様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１４　日現在

機関番号：　３２６４４
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2016
課題番号：　２５３３０１５９

研究課題名（和文）Smudge攻撃に耐性を有するタッチスクリーン型モバイル端末向けユーザ認証方式

研究課題名（英文）A User Authentication Method for Touch Screen Devices Having the Tolerance to Smudge Attacks

研究代表者

内田　理（Uchida, Osamu）

東海大学・情報理工学部・教授

研究者番号：５０３２９３０６

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：スマートフォンをはじめとするタッチスクリーン端末では、機密情報を含むドキュメントファイルの閲覧やダウンロードが日常的に行われるため、従来型の携帯電話よりセキュリティの向上が必要とされる。本研究では、スクリーン上の汚れから認証パターンを推測するsmudge攻撃に耐性を有するタッチスクリーン端末向けユーザ認証手法を提案し、実際にスマートフォン向けアプリケーションとして実装した。提案手法は、ユーザ自身が撮影した画像をパス画像として利用する画像認証方式であり、覗き見攻撃や録画攻撃にも耐性を有している。また、認証成功率や攻撃耐性に対する各種考察を行い、それらを向上させるため改良についても検討を行った。

研究成果の概要（英文）：Users of smartphones and/or tablet computers browse and download confidential document
files routinely. Therefore, the higher security level is needed for smartphones and tablet computers than conventional mobile phones (feature phones). In this study, we proposed a user authentication method for touch screen devices that is resistant to smudge attacks, which guesses authentication pattern from dirt on the screen. We actually implemented it as an application for smartphones. The proposed method is an image authentication method that uses images taken by users themselves as pass images, and is also resistant to observation attacks and recording attacks. In addition, we conducted various considerations on the success rate of authentication and attack resistance, and examined improvements to improve them.

研究分野：　情報通信工学

キーワード：　ユーザ認証　画像認証　スマートフォン　タッチスクリーン端末　smudge攻撃

１．研究開始当初の背景

近年、スマートフォンやタブレット型端末など、タッチスクリーン搭載型モバイル端末が急速に普及しており、今後もこのような傾向が継続すると考えられる。最近は通信速度の向上やクラウド型ストレージサービスの普及などにより、 スマートフォンを用いて外出先から機密情報を含む各種ドキュメントファイルの閲覧や編集、ダウンロードを行うことが日常的に行われるようになり、従来型の携帯電話よりもセキュリティの向上が必要とされている。スマートフォンにおけるスクリーンロックは、標準では画面の指定された場所をフリックする（指でなぞる）だけで解除できるため、セキュリティの意味合いは有していない。スクリーンロック解除に認証を掛ける場合には、Android 端末においては「ロック No. 方式」、「パスワード方式」、「パターン方式」の三種類の方法が用意されている．このうち「ロック No. 方式」、「パスワード方式」は、一般的に利用される PIN コード認証やパスワード認証と同様のものであるため、タッチスクリーンであり、なおかつスクリーン領域が小さいスマートフォンでは使い勝手が良い方式であるとは言えない。「パターン方式」は画面上に表示される 9 つの点から 4 つ以上の点を自分で設定した順番に指でなぞる方式である（同じ点を 2 回通ってはいけない等の制約有り）。この方式におけるロックパターンは 389,112 通りあり、セキュリティの強度としては 5 桁の PIN コードよりも強く、また指でなぞるというタッチスクリーンの特性を活かした使い勝手の良い認証方式である。しかし、この「パターン方式」には smudge 攻撃（汚れ攻撃）という攻撃手法が存在する。これは、タッチスクリーン上の汚れからユーザの最近の入力についての情報を得てロックパターンを推測するという攻撃であり、高い確率でパターンの推測が可能であるとの実験結果が知られている。そこで本研究では、smudge 攻撃に耐性を有するスマートフォン向けユーザ認証方式について検討を行う．

２．研究の目的

近年、スマートフォンなどモバイル環境での利用を前提とした端末の普及が進んでいるが、ユーザ認証は簡易な方法である場合が多く、セキュリティ上の危険性が指摘されている。タッチスクリーン向けユーザ認証方式の一つに、指でスクリーン上のパターンをなぞる「指リスト方式」というものがある。セキュリティ強度、及び使い勝手の良さから多くのスマートフォンユーザに利用されているが、スクリーン上の汚れから認証パターンを推測する smudge 攻撃の有効性が報告されている。本研究では、smudge 攻撃に耐性を有するタッチスクリーン向けユーザ認証方式の提案、実装、及び検証実験を行う。更に、端末に搭載されている各種センサの利用も併せて検討し、タッチスクリーン搭載型端末での利用に最適化されたユーザ認証方式の開発を目指す。

３．研究の方法

画像を用いた認証方式の採用を検討する。画像認証は、通常のパスワード方式における文字列の代わりに画像を用いて認証する方式である。画像認証の利点として、画像は記憶が比較的容易であること、キーロガーなどによるハッキングへの耐性が高いことなどが挙げられる。画像認証方式には様々なものが提案されているが、多くはおとりを含む複数枚の画像の中から、ユーザがあらかじめパスワードの代わりとして登録したパス画像を正しく選択することで認証を行う。本研究でもパス画像とおとり画像を複数枚表示し、それを決められたルールに従って指でフリックすることによりアンロックする方式を検討する。パス画像とおとり画像の表示方法を工夫することにより、smudge 攻撃への耐性を持たせることが可能となる。また、これまで提案されている画像を用いた認証方式は、推測攻撃やのぞき見攻撃に対する耐性の面で課題を残しているが、本研究ではカメラ機能を搭載したスマートフォンの特性を活かし、パス画像をユーザが日々撮影する写真によって逐次更新することによる耐性強化を検討する。

４．研究成果

本研究では、一貫して Smudge 攻撃を代表とする各種攻撃への耐性を有するタッチスクリーン端末向けユーザ認証方式について検討を行った。以下にその成果を時系列順に列挙する。

(1) Smudge 攻撃への耐性を有するユーザ認証の基本方式の提案

ユーザ自身が撮影した画像をパス画像やおとり画像として利用するタッチスクリーン端末向け画像認証方式を提案した。本方式は、複数枚の画像をスクリーンに表示し、パス画像をスワイプさせることにより認証を行う。パス画像やおとり画像の表示位置が毎回変わるため、smudge 攻撃に耐性を有している。また、直近に撮影した画像をパス画像として利用するため、写真撮影を行うたびにパス画像が更新されることとなり、覗き見攻撃への耐性も有している。図 1 に認証動作の例を示す。この例では、認証動作は 3 回とし、スワイプする方向は上下左右、及び各斜め方向の合計 8 方向としている。ユーザは予め、各認証回におけるスワイプ方向、及び認証画面にパス画像が出現した際にパス画像をスワイプする方向を記憶しておく。パス画像が現れなかった場合には、任意のおとり画像を指定された方向にスワイプすればよい。本方式は画像をスワイプするだけで認証できるため、タッチスクリーン端末での認証に適し

図 1 Smude 攻撃への耐性を有するタッチスクリーン端末向けユーザ認証方式の動作例

た方法であると言える。

(2) セキュリティ強度を向上させたタッチスクリーン端末向け画像認証方式の提案

(1) で提案した手法は、smudge 攻撃への耐性は有しているが、セキュリティ強度が低いという問題点があった。認証動作の回数を N、表示される画像の枚数 P、スワイプ方向を D としたとき、パスワード空間の大きさは PD^N であり、(1)で想定していた N= 3、P= 9、D = 8 の場合 4,608 となる。これは 4 ケタの PIN コードよりも小さい。そこで、(1)の手法に改良を加え、高いセキュリティ強度を有する手法を提案した。具体的には、ユーザ自身が撮影した端末内の画像のみならず、Web から取得した画像（フェイク画像）も認証に利用することにより、セキュリティ強度の向上を図った。また、Android 端末用アプリケーションとして実装した（SWIPASS と命名）。本改良によりセキュリティ強度は高くなった（(1)の手法よりパスワード空間の大きさが P 倍拡大して P^2D^N となった。従って、N= 3、P= 9、D = 8 の場合 41,472 となり 4 桁の PIN コードよりも大きい）。しかし、smudge 攻撃への耐性は損なわれず、ユーザの記憶負荷も増加しない。また、覗き見攻撃を想定した実験の実施により、覗き見攻撃への耐性の評価も行ったところ、実用的な耐性を有していることがわかった。

(3) SWIPASS の認証成功率を向上させるための改良法の提案

(2)で実装した SWIPASS は、パス画像と類似する画像が端末内に存在する場合、ユーザがパス画像を識別できず認証に失敗してしまうケースが生じるという問題点があった。そこで、パス画像と誤認識する可能性が高い画像をおとり画像として認証画面に表示する対象から除外する手法を提案した。提案手法は具体的には、色合いや空間周波数の類似性に基づいてパス画像と誤認しやすいおとり画像を抽出し除外する。図 2 に画像除外の例を示す。左がパス画像であり右がおとり画像であるが、本手法により右のおとり画像は除外され認証画面に表示されなくなる。これにより、認証成功率の向上が期待される。

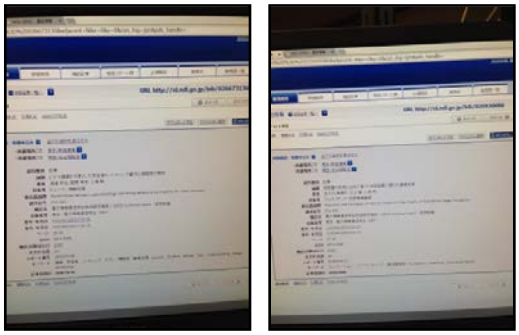

図 2 提案手法による類似画像除外の例

(4) SWIPASS の攻撃耐性を向上させるための改良法の提案

(2)で実装した SWIPASS は、認証時に必ずスワイプ対象となるフェイク画像が、端末の不正利用を目的とする攻撃者によって特定されやすいという問題点が存在した。そこで、認証に使われる画像に不鮮明化処理を施すことにより、攻撃耐性を向上させる手法を提案し、実験によりその有用性を検証した。

上記(1)～(4)の成果は、雑誌論文（3 件）、及び学会発表（6 件）にて公表した。なお、(4)の成果については雑誌論文への投稿を準備している。

５．主な発表論文等

〔雑誌論文〕（計 3 件）

(1) 鈴木 壮史, 小杉 将史, 内田 理, “タッチスクリーン端末向け認証方式 SWIPASS における認証成功率向上のための検討”, 画像電子学会誌, Vol.46, No.2, pp.330-335, April 2017.
URL:
http://cebook.dolab.jp/DcSeRO/DcSeRO57.dll?JVV&ID=4MKEXB1xC7

(2) Masafumi Kosugi, Tsuyoshi Suzuki, Osamu Uchida and Hiroaki Kikuchi, “SWIPASS: Image-Based User Authentication for Touch Screen Devices”, Journal of Information Processing, Vol.24, No.2, pp.227-236, March 2016.
URL:
http://doi.org/10.2197/ipsjjip.24.227

(3) 高橋 達哉, 内田 理, “Smudge 攻撃への耐性を有するスマートフォン向けユーザ認証方式”, 画像電子学会誌, Vol.42, No.5, pp.650-654, Sept. 2013.
URL:
http://cebook.dolab.jp/DcSeRO/DcSeRO57.dll?JVV&ID=kEU5vo3D5S

〔学会発表〕（計 6 件）

(1) Tsuyoshi Suzuki, Masafumi Kosugi, Osamu Uchida, “Improvement of Attack Resistance for the User Authentication Method for Touch Screen Devices “SWIPASS” by Image Blurring”, Image Electronics and Visual Computing Workshop 2017, 2017 年 3 月 2 日, ダナン(ベトナム）.

(2) 鈴木 壮史, 小杉 将史, 内田 理, “ボロノイ図を用いた画像の不鮮明化によるタッチスクリーン端末向け認証方式 SWIPASS の攻撃耐性向上に関する検討”, 2016 年電子情報通信学会ソサイエティ大会, 2016 年 9 月 21 日, 北海道大学（北海道札幌市）.

(3) 鈴木 壮史, 小杉 将史, 内田 理, “タッチスクリーン端末向け認証方式 SWIPASS における攻撃耐性向上に関する検討”, 画像電子学会第 44 回年次大会, 2016 年 6 月 18 日, 早稲田大学国際会議場（東京都新宿区）.

(4) 鈴木 壮史, 小杉 将史, 内田 理, 菊池 浩明, “タッチスクリーン端末向け認証方式 SWIPASS における認証成功率向上に関する検討”, 画像電子学会第 276 回研究会, 2016 年 3 月 4 日, 九州工業大学情報工学部（福岡県飯塚市）.

(5) 青木 将知, 小杉 将史, 鈴木 壮史, 内田 理, “録画攻撃への耐性を有するスワイプ型画像認証方式”, 画像電子学会第 276 回研究会, , 2016 年 3 月 4 日, 九州工業大学情報工学部（福岡県飯塚市）.

(6) 小杉 将史, 内田 理, 菊池 浩明, “SWIPASS:タッチスクリーン端末向け画像認証方式”, 画像電子学会第 272 回研究会, 2015 年 2 月 17 日, 和歌山大学システム工学部（和歌山県和歌山市）.

６．研究組織

(1)研究代表者
内田 理（UCHIDA OSAMU）
東海大学・情報理工学部・教授
研究者番号：50329306

(2)研究分担者
菊池 浩明（HIROAKI KIKUCHI）
明治大学・総合数理学部・教授
研究者番号：20266365