がある．

モバイル端末の画面ロックは，ポケットやバッグの中などに入れている間は，常に身に着けていても画面ロックの状態になるため，メールや電話など，モバイル端末を利用するたびに画面ロックの解除が必要になり，解除のための本人認証の頻度が多くなってしまう．このため，デスクトップ端末よりもユーザビリティに配慮した画面ロックの解除認証が重要になる．

2.2　覗き見耐性を持つ認証方式

覗き見耐性を持つ認証方式とは，認証動作を他人に見られていても認証情報が露呈しない方式である．覗き見耐性を持たない認証方式では，認証情報を盗まれないようにするために，常に周りの目を気にして認証しなければならない．また，他人に見られるだけでなく，監視カメラなどの録画機器に認証動作を録画され，認証情報が露呈する危険性もある．そのため，覗き見耐性を持たせるためには，何度も見られても認証情報が露呈しないように，認証方式を複雑にする必要がある．

覗き見による攻撃方法は，大きく 2 つに分けることができる．1 つは「他人が認証動作を直接覗き見る攻撃」(以下，覗き見攻撃) であり，もう 1 つは「監視カメラなどの録画機器によって

記録し解析する攻撃」(以下，録画攻撃) である．一般に，認証動作を完全に記録できる録画攻撃の方が，覗き見攻撃よりも耐性を持たせることが難しく，ユーザビリティも低下してしまう．

2.3 関連研究

上記で述べた問題を解決するために様々な手法が提案されている [1, 2, 3, 4, 5, 6, 7]．以下では，特に覗き見耐性またはユーザビリティに重きを置く認証方式と問題点について述べる．

2.3.1 背景配列の移動量を用いた個人認証方式

この方式は，パスワードによるチャレンジレスポンス型の個人認証方式として，入力を工夫し覗き見耐性を持たせた方式である [5]．文字の背景に異なる色や図形の配列 (背景配列) を表示し，背景配列が移動した量を用いて認証を行う．この方式は，録画攻撃に耐性を持つように工夫され，ATM などに適用することを目標としている．しかし，確率的誤認証に対する耐性を考慮した場合，使用できる文字をモバイル端末で画面に表示しやすい数字 10 文字のみとすると，ATM での既存方式と同じ確率を得るには，パスワードの長さは最低 14 文字必要である．これは，人が記憶するには困難なことが予想され，この方式をモバイル端末に用いることは困難である．

2.3.2 複数回の覗き見に耐性を有するパスワード認証方式

この方式は，0 から 9 までの番号を画面の左右に 4 桁ずつ配置し，予め定めた暗証番号が含まれている 4 桁の番号を右か左かで答える認証方式である [6]．覗き見への対策として，暗証番号が含まれていない場合の偽入力を備えており，暗証番号を特定されにくいように工夫されている．しかし，認証入力は右か左かという 2 つの入力しかないため，1 回の認証入力における認証成功の確率は 2 分の 1 であり，確率的誤認証に対する耐性は低いという問題がある．

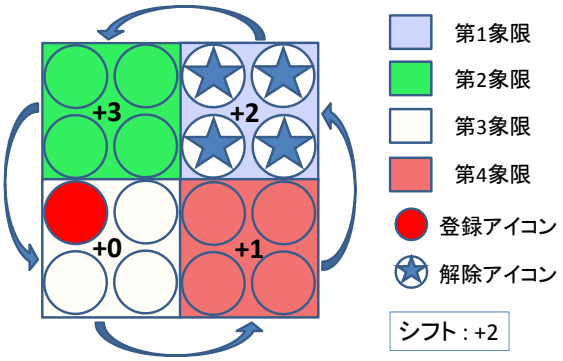

図 1: Secret Tap 方式

2.3.3 Android Password Pattern

この方式は，縦横に並んだ点に対し，認証情報として 4 点以上を結ぶパターンを予め決めておき，それを指でなぞり認証するという方式である．Google が開発し，Android 端末での画面ロックの解除方法として標準で採用されている方式である [7]．この方式は，ユーザビリティが高い反面，覗き見耐性が低いという問題がある．

2.4 Secret Tap 方式

我々が以前提案した，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がある [1]．この認証方式は，利用者個人が覚えやすいアイコンを予め用意し，その中から認証情報として正解のアイコンをいくつか登録する．認証時に複数回表示されるアイコン群の中から正解のアイコンを選択することにより認証を行うため，扱いやすい認証入力により，高いユーザビリティを保つことができる．

この認証方式には，覗き見耐性を持つ 3 つの認証方式を採用しており，その中の 1 つである Secret Tap 方式を，図 1 に示す．Secret Tap 方式は，4 × 4 マスの認証画面を用いて，認証情報として利用者が予め登録したアイコン (以下，登録アイコン) を必ず 1 つ含むアイコン群をランダムに表示する．そして，アイコンを 1 つタップすると，再び別のアイコン群をランダムに表示する．これを予め定めた入力回数分だけ繰り返し，すべての入力で認証情報として正しいア

イコンを選ぶと認証が成功し，画面ロックを解除する．

この方式では，覗き見攻撃への対策として，「シフト」という機能を提案している．シフトとは，アイコン群の中に表示された登録アイコンの象限から，予め定めた値 (シフト量) の象限だけ移動した先にある象限に表示されたアイコンを，認証情報として正しいアイコン (以下，解除アイコン) とする機能である．

シフト量について，図 1 を用いて説明する．まず，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 象限とする．そして，登録アイコンを含む象限からシフト量の分だけ反時計回りに象限を移動し，その移動先の象限内にある 4 つのアイコンを解除アイコンとする．例えば，図 1 の第 3 象限にある登録アイコンにおいて，シフト量を+2 とした場合，2 象限分だけ移動し，移動先の第 1 象限内にある 4 つのアイコンが解除アイコンになる．利用者はこの 4 つの解除アイコンのいずれかをタップすればよい．

アイコン群を象限によって分けることにより，登録アイコンを直接タップしなくても解除認証が可能になるため，覗き見されていても登録アイコンを特定されることはない．また，シフト量も+0 から+3 まで利用者が任意に予め登録できるため，登録アイコンをより特定されにくくなる．

しかし，この認証方式では，表示したアイコン群の 4 分の 1 は解除アイコンであるため，確率的誤認証の可能性が高いという問題点がある．確率的誤認証の耐性を持たせるには，認証の入力回数を増やすことが必要となる．しかしながら，ユーザビリティの観点から，利用者が記憶しておく必要のある登録アイコン数には限界がある．このとき，登録アイコン数よりも入力回数が多くなると，既に出現した登録アイコンが再び出現する可能性があり，覗き見攻撃や録画攻撃に対する耐性が低下してしまうという問題も出てくる．

3 提案手法

3.1 目的と設計方針

本研究では，モバイル端末の画面ロック解除において，覗き見耐性だけでなく，確率的誤認証に対する耐性を持つことを目的とした認証方式の提案を行う．提案手法では，前述した Secret Tap 方式 [1] に，新たな認証機能を追加することにより，確率的誤認証に対する耐性を高める．

認証の入力には，Secret Tap 方式と同様に，アイコンとタッチパネル液晶を用いたタップ操作による入力を用いる．アイコンは，利用者本人は覚えやすく，他人は覚えにくい性質がある．そのため，数あるアイコン群から特定のアイコンを選択することは，覗き見耐性を持たせる上で有用である．また，タッチパネル液晶を用いてアイコンを直接タップすることにより，直感的にアイコンを選択する操作ができ，ユーザビリティを保つことができると考えている．

提案する認証方式における目標として，以下の 4 つの項目を考慮する．

- 覗き見攻撃に対する耐性

  他人に何回も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とする．

- 録画攻撃に対する耐性

  録画により記録および解析されても認証情報が露呈することはない強度を持つこと．日常生活において，認証動作が監視カメラなどの録画機器に偶然写ってしまうことが考えられる．しかしながら，モバイル端末は移動しながら操作することが多く，1 つの録画機器に複数回録画される可能性が極めて低いと考えられる．そこで，録画攻撃のリスクを回避するために，1 回の録画攻撃に対して耐性を持つことを目標とする．

- 確率的誤認証に対する耐性

  認証動作の覗き見の有無に関係なく，偶然に認証を突破されることはない強度を持つこと．この耐性の強度は，ATM などで現

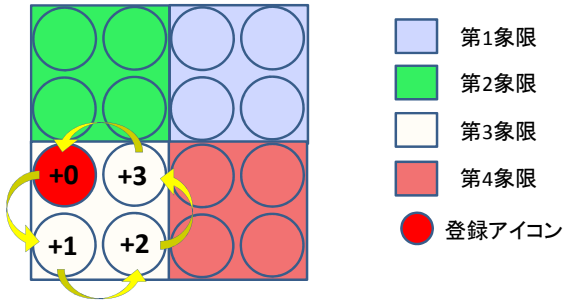

図 2: 象限内にシフトを用いた認証方式

在広く普及している 10 進数の PIN4 桁相当を目標とする．

- ユーザビリティ

  利用者に受け入れられるユーザビリティを持つこと．登録アイコン数は覚えやすい個数であることを目標とする．

3.2 STDS 方式

前述した各目標を達成するために，Secret Tap 方式を改良した Secret Tap with Double Shift (STDS) 方式を提案する．STDS 方式は，象限間のシフトに加え，象限内のアイコンもシフトを用いることで，2 種類のシフトを併用する方式である．この方式について，図 2 を用いて説明する．各象限内の 4 つのアイコンを，右上，左上，左下，および，右下のアイコンとして分ける．そして，登録アイコンからシフト量の分だけ反時計回りに移動した先のアイコンを解除アイコンとする．

STDS 方式を用いた例を，図 3 に示す．2 種類のシフトをそれぞれ区別するために，象限間のシフトを第 1 シフト，象限内のシフトを第 2 シフトとする．

図 3 において，第 1 シフトを+2，第 2 シフトを+1 とした場合，登録アイコン (第 3 象限・左上) に対し，解除アイコンは 1 つのアイコン (第 1 象限・左下) に定まる．これにより，表示したアイコン群に占める解除アイコンの割合は 4 分の 1 から 16 分の 1 になり，認証の入力回数を増やさなくても，確率的誤認証に対する耐性を高めることができる．

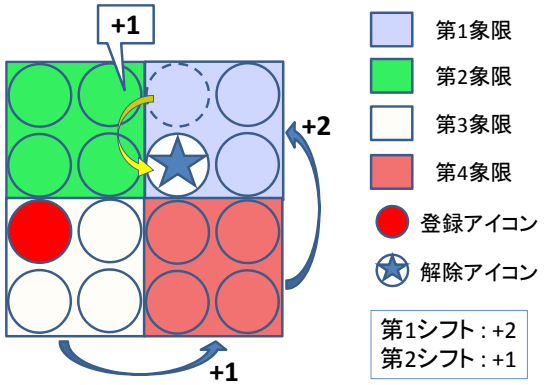

図 3: STDS 方式を用いた例

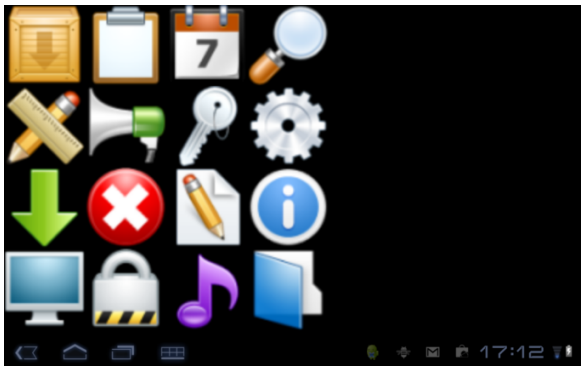

図 4: 実装したアプリケーションの認証画面

3.3 STDS 方式の実装

提案手法が確率的誤認証に対する耐性を有しているかを評価するために，STDS 方式を Android 端末上にアプリケーションとして実装した．実装したアプリケーションの認証画面を，図 4 に示す．メニューから，第 1 シフトおよび第 2 シフトのシフト量をそれぞれ定義することができる．そして，この認証画面を規定の入力回数だけアイコンをタップすると，認証に成功したか失敗したかを表示する．さらに，アイコン設定画面 (図 5 を参照) を実装し，入力回数および登録アイコンを設定できるようにした．登録アイコンは，50 個のアイコンの一覧表から任意のアイコンをタップすることにより設定でき，最大 10 個まで登録可能である．

また，1 回の録画攻撃の対策として，登録アイコンの出現確率を一連の認証動作を通して均一になるようにしている．この機能は，複数回の

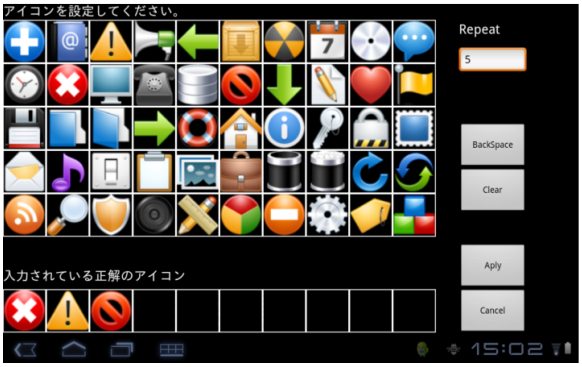

図 5: アイコン設定画面

認証中に既出のアイコンが再出現して，第三者にばれてしまうのを防ぐ目的がある．これにより，入力回数よりも登録アイコン数が多く，かつ，アイコン群として十分な数のアイコンを用意することができれば，1 回の録画攻撃に対しては，十分な強度の耐性を確保することが可能である．そのため，入力回数を増やさないことは，それを上回るために登録アイコン数を増やすことを抑えられるため，登録アイコン数を利用者が覚えやすい個数で設定しやすくなることが考えられる．

4 評価および考察

4.1 確率的誤認証に対する耐性の評価

STDS 方式，Secret Tap 方式, 10 進数 PIN, および, Android Password Pattern において，確率的誤認証の確率を表 1 に示す．確率的誤認証の確率は，入力回数が n 回の場合，Secret Tap 方式では $1/4^n$，STDS 方式では $1/16^n$ となる．同表において，10 進数 4 桁 PIN に相当する強度 (1/10000) を超える回数の確率は太字で示している．

確率的誤認証に対する耐性は表 1 より，STDS 方式の場合は入力回数が 4 回のときに 10 進数 4 桁 PIN に相当することが確認できる．Secret Tap 方式の場合は入力回数が 7 回のときに 10 進数 4 桁 PIN に相当し，Android Password Pattern よりも確率的誤認証に対する耐性が低いことが確認できる．これらから，STDS 方式は Secret Tap 方式よりも確率的誤認証に対する耐性が高くなったことが言える．

4.2 評価実験の実施

STDS 方式が，3.1 節の各項目を十分に有しているかを確認するために実験を行った．実験は，神奈川工科大学情報学部に所属する学生 8 人に被験者として協力してもらい，3.1 節の各項目の目標を達成しているかどうかを，実験結果を通して判断する．

4.2.1 登録アイコン数の評価実験

利用者にとって覚えやすい登録アイコン数を確認するために，即座に覚えることができるアイコン数の限度について調べた．被験者には，3.3 節で実装に用いた 50 個のアイコン群からランダムに選択したアイコンを 1 個から 10 個並べたものを，それぞれ 15 秒間ずつ見せた後に，50 個のアイコン群から覚えているアイコンを選択して答えてもらった．

見せたアイコンを全て正解した人数を，表 2 に示す．表 2 より，アイコン 5 個までは全員が全てのアイコンを正解し，6 個以降は正解者が著しく減っていることが確認できる．この結果から，覚えやすい登録アイコン数の限度は 5 個であることが言える．

前節で述べた確率的誤認証の確率より，STDS 方式は入力回数が 4 回で 10 進数 4 桁 PIN の強度と同等になるため，利用者が覚えやすい登録アイコン数の限度を超えずに，強度が十分である入力回数を設定できる．このことから，ユーザビリティを保ちつつ，確率的誤認証の耐性を有したことが言える．

4.2.2 複数回の覗き見攻撃に対する評価実験

覗き見攻撃に対する耐性を有しているかを確認するために，複数回の覗き見攻撃に対する評価実験を行った．実験方法として，STDS 方式と Secret Tap 方式について説明および試用し，十分な理解を得た上で，それぞれの認証方式を

表 1: 確率的誤認証の確率

入力回数	3 回	4 回	5 回	6 回	7 回	8 回
STDS 方式	1/4096	**1/65536**	1/1048576	1/16777216	–	–
Secret Tap 方式	1/64	1/256	1/1024	1/4096	**1/16384**	1/65536
10 進数 PIN	1/1000	**1/10000**	1/100000	10^{-6}	10^{-7}	10^{-8}
Android PP	–	1/1624	1/8776	**1/34792**	1/107704	1/248408

表 2: 見せたアイコンを全て正解した人数

見せたアイコン数	1 個	2 個	3 個	4 個	5 個	6 個	7 個	8 個	9 個	10 個
全て正解した人数	8	8	8	8	8	6	3	1	0	0

被験者に 10 回繰り返して見せ，登録アイコンを推察してもらった．

認証の条件として，登録アイコン数は前節の実験結果により 5 個，認証の入力回数は 10 進数の 4 桁 PIN に相当する強度を考慮し，STDS 方式は 4 回，Secret Tap 方式は 7 回とした．

本実験において登録アイコンを特定できた人数を，表 3 に示す．実験結果より，Secret Tap 方式ではアイコンを 1 個以上特定できた人が 2 名であるのに対し，STDS 方式では誰も特定できなかった．これにより，提案手法は覗き見攻撃に対する耐性を十分に有したことが言える．

4.3 1 回の録画攻撃に対する耐性の考察

認証入力画面を録画されているとき，認証入力画面に表示されている登録アイコンやそれ以外のアイコンにおいて，既出のアイコンが再出現すると，そこから認証情報を解析されてしまう可能性がある．

今回の実装では総アイコン数は 50 個であるが，認証入力のたびに画面上の全てのアイコンが入れ替わり，既出のアイコンが再出現しない程度の総アイコン数を有していると仮定した場合の，STDS 方式と Secret Tap 方式それぞれの 1 回の録画攻撃に対する耐性について比較し，考察する．

表 1 の確率的誤認証の確率より，10 進数の 4 桁 PIN に相当する強度を持たせるには，STDS 方式は 4 回，Secret Tap 方式は 7 回の入力回数が必要である．

認証入力のたびに既出の登録アイコンが再出現しないためには，入力回数分の登録アイコン数が必要である．4.2.1 節の実験結果より，利用者が覚えやすい登録アイコン数の限度は 5 個であるため，Secret Tap 方式の場合，入力回数分の登録アイコン 7 個を覚えることは利用者にとって負担になる．そして，負担を避けるために登録アイコン数を 5 個にすると，入力回数よりも登録アイコン数が少ないため，既出の登録アイコンが最高で 2 個再出現することになり，登録アイコンを特定される可能性がある．

一方，STDS 方式の場合，入力回数分の登録アイコン数は 4 個となるため，利用者にとって覚えやすい登録アイコン数に収まり，かつ，認証入力ごとに登録アイコンを含む全てのアイコンが入れ替わり，既出のアイコンが再出現しない認証入力画面を実現できる．この実現により，認証入力画面を偶然に録画されても，その画面から登録アイコンを特定する情報を与えることがなく，また，このときの全ての登録アイコンを特定される確率は，入力回数を 4 回とした場合，$1/16^4 = 1/65536$ であるため，登録アイコンを特定されにくい．

これにより，STDS 方式は 1 回の録画攻撃に対する耐性を十分に有したことが言える．

表 3: 登録アイコンを特定できた人数

特定できたアイコン数	0 個	1 個	2 個	3 個	4 個	5 個
STDS 方式	8	0	0	0	0	0
Secret Tap 方式	6	1	1	0	0	0

5 まとめ

本論文では，確率的誤認証に対する耐性を高めるために，従来の覗き見攻撃耐性を持つ認証方式である Secret Tap 方式に，新たな認証条件を追加した STDS 方式という認証方式を提案した．STDS 方式を Android 端末上に実装し，実際に確率的誤認証に対する耐性を有しているかを実験によって評価した．その結果，STDS 方式は Secret Tap 方式よりも確率的誤認証に対する耐性を有していることを確認できた．

今後の課題を以下に述べる．

- 複数回の録画攻撃への対策

  STDS 方式では，2 種類のシフトによって解除アイコンが 1 つのアイコンに定まる．そのため，複数の認証動作の記録を照らし合わせられ，2 種類のシフト量が解析されれば，登録アイコンが自ずと絞り込めてしまう．このことから，複数回の録画攻撃に対する耐性が低くなることが懸念される．

  この対策として，認証ごとに各シフト量を変更することなどが挙げられるが，それに伴うユーザビリティ低下の可能性も出てくるため，対策案を講じる必要がある．

- ユーザビリティの評価および向上

  第 2 シフトを追加したことにより，利用者はアイコンだけでなくシフト量についても覚え，考慮する必要があるため，ユーザビリティに影響が出る可能性がある．そこで，アイコンやシフト量によってユーザビリティにどれだけ影響があるかを評価し，ユーザビリティの向上を検討する必要がある．

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 (DICOMO2012) シンポジウム, pp.2402-2409 (2012).

[2] P.C. Van Oorschot, R.Biddle, S.Chiasson, “Graphical passwords: learning from first twelve years,” ACM Computing Surveys, Vol.44, No.4, (2011).

[3] 藤田和秀, 平川豊, “覗き見・盗撮に耐性を持つパスワード認証の検証,” 電子情報通信学会技術研究報告, MoMuC, モバイルマルチメディア通信, Vol.107, No.446, pp.61-66, (2008).

[4] 内山毅, “携帯端末等における覗き見攻撃への安全性を向上させる入力方法の提案,” 暗号と情報セキュリティシンポジウム (SCIS2012), 2E1-1, pp.1-6, (2012).

[5] 桜井鐘治, 撫中達司, “背景配列の移動量を用いた個人認証方式ののぞき見に対する安全性評価,” 情報処理学会論文誌, Vol.49, No.9, pp.3038-3050, (2008).

[6] 北林良太, 稲葉宏幸, “複数回の覗き見に耐性を有するパスワード認証方式の提案,” 電子情報通信学会技術研究報告, ICSS, 情報通信システムセキュリティ, Vol.109, No.115, pp.21-26 (2009).

[7] Google, “Android - open source project,” http://source,android.com/