1W-05

複数の認証手法を用いた 視覚的なフェイク入りロック解除方式の提案

菊地　友斗† 　佐々木　槙吾† 　高橋　啓伸† 　立花　聖也† 　藤原　貴正†
小倉　加奈代‡ 　Bhed Bahadur Bista‡ 　高田　豊雄‡
岩手県立大学大学院† 　岩手県立大学‡

1. はじめに

近年，スマートフォンをはじめとするスマートデバイスの急速な普及に伴い，紛失数も増加している．スマートデバイスは電子商取引やインターネットバンキングにも用いられ，多くの個人情報や秘密情報が格納されており，紛失時の情報漏えい対策は重要である．

情報漏えい対策のひとつに Personal Identification Number（PIN）やパスワード，パターンを用いたロック解除方式がある．これらの認証方式では，複雑な PIN やパスワード，パターンを設定することで容易にセキュリティ強度を高めることができる．しかし，セキュリティ強度を高めるほどユーザの記憶負荷や操作性が問題となる．

本稿では，実際の認証方式とは異なる認証方式をフェイクとしてスマートデバイスの画面に表示することで，ユーザ負荷を増やすことなく，不正利用者によるロック解除を困難にする視覚的なフェイク入りロック解除方式を提案する．

2. 関連研究

スマートデバイスの盗難・紛失を想定した研究として遠隔ロックと遠隔削除を行うシステムが提案されている [1]．これにより，不正利用者は個人情報や秘密情報の取得が困難になる．しかし，所有者が盗難や紛失に気づくまでは，ロック解除方式が個人情報や秘密情報を守る砦となる．

また，従来の PIN やパターンを用いたロック解除方式はセキュリティ強度が低いことが問題である [2) 3)]．特に覗き見耐性を強化するために，背景画像とスマートデバイス特有の機能を用いた認証方式 [4)]が提案されている．しかし，前述のとおり，ユーザの記憶負荷や操作性の問題が残されている．

本稿では，記憶負荷や操作性の問題を解決するため，従来の認証方式を視覚的なフェイクとして利用したロック解除方式を提案する．なお，本研究と同様に，従来の認証方式をフェイクとして利用する研究は，著者らの知る限りでは存在しない．

3. 提案手法

提案手法では，PIN，Pattern，Password（フリック方式）を認証方式として採用する．それぞれの認証画面を図 1 に示す．PIN は 0～9 の数字，Pattern は 12 点を結ぶルート，Password はフリック方式でひらがな 46 文字を入力できる．

提案手法では，正規の認証方式とは異なる認証方式の画面をスマートデバイス上に視覚的なフェイクとして表示する．正規の認証方式を PIN，フェイクの認証画面を Pattern とした場合の例を図 2 に示す．この場合，表示された認証画面に従って Pattern を入力しても認証は成功しない．あらかじめ設定した PIN を入力することで認証が成功する．

正規の認証方式とフェイク画面の組み合わせは表 1 に示すように 6 通りある．なお，認証画面では PIN の番号と Pattern の点，Password 入力ボタンの位置が相互に対応する．たとえば，PIN の「1」は Pattern の左上の点と Password の「あ」の入力と対応する．

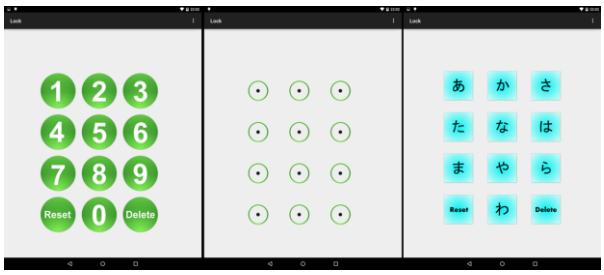


図 1. 各認証画面
（左より，PIN，Pattern，Password）

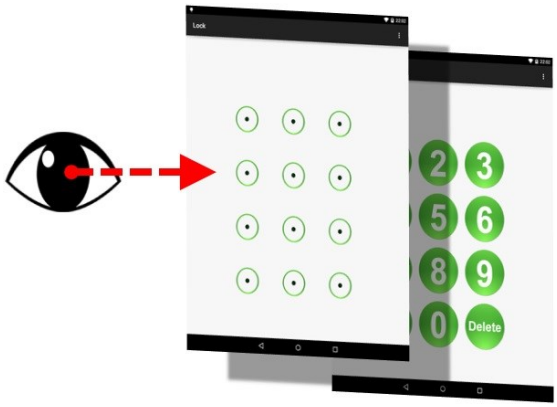


図 2. 正規の認証方式が PIN でフェイクの認証画面が Pattern の場合

表 1. 正規の認証方式とフェイク画面の組み合わせ

		正規の認証方式		
		PIN	Pattern	Password
フェイク画面	PIN	×	○	○
	Pattern	○	×	○
	Password	○	○	×

A Proposal of Unlock System Containing Visual Fake Using Multiple Authentication Methods
†Iwate Prefectural University Graduate School
‡Iwate Prefectural University

4. 評価実験

提案手法の攻撃耐性を評価するため，大学生 12 人を対象とし，正規の認証方式とフェイク画面の組み合わせ（表 1）につきそれぞれ 2 人ずつ，次節以降説明する 3 種類の攻撃実験を行った．実験は，攻撃者が「スマートデバイスを拾った」場面を想定し，認証情報は，容易に推測可能で脆弱な暗証番号，パターン，パスワードを設定した．表 2 に各実験で設定した認証情報を示す．なお，一般的なスマートデバイスは認証回数に制限があるため，本実験では試行回数を 20 回までとした．

4.1. 実験 1：攻撃者が提案手法を把握していない場合を想定した攻撃実験

実験 1 では，被験者に提案手法を伝えずにロック解除を試みてもらった．結果として，正規の認証方式が PIN でフェイク画面が Password の際に，1 名の被験者が 11 回目の試行でロック解除に成功した．攻撃が成功した理由は，設定していた暗証番号が「1234」であり，被験者は単純な入力のひとつである「あかさた」を入力したためである．フェイク画面が偽の認証画面であると気づいて攻撃した被験者はいなかった．

4.2. 実験 2：攻撃者が提案手法を把握している場合を想定した攻撃実験

実験 2 では，被験者に提案手法を説明したうえでロック解除を試みてもらった．結果として，フェイク画面が PIN で正規の認証方式が Password の組み合わせの場合に 2 名，フェイク画面が Pattern で正規の認証方式が Password の組み合わせの場合に 1 名がロック解除に成功した．実験 1 同様にいずれの被験者も脆弱な認証情報を入力して攻撃を行っていたため，ロック解除に成功したと考えられる． また，12 人中 9 人の被験者は，フェイク画面以外の 2 種類の認証方式を意識した攻撃を行っていた．

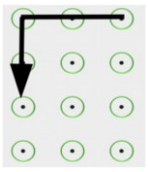
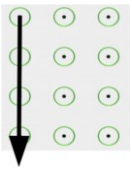
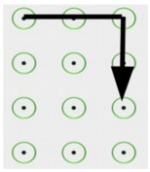
4.3. 実験 3：攻撃者が提案手法とスマートデバイス所有者の個人情報を把握している場合

実験 3 では，攻撃者が提案手法を把握しており，知人のスマートデバイスを拾得した想定の実験を行った．そのため，知人の個人情報として，住所，氏名，電話番号，誕生日，所有する車のナンバー，趣味，好きな有名人，好きな食べ物，SNS の ID 等を事前に用意し，被験者に提示した．また，ロック解除に用いる暗証番号とパスワードは提示した個人情報をもとに設定した．結果として，フェイク画面が PIN で正規の認証方式が Password の組み合わせの場合に 2 名，フェイク画面が PIN で正規の認証方式が Pattern の場合に 1 名がロック解除に成功した．12 人中 11 人の被験者は，フェイク画面以外の 2 種類の認証方式を意識した攻撃を行っていた．

5. おわりに

本稿では，複数の認証手法を用いた視覚的なフェイク入りロック解除方式を提案した．提案手法をスマートデバイス上に実装し，紛失時を想定した攻撃耐性の評価実験を行った．

表 2. 設定した暗証番号，パターン，パスワード

	実験 1	実験 2	実験 3
PIN	1234	2580	3564
Pattern			
Password	かきくけ	あいうえ	ひめかみ

結果として，実験 1 では，12 名中 1 名，実験 2 および 3 では，12 名中 3 名の被験者がロック解除に成功した．今回設定した認証情報は，いずれも容易に推測可能であったため，解除に成功した可能性が高い．今後，強度の高い認証情報を設定し，追加実験を行う予定である．

また，フェイク入りロック解除方式について，実験 1 では，提案手法に気づいて攻撃した被験者は存在せず，実験 2 および 3 では，ロック解除に成功した被験者を除いて，解除すべき認証方式に気づいた被験者はいなかった．このことから，提案手法が有効であること，提案手法が普及した場合でも，認証情報だけではなく，認証方式の特定が必要であるため，従来の単一の認証方式よりも攻撃耐性が高くなることを被験者の認証行動より確認した．

今後は，被験者数を増やし実験を行い，さらに，新たな認証方式を追加することで攻撃耐性を向上させるアプローチを検討する．

謝辞

本研究は，岩手県立大学大学院ソフトウェア情報学研究科およびソフトウェア情報学部によるプロジェクト学習（PBL2015-18）及び JSPS 科研費 26330159 の助成を受けたものである．

参考文献

1) G. Nigam，P. Singh，P. Agarwal：Smartphone Remote Lock and Wipe System，*International Journal of Electrical, Electronics and Data Communication (IJEEDC-2014)*，Vol.2，pp.89‐91（2014）．
2) E. V. Zezschwitz，P. Dunphy，A. D. Luca：Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices，*Human-Computer Interaction with Mobile Devices and Services (Mobile HCI 2013)*，pp.261‐270（2013）．
3) S. U. Uellenbeck，M. Dürmuth，C. Wolf：Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns，*ACM SIGSAC Conference on Computer and Communications Security（CCS-2013）*，pp.161‐172（2013）．
4) 益子純平：タブレット PC のマルチタッチ機能を用いた個人認証手法の提案，岩手県立大学ソフトウェア情報学部卒業論文（2012）．