RL-002

STDS 認証方式における録画解析による攻撃への耐性に関する一検討

A Study of Video-Analysis-Hack Resistant for STDS Authentication Method

喜多 義弘† 菅井 文郎‡ 朴 美娘† 岡崎 直宣‡
Yoshihiro Kita Fumio Sugai MiRang Park Naonobu Okazaki
西村 広光† 鳥井 秀幸† 岡本 剛†
Hiromitsu Nishimura Hideyuki Torii Takeshi Okamoto

1. はじめに

近年, スマートフォンなどのモバイル端末の普及により, それらを利用した様々なコンテンツやビジネス体系が確立されている. それに伴い, モバイル端末で個人情報や社内情報を扱う機会が増え, それらの情報漏洩が問題視されている. 情報漏洩を防ぐために PIN(Personal Identification Number, 暗証番号)やパターンなどを用いた個人認証が広く利用されている. しかしながら, 既存の多くの認証方式では, 覗き見耐性を持っておらず, 人の目にさらされた環境で認証動作を行うと, 認証情報が他人に漏洩する危険性がある. そのため, 覗き見耐性を持つ認証方式の研究開発が求められている.

我々は以前に, 2 種類のシフト機能を用いた覗き見耐性を持つ認証方式である STDS(Secret Tap with Double Shift)認証方式[1]を提案した. この認証方式は, 格子状にランダムで表示されたアイコンをタップして認証情報を入力する方式である. 認証の鍵となるアイコンは, ユーザが事前に登録したアイコンから 2 種類の移動法則(シフト機能)を用いて移動した先のアイコンとする. シフト機能による移動量はユーザしか知らず, 移動先のアイコンも認証の度に異なるため, 攻撃者は認証動作を目視しても認証情報を盗むことができない. しかし, 監視カメラなどの録画機器によって認証動作を複数回録画された場合, それらの記録を解析することでシフト機能による移動量が判明し, 登録したアイコンが特定されてしまう.

そこで本論文では, 認証情報の漏洩を防ぐために, 覗き見攻撃だけでなく, 録画解析による攻撃にも耐性を持つ認証方式を提案する.

2. 研究背景

2.1 画面ロックによるセキュリティ

モバイル端末には, 画面ロックの機能が搭載されている. 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の認証が必要になる. これは端末の置き忘れ, 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.

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, 端末を利用するたびに画面ロックの解除が必要になり, 解除のための個人認証の頻度が多くなる. このため, 安全性よりもユーザビリティが優先されがちになる.

画面ロックで利用される認証方式の 1 つに Android Password Pattern がある. この認証方式は, 格子状に並んだ点に対し, 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[2]. Google が開発し, Android 端末での認証方式として標準で採用されている. この方式はユーザビリティが高い反面, 認証動作を覗き見られると, 容易に認証情報が漏洩してしまう問題がある.

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漏洩しない方式である. 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, 認証情報が漏洩する危険性もある. 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漏洩しないように, 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.

† 神奈川工科大学, Kanagawa Institute of Technology
‡ 宮崎大学, University of Miyazaki

2.3 関連研究

2.3.1 背景配列の移動量を用いた個人認証方式[3]

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認証方式である．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，任意の入力によって偶然に認証が成功してしまうこと(以下，確率的誤認証)に対する耐性を考慮した場合，ATM での既存方式と同じ確率(10 進数 PIN 4 桁，1/10000)を得るには，パスワードの長さは 14 文字以上必要である．これは，ユーザが記憶するには困難なことが予想される．

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[4]

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．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，暗証番号が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の 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 1/2 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．

2.3.3 認証情報に画像を用いた認証方式[5]～[9]

認証情報にアイコンや写真などの画像を用いた認証方式であり，ユーザ本人にしか知りえない情報を認証情報にすることによって，覗き見攻撃への対策を施している．これらの論文は，数十個のアイコンをランダムに画面に表示し，ユーザが認証情報のアイコンを選択する認証方式である．ユーザが秘密情報として選択したアイコンを頂点とし，それらを結び囲んだ多角形内に含まれるアイコンを認証情報のアイコンとする．認証情報となるアイコンは，秘密情報のアイコンの位置によって毎回異なるため，認証動作を覗き見られても認証情報が漏洩することはない．しかし，録画解析により秘密情報のアイコンがある程度絞られてしまう可能性があるため，録画攻撃に対する耐性を有していない．

2.3.4 録画攻撃への耐性を有する認証方式[10]

録画攻撃への耐性を有する認証方式として，PIN と背景にあるマークの組み合わせによって認証を行う方式である．PIN は永続記憶による固定パスワードであり，マークは常にランダムに生成される使い捨てパスワードを利用している．その 2 種類の認証情報によって，どちらかの情報が漏洩しても認証情報の特定が困難である．しかし，この認証方式は，認証を行う前に使い捨ての認証情報である背景のマークを取得する手間が発生し，また，それを取得する際に覗かれないように人目を気にする必要がある．

3. 提案手法

本研究では，モバイル端末の画面ロック解除において，覗き見攻撃だけでなく，録画攻撃への耐性も持つことを目的とした認証方式を提案する．この認証方式では，数多くのアイコンからランダムに 16 個選択し，4×4 の格子状に配置する．この中にはユーザが認証情報として予め登録したアイコン(以下，登録アイコン)も含んでいる．認証の入力には，モバイル端末のタッチパネル液晶を用い，認証の鍵として表示したアイコン(以下，認証アイコン)をタップすることにより，入力を行う．認証アイコンは，登録アイコンから 2 種類のシフト機能を用いて移動した先のアイコンとする．

録画攻撃への耐性を持つために，2 つの機能を提案する．1 つは Any Shift という，2 種類のシフト機能のうちの 1 つの移動量を固定しない機能である．もう 1 つは Fake Mode という，ユーザが任意に選択した，シフト機能の移動量に関係しないアイコンをタップする機能である．これらの機能により，攻撃者がシフト機能の移動量を特定することができないため，録画されても登録アイコンが漏洩しないことが見込まれる．

提案する認証方式の目標を，以下に 3 項目挙げる．

- 覗き見攻撃に対する耐性
  他人に何回も認証動作を覗き見られても認証情報が漏洩しない強度を持つことを目標とする．
- 録画攻撃に対する耐性
  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に写ってしまうことが考えられる．そのときの脅威として，「攻撃者が認証画面と認証動作の両方の情報を得ること」と「攻撃者が同一ユーザの認証動作を複数得ること」の 2 つが考えられる．そのため，これらの脅威が発生しても認証情報が漏洩しない強度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を目標とする．その強度は，米国国立標準技術研究所の「電子的認証に関するガイドライン」[11]による，パスワードおよび暗証番号に必要な強度 2^{-14}(1/16384)を目指す．

図 1. 象限間シフトの移動方法

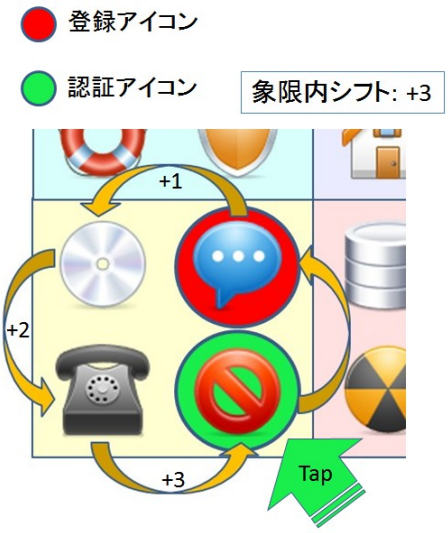

図 2. 象限内シフトの移動方法

3.1 STDS 認証方式

前述した目標を達成するために，我々が以前に提案した認証方式 STDS 認証方式[1]を利用する．本方式では，4×4 のアイコン群を 2×2 の 4 個組(以下，象限)のアイコン群に分ける．登録アイコンを含む象限から，「シフト」と呼ぶ独自の移動法則を用いて象限間または象限内を移動し，その移動先にあるアイコンを認証アイコンとする．シフトの対象が象限間の場合を象限間シフト，象限内の場合を象限内シフトとする．

図 3. 象限間シフトと象限内シフトの併用方法

象限間シフトの移動方法を，図 1 に示す．この例では，第 2 象限の左上のアイコンを登録アイコンとし，象限間シフトは+2 とする．登録アイコンがある第 2 象限から象限間を反時計回りに 2 象限分移動する．移動先の象限は第 4 象限となり，この象限に含まれるアイコンが認証アイコンの候補になる．

象限内シフトの移動方法を，図 2 に示す．この例では，第 3 象限を対象とし，象限内の右上のアイコンを登録アイコンとし，象限内シフトは+3 とする．登録アイコンから象限内を反時計回りに 3 アイコン分移動し，移動先のアイコンが認証アイコンの候補になる．

象限間シフトと象限内シフトの併用方法を，図 3 に示す．この例では，第 2 象限の右下のアイコンを登録アイコンとし，象限間シフトは+2，象限内シフトは+1 とする．まず登録アイコンがある第 2 象限から，象限間を反時計回りに 2 象限分先の第 4 象限へ移動する．次に第 4 象限内で，登録アイコンと同位置である右下のアイコンから象限内を反時計回りに 1 アイコン分移動する．移動先のアイコンが認証アイコンとなり，ユーザはこのアイコンをタップする．この動作を登録アイコンの数だけ繰り返し，認証を行う．

STDS 認証方式に録画攻撃への耐性を持たせるために，2 つの機能を導入する．1 つは Any Shift という，シフト値を固定せず，認証時にユーザが移動量を任意選択できる機能である．もう 1 つは Fake Mode という，認証時にシフト値での移動に関係のないアイコンを，ユーザが任意選択する機能である．これにより，認証動作を録画されても，攻撃者がシフト値を特定できないようにする．

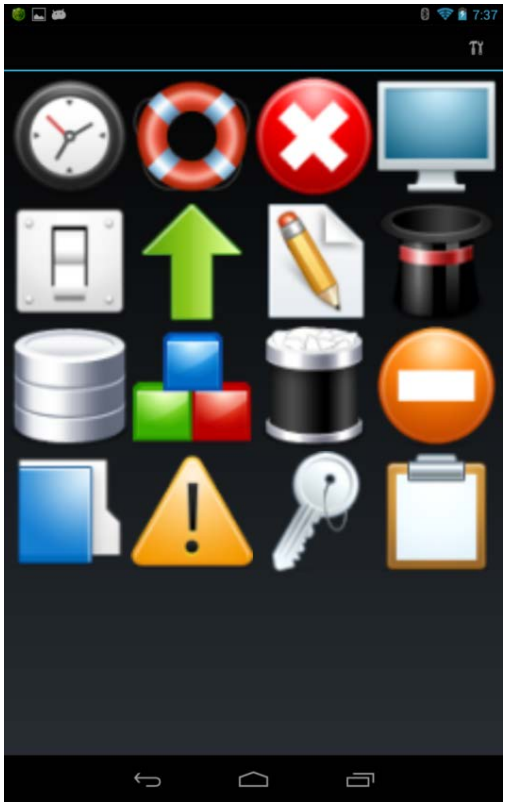

図 4. Android 端末上の認証画面

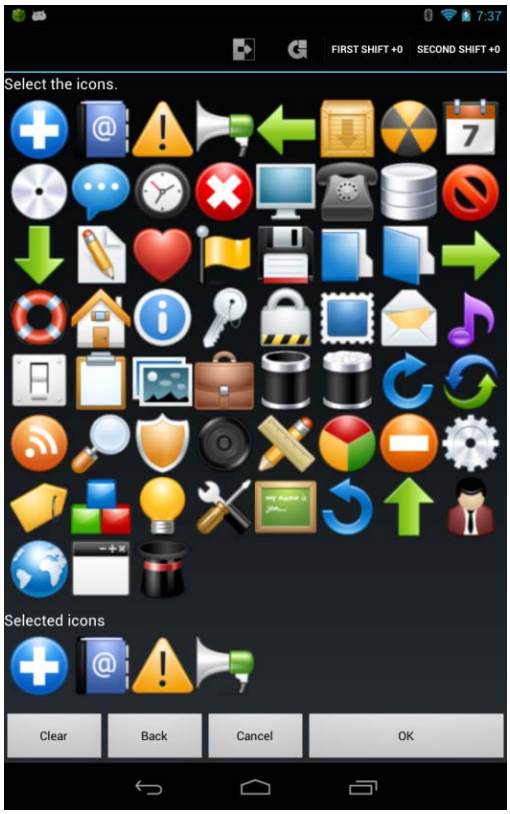

図 5.　アイコン登録画面

3.2 STDS 認証方式の実装

提案手法が，覗き見攻撃および録画攻撃への耐性を有しているかを評価するために，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．画面ロックを解除する際，この認証画面を自動的に表示する．ユーザは予め登録したアイコンとシフト値によって，認証アイコンを探し，タップする．タップするたびに表示しているアイコンがランダムに入れ替わる．登録アイコン数だけタップを行うと，自動的に認証判定に移行し，認証成功であればアプリケーションを終了できる．また，画面上部のアクションバー内にある右隅のアイコンをタップすることにより，アイコン登録画面へ移行する．認証失敗であれば再び認証画面を表示し，3 回以上認証を失敗すると，強制終了し，認証を行うことができなくなる．

アイコン登録画面を，図 5 に示す．この画面上で，ユーザは任意のアイコンを直接タップすることにより，アイコンを選択することができる．画面下部の 4 つのボタンによって，選択したアイコンに対して操作することができる．それぞれのボタンの機能は左より，Clear ボタンは選択アイコンの全解除，Back ボタンは選択アイコンの単数解除，Chancel ボタンはアイコン未登録のまま終了し，OK ボタンはアイコンを登録して終了する．画面上部のアクションバー内には各種機能のアイコンを表示している．それぞれのアイコンの機能は左より，モード切り替え，シフト回転向きの切り替え，象限間シフト値の選択，および，象限内シフト値の選択である．

3.2.1　シフト値 Any Shift の導入

例として，象限間シフトのシフト値選択画面を，図 6 に示す．この画面は，アイコン登録画面でアクションバー内にあるシフト値選択のアイコンをタップすることによって表示する．ユーザはこの画面上で+0～+3 のシフト値を任意に選択することによって，シフト値を決定することができる．

また，覗き見攻撃および録画攻撃への耐性の向上，および，ユーザビリティの向上のために，シフト値「Any Shift」を導入する．このシフト値は，+0～+3 のシフト値を全て含む値であり，各シフト値での移動先にあるいずれのアイコンも認証アイコンとして扱う．各シフトにおける Any Shift 時の解除アイコン例を，図 7 に示す．登録アイコンの位置を左上とし，一方のシフトを Any Shift，もう一方のシフトを+1 とする．図中の上の例は象限内シフトが Any Shift の場合であり，象限間シフトで移動した先の象限のアイコン全てが認証アイコンになる．一方，下の例は象限間シフト

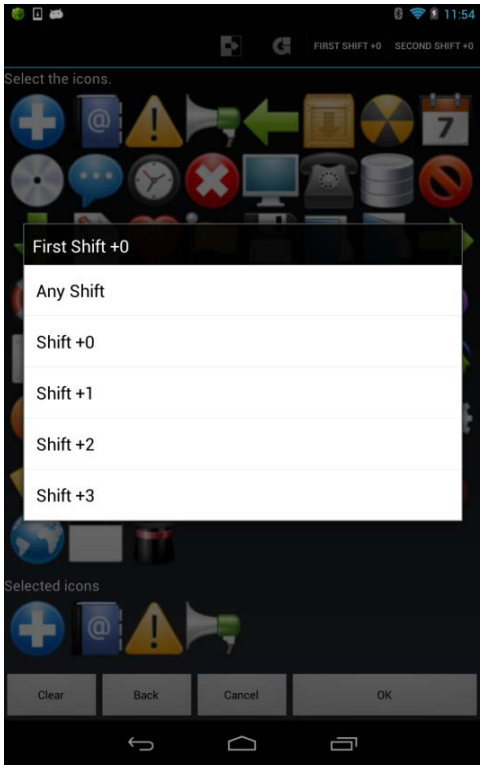

図 6. 象限間シフトのシフト値選択画面

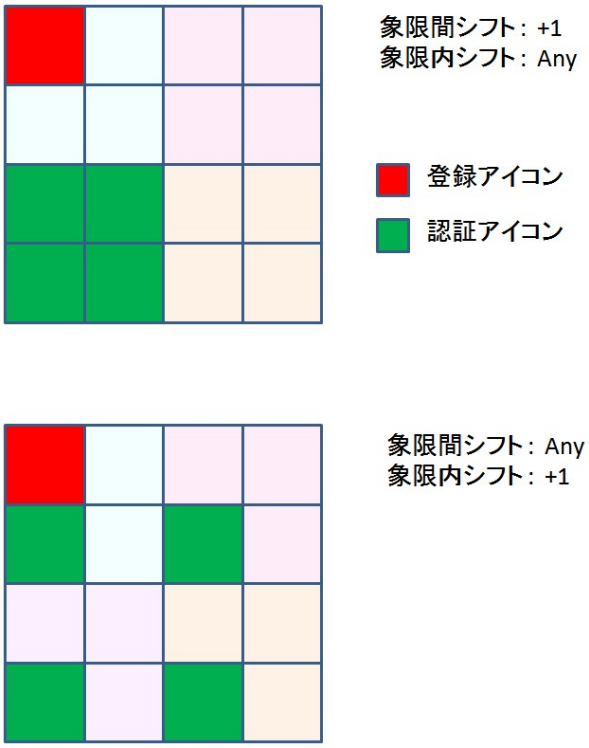

図 7. 各シフトにおける Any Shift 時の解除アイコン例

が Any Shift の場合であり，全ての象限において，象限内シフトによる移動を行う．これによって，認証アイコンが 4 個になり，ユーザはこれらのアイコンのいずれかをタップすることによって，認証を行うことができる．両シフト共に Any Shift にした場合，それぞれのシフト値は+0 に自動リセットする．

認証入力の際に，Any Shift を用いて認証アイコンを任意にタップすることにより，攻撃者を混乱させ，シフト値を容易に特定できないようにすることができる．また，ユーザもシフトの動きさえ把握していれば，片方のシフト値のみを考慮するだけでよく，シフト値の計算の負担を軽減することができる．しかし，認証アイコンが 1 画面につき 4 個になることにより，確率的誤認証の確率が上がってしまうことが考えられる．

3.2.2 録画攻撃対策用モード Fake Mode の導入

Any Shift によって覗き見攻撃への耐性を上げることができるが，片方のシフト値を固定しているため，録画攻撃によって認証動作を解析された場合，シフト値が特定されてしまう可能性がある．そこで追加の機能として，Fake Mode を導入する．

Fake Mode は，認証入力の際，アプリケーションが合図を発したときに認証アイコンとは異なるアイコンをわざと入力することによって，攻撃者の混乱を誘う認証方式である．合図には，バイブレート機能を用いる．その理由として，覗き見や録画されている場合でも，攻撃者に気づかれることなく，ユーザに合図として伝えることができるからである．なお，Fake Mode による偽の入力は認証の成否判断に用いない．そのため，1 回の認証におけるアイコンのタップ数は，「登録アイコン数+偽の入力数」になる．

Fake Mode で認証を行うことにより，もしも認証動作を録画されても，シフト値が固定していないため，特定することが困難になる．そのため，録画攻撃に耐性を持つことができると考えられる．

4. 評価

4.1 覗き見攻撃耐性の評価

本提案手法の覗き見攻撃耐性を評価するために，覗き見攻撃の実験を行った．被験者として，神奈川工科大学情報学部の学生 8 人に協力してもらった．

8 人の被験者から親を 1 人決め，親が他の 7 人が見ている前で，PIN，Android Password Pattern，本提案方式の 3 種類の認証方式を行い，他の 7 人はその認証動作を覗き見て，認証情報を見破る実験を行った．この時の登録した認証情報は普段の画面ロック解除に使用することを想定し，PIN は 4 桁の数字，Android Password Pattern は 7 個の頂点，提案方式はアイコン数 4 個である．認証動作は 10 回繰り返した．その結果，PIN およ

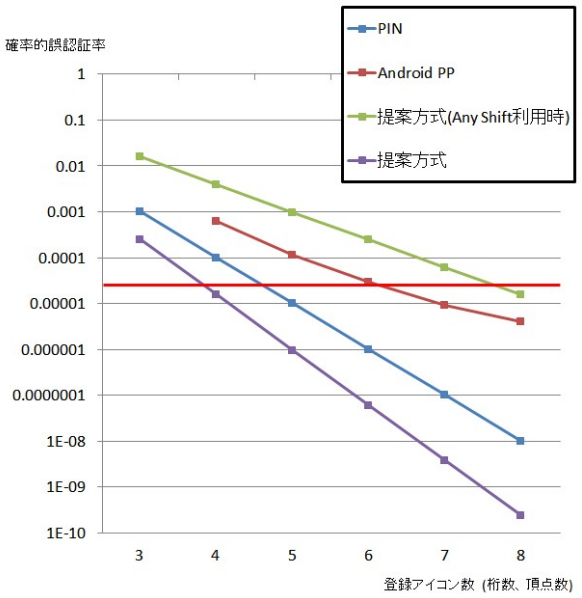

図 9. 各認証方式における確率的誤認証率

び Android Password Pattern は全員が認証情報を見破ったが，提案方式は全員とも認証情報を見破ることができなかった．これにより，提案方式は覗き見攻撃に耐性を有していることが言える．

4.2 確率的誤認証率の評価

各認証方式における確率的誤認証率を，図 9 に示す．PIN，Android Password Pattern，提案方式の 3 つの認証方式を比較し，提案方式についてはシフト値を Any Shift 利用時と他のシフト値の場合に分けている．グラフの縦軸が確率的誤認証率であり，横軸が登録アイコン数(PIN の場合は桁数，Android Password Pattern の場合は頂点数)を示す．グラフ中の赤線は，目標値である 2^{-14}(1/16384)の確率的誤認証率を示す．

グラフより，提案方式では登録アイコン数が 4 個であれば，目標値を達成することが確認できる．Any Shift 利用時の場合は，目標値を達成するには登録アイコン数が 8 個以上必要であり，PIN や Android Password Pattern と比較しても確率的誤認証率が高いことが確認できる．また，8 個以上の登録アイコンを覚えることは，ユーザに負担がかかることが懸念される．対策として，認証入力時に提示するアイコン数を現在の 16 個(4×4)から増やすことによって，確率的誤認証率を低くすることが考えられるが，モバイル端末上で提示できるアイコンの数や大きさを考慮する必要がある．

4.3 録画攻撃耐性の評価

本提案手法の録画攻撃耐性を評価するために，今回導入した Any Shift と Fake Mode において，攻撃者が認証画面と認証動作の両方の情報を得た場合と，攻撃者が同一ユーザの認証動作を複数得た場合の録画攻撃耐性について，それぞれ考察を行う．

4.3.1 Any Shift を使用する場合の録画攻撃耐性の評価

(1) 攻撃者が認証画面と認証動作の情報を得た場合
Any Shift を使用しないときは，認証画面よりユーザがタップしたアイコンを基に，シフト値別に全てのアイコンを割り振ることができる．そのため，登録アイコンの数に関わりなく 16 通りの登録アイコンの候補に絞られてしまう．一方，Any Shift を使用したときは，4 箇所の認証アイコンからユーザが任意に 1 個を選択するため，1 回の入力に対して登録アイコンの候補が 4 通り考えられ，それ以上絞り込むことができない．そのため，登録アイコン数を n，すなわち，n 回の入力では登録アイコンの候補が 4^n 通りになり，この中から登録アイコンを特定することは困難である．

(2) 攻撃者が同一ユーザの認証動作を複数得た場合
本提案手法では，認証のたびにアイコンの配置や種類が変化するため，複数の認証動作を比較することによって，常に固定である登録アイコンを特定されやすい．Any Shift を使用した場合でも，各認証動作を通して共通の候補を絞り込むことによって，登録アイコンを特定されてしまう．

これらにより，Any Shift を使用すると，認証画面と認証動作の両方を録画されても特定されにくいが，複数の認証動作を録画された場合は，登録アイコンを特定されやすくなることが言える．

4.3.2 Fake Mode を使用する場合の録画攻撃耐性の評価

(1) 攻撃者が認証画面と認証動作の情報を得た場合
Any Shift と同様に，タップしたアイコンを基にシフト値別にアイコンを振り分けると，16 通りのアイコン群に振り分けることができる．しかし，1 つのアイコン群には Fake Mode による偽の入力も含まれるため，登録アイコン数を n，偽の入力数を f としたとき，1 つのアイコン群から得られる登録アイコンの候補は ${}_{(n+f)}C_n$ になる．これにより，登録アイコンの候補は総数で ${}_{(n+f)}C_n \times 16$ 通りとなり，この中から登録アイコンを特定することは困難である．

(2) 攻撃者が同一ユーザの認証動作を複数得た場合
これも Any Shift と同様に，登録アイコンが固定であるため，複数の認証動作を比較すると共通の候補が絞り込めるため，登録アイコンを含むアイコン群を特定されてしまう．また，偽入力のアイ

表 1. 各機能および改良案の特徴

	複数の録画データ解析により絞り込まれる登録アイコン候補数	確率的誤認証率	ユーザビリティ
Any Shift	$4^{(n+1)}$	$1/4^n$	STDS 認証方式と同等
Fake Mode	${}_{(n+f)}C_n$	$1/16^n$	STDS 認証方式と同等
登録アイコンと偽の入力回数の増加	${}_{(n+f)}C_n$	$1/16^n$	ユーザの負担増加
出現アイコンのシフト値別の固定	${}_{(n+f)}C_n \times 16$ または ${}_{(n+f)}C_n \times 4^{(n+f)}$	$1/16^n$ または $1/4^n$	STDS 認証方式と同等
シフト値の変動	${}_{(n+f)}C_n \times 16^n$ または ${}_{(n+f)}C_n \times 4^{(n+f)n}$	$1/16^n$	ユーザの負担増加

コンも，ユーザの任意で選択するが常に同じアイコンが出現するとは限らないため，認証のたびに異なり，その結果アイコン群の中の登録アイコンも特定されてしまうことが考えられる．

これらにより，Fake Mode を使用した場合も，Any Shift と同様に，認証画面と認証動作の両方を録画されても特定されにくいが，複数の認証動作を録画された場合は，登録アイコンを特定されやすくなることが言える．

4.3.3 複数の録画データ解析への対策とその耐性の考察

複数の録画データを解析された場合，現段階の本提案手法においては，登録アイコンを特定されやすい．そこで，本提案手法の改良案として，以下を挙げる．

- 登録アイコン数と偽の入力数を増加する
- 出現するアイコンをシフト値別に全て固定する
- シフト値が入力のたびに変動する

それぞれの改良案における録画攻撃への耐性について，以下に述べる．

(1) 登録アイコン数と偽の入力数の増加

4.3.2 節より，登録アイコンを含むアイコン群を特定された場合，さらにそこから絞り込まれる登録アイコンの候補数は${}_{(n+f)}C_n$ である．そのため，登録アイコン数と偽の入力回数を増やすことにより，その候補数は増加し，登録アイコンの特定を一時的に防ぐことができる．しかし，登録アイコン数と偽の入力回数を増やすことにより，ユーザが入力する回数も増加し，ユーザの負担が大きくなることが懸念される．また，認証動作をさらに録画されれば，登録アイコンが特定されやすくなるため，根本的な解決には至らない．

(2) 出現アイコンのシフト値別の固定

登録アイコンだけでなく全てのアイコンの種類や出現パターンをシフト値別に固定することにより，複数回の録画データを比較しても絞り込むことができないため，Fake Mode を使用したときの登録アイコンの候補数${}_{(n+f)}C_n \times 16$ 通りを維持することができる．また，Any Shift を組み合わせることによって，その候補数を${}_{(n+f)}C_n \times 4^{(n+f)}$まで増大することができる．そのため，これらの候補数から登録アイコンを特定することは困難である．また，確率的誤認証率を考慮すると，Fake Mode のみの場合の確率的誤認証率は $1/16^n$ になるが，Any Shift を併用した場合の確率的誤認証率は $1/4^n$ となり，目標である $2^{-14}(1/16384)$ の強度を保つことが困難になる．

(3) シフト値の変動

現段階の本提案手法ではシフト値が固定であるため，登録アイコンを含むアイコン群がシフト値別の 16 通りのみである．しかし，入力のたびにシフト値を変動させることにより，そのアイコン群の総数は 16^n になる．そこから Fake Mode を考慮した登録アイコンの候補数は${}_{(n+f)}C_n \times 16^n$ 通りになり，さらに Any Shift を併用すると登録アイコンの候補数は${}_{(n+f)}C_n \times 4^{(n+f)n}$ 通りになる．これらの中から登録アイコンを絞り込むことは困難である．しかし，出現するアイコンは固定ではないため，録画データがさらに増えると登録アイコンを特定される可能性がある．また，入力のたびにシフト値を変動すると，ユーザはそのたびにシフトを計算して移動先のアイコンを探索することになるため，ユーザの負担が大きくなることが懸念される．

4.3.4 録画攻撃への耐性のまとめ

4.3.3 節の複数の録画データ解析に対する改良案も含めた，各機能および改良案の特徴について，表 1 に示す．各機能において，覗き見攻撃耐性と攻撃者が認証画面と認証動作の両方の情報を得た場合の録画攻撃耐性については有しているとする．表より，4.3.3 節で述べた改良案は複数の録画データ解析への耐性を有することが言える．それらの案を実装する際，確率的誤認証を優先する場合は，登録アイコンや偽の入力回数の増加およびシフト値の変動が有効であると言える．一方，ユーザビリティを優先する場合は，出現アイコンのシフト値別の固定が有効であると言える．

さらなる発展として，これらの案を組み合わせ，それぞれの特徴を活かすことにより，有用性が拡大することが見込まれる．例えば，出現アイコンの種類をシフト値別に固定し，さらにシフト値を変動させることにより，確率的誤認証率が Fake Mode のみの場合は 1/16 から $1/16^n$ に，Any Shift を併用する場合は $1/4^n$ から $1/4^{(n+f)n}$ になり，ユーザビリティを保持したまま確率的誤認証への耐性の目標を達成することができると見込んでいる．

5. おわりに

本研究では，モバイル端末の画面ロック解除認証時において，覗き見攻撃および録画攻撃による認証情報の漏洩を防ぐために，覗き見攻撃および録画攻撃に耐性を持つ STDS 認証方式を提案した．認証方式は，画面上のアイコンをタップすることによって認証入力を行う方法を用いた．覗き見攻撃への対策として，2 種類のシフト機能によって登録アイコンの情報が露呈しない方法を用いた．録画攻撃への対策として，シフト値 Any Shift や端末のバイブレート機能を利用した Fake Mode によって，シフト値や登録アイコンを特定させない方法を提案した．

また，実験によって，覗き見攻撃に対する耐性と確率的誤認証に対する耐性を有することを確認し，録画攻撃に対する改良案を考察できた．これらにより，本提案手法を用いることによって，覗き見攻撃および録画攻撃による情報漏洩を防ぐことができる．

今後の課題を以下に述べる．

- 確率的誤認証への対策
  Any Shift を用いた提案手法は，既存の認証方式よりも確率的誤認証への耐性が低く，覗き見されなくても偶然に認証を突破される可能性がある．そのため，1 回の入力に提示するアイコン数を増やすなどの対策が必要であるが，モバイル端末上で扱うことができるアイコンの数や大きさを考慮する必要もある．
- ユーザビリティの向上
  Any Shift や Fake Mode により，シフトの計算が減ることでユーザビリティの向上を期待できるが，確率的誤認証の対策を考慮した場合，提示するアイコン数や登録アイコン数の増加によって，ユーザビリティが低下することも考えられる．そのため，シフトの計算の簡略化などの対策を講じる必要がある．

参考文献

[1] 喜多義弘，菅井文郎，朴美娘，岡崎直宣: 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，コンピュータセキュリティシンポジウム(CSS2012), 2D2-1, pp.1-8 (2012).

[2] Google: Android – open source project, http://source.android.com/

[3] 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).

[4] 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).

[5] Wazir, Z.K., Mohammed, Y.A., Yang, X.: A Graphical Password Based System for Small Mobile Devices, International Journal of Computer Science Issue, Vol.8, Issue 5, No.2, pp.145-154 (2011).

[6] Arash, H.L., Omar, B.Z., Samaneh, F., Rosli, S.: Shoulder Surfing Attack in Graphical Password Authentication, International Journal of Computer Science and Information Security, Vol.6, No.2, pp145-154 (2009).

[7] Luigi, C., Clemente, G.: A Graphical PIN Authentication Mechanism with Applications to Smart Cards and Low-Cost Devices, Proceedings of the 2nd IFIP WG 11.2 International Conference on Information Security Theory and Practices: Smart Devices, Convergence and Next Generation Networks, pp.16-35 (2008).

[8] Lugi, C., Clemente, G.: On the Security of a Two-Factor Authentication Scheme, Proceedings of the 4th workshop on Information Security Theory and Practices (WISTP 2010), pp.245-252 (2010).

[9] Windenbeck, S., Waters, J., Sobrado, L., Birget, J.C.: Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, Proceedings of the Working Conference on Advanced Visual Interfaces, pp.177-184 (2006).

[10] 高田哲司: fakePointer：映像記録による覗き見攻撃にも安全な認証手法，情報処理学会論文誌，Vol.49，No.9，pp.3051-3061 (2008).

[11] NIST Special Publication 800-63-1 Electronic Authentication Guideline, National Institute of Standards and Technology, (2011).