5Z-2

# 携帯電話におけるインカメラを用いたパスワード入力方法の提案

小林　靖幸 †　　岡村　真吾 ‡

† 奈良工業高等専門学校 専攻科 電子情報工学専攻　　‡ 奈良工業高等専門学校 情報工学科

## 1　はじめに

携帯電話では，携帯電話の機能を所有者以外の人に利用させないようにする機能ロックの解除や Web サイトへのログインなどでパスワードを入力することがある．しかし，第三者が存在する空間でパスワードを入力せざるを得ない状況が考えられる．その際，攻撃者にパスワード入力する際の指の動きや画面をユーザの背後から覗き見られることでパスワードが盗まれ，盗まれたパスワードを攻撃者に不正利用される危険がある．また Raguram らによるとカメラの性能向上により，例えばユーザの後方 3m から携帯電話のカメラを利用してパスワード入力を録画・解析することでパスワードを取得できることが示されている [1].

そこで覗き見の対策として，携帯電話の特徴を利用することを考える．画面上にパスワード入力に必要な記号列を複数表示し，携帯電話に搭載されているインカメラを用いてユーザによる画面の注視範囲を計測することで入力された記号を推測するパスワード入力方法を提案する．

## 2　関連研究

人の眼球の動きを計測してどこを見ているか推定する視線計測装置が存在する．視線計測装置を用いたパスワード入力方式として Kumar らの研究がある [2]．しかし携帯電話に視線計測装置を装着するのは，コスト面から困難である．また，視線計測装置で行なっていた計測をビデオカメラに代用させる研究 [3] もされている．それらの結果と予備調査から，携帯電話の画面を 4 つの範囲に分け，インカメラによってそれぞれの範囲を注視していることを特定できる知見が得られている．

数種類の選択肢からの選択を繰り返すことでパスワードを入力する手法として，北林らの手法がある [4]．この手法では，0 から 9 までの 10 個の数字から重複がないように 8 個選び，それを画面の左右に 4 桁の数字列に分けて配置する．ユーザには入力したい暗証番号が含まれている 4 桁の数字列を選択させ，すべての選択が正しければ正しい入力がされたと判断する．覗き見への対策として，選ばれた 8 個の中に入力したい暗証番号が含まれていない際に，偽の入力行為をすることで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，攻撃者が選択をランダムに行ったときに認証が成功する確率はパスワード長を $n$ とすると $\frac{1}{2^n}$ となる．

## 3　提案方式

インカメラを搭載した携帯電話において画面注視を用いたパスワード入力方法を提案する．図 1 のように携帯電話の画面を 5 つの範囲に分ける．画面上部の領域 $P_1$ を 4 つの範囲に区切り，各範囲内に記号列 $m_1$ から $m_4$ を 1 つずつ表示する．画面下部の領域 $P_2$ には記号列 $r$ を表示する．ユーザは 2 組の情報を記憶しておく．1 つ目は，パスワード $a$ と数字列 $b$ である．$b$ は $a$ と同じ長さであり，$a$ の各記号について記号列 $m_1$ から $m_4$ のいずれか 1 つにおける左からの位置を示している．2 つ目は 1 つ目のパスワードが入力できない際に使用するパスワード $d$ と左か右という情報を示した $\epsilon$ であり，ランダムなキー入力によって認証が成功する確率を下げるために設定する．入力システムは，インカメラによって画面の注視を上下左右の 4 箇所の範囲で区別できるものとして考える．

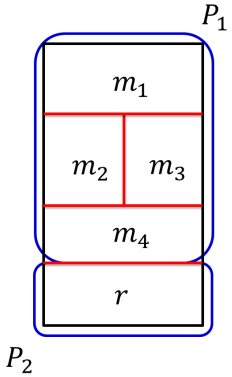


図 1　提案手法での携帯電話の画面

---

A password input method on mobile phones with front-facing cameras
†Yasuyuki KOBAYASHI,
Advanced Electronic and Information Engineering Course, Nara National College of Technology
†Shingo OKAMURA,
Information Engineering, Nara National College of Technology

$a$ の $i$ 番目の記号を $\alpha_i$，$b$ の $i$ 番目の数字を $\beta_i$ とする．また，$P_1$ 内の $m_1$ から $m_4$ と $r$ は $\alpha_i$ を入力するために $l$ 回変化する．変化のタイミングは $m_1$ から $m_4$ のうちいずれかの記号列に瞳を向けられたときである．$l$ 回の変化のうち少なくともある回の記号列 $m_1$ から $m_4$ には左から $\beta_i$ 番目の記号が $\alpha_i$ である記号列が存在する．また，同じ画面に表示されている記号列 $m_1$ から $m_4$ において，左から $\beta_i$ 番目の記号が $\alpha_i$ である記号列は高々 1 つ存在する．

入力方法を示す．まずユーザは携帯電話のキーボードから 0 から 9 の数字のいずれか 1 つを攻撃者に知られないように入力し，これを $\gamma$ とする．ユーザが $\alpha_i$ を入力したい場合，$P_1$ 内に左から $\beta_i$ 番目の記号が $\alpha_i$ である記号列が存在すれば，瞳をその記号列の方向に向ける．$P_1$ の中に選択できる入力記号が存在しない場合，図 1 に示す表示領域 $P_2$ 内に表示されている記号列 $r$ の中に，$d$ の $j$ 番目の記号 $\delta_j$ が含まれている．記憶している情報 $\epsilon$ と最初に入力した数字 $\gamma$ から，$\delta_j$ の左または右 $\gamma$ 番目にある記号を入力記号 $\zeta$ として，$P_1$ 内の $m_1$ から $m_4$ のうち $\zeta$ を含む記号列に瞳を向ける．これを $l$ 回行うと $\alpha_i$ の入力が終わり，次の記号 $\alpha_{i+1}$ の入力に移る．

## 4 評価と考察

記号の定義を以下の通りとする．

- $\boldsymbol{C}$: パスワードに利用できる記号集合
- $m, r$: $\boldsymbol{C}$ から生成される固定長記号列
- $(a, b) = (\alpha_1 \cdots \alpha_n, \beta_1 \cdots \beta_n)$: 1 つ目のパスワード $\left(n$: パスワード長$, \alpha_i \in \boldsymbol{C}, 1 \leq \beta_i \leq |m|\right)$
- $(d, \epsilon) = (\delta_1 \cdots \delta_o, \epsilon)$: 2 つ目のパスワード $\left(o$: パスワード長$, \delta_j \in \boldsymbol{C}, \epsilon \in \{$ 左, 右 $\}\right)$
- $\gamma$: キーボードから入力した 1 から 9 の数字のいずれか 1 つ
- $l$: $\alpha_i$ を入力するために表示される $P_1$ 内の $m_1$ から $m_4$ の変化数 ($\alpha_i$ 当たりの入力試行回数)

$\alpha_i$ の入力行為を 1 回覗き見した攻撃者が，$\alpha_i$ と $\beta_i$ を特定できる確率の最小値は，$l$ が攻撃者に既知だとすると，$4l \leq |\boldsymbol{C}|$ のとき $\frac{1}{4|m|l}$ となる．しかし同じ画面に表示されている記号列 $m_1$ から $m_4$ において，左から数えて同じ位置に同じ記号を含む記号列が複数存在した場合，その記号と位置の組はユーザが入力したものではない．そのため，その組は正しい記号と位置の組み合わせの候補から除外することができる．よって，記号と位置を特定できる確率は $\frac{1}{4|m|l}$ 以上になる．そのため，1 つの画面に表示する $m_1$ から $m_4$ を縦に 4 つ並べ，されにこれらを各画面について縦に $l$ 個並べた際に，各列は記号の重複ないように記号列 $m_1$ から $m_4$ を生成することで理論値 $\frac{1}{4|m|l}$ に近づけられる．

また，攻撃者がランダムにキー入力を行う攻撃をした際に認証が成功する最小の確率は，$\frac{1}{4^{nl}}$ となる．北林らの手法 [4] で 4 つの範囲を設定した場合 $\frac{1}{4^n}$ となるため，ランダム攻撃に関しても提案手法の方が耐性が高いことが示せる．しかし，パスワード長によっては暗証番号を入力する方式におけるランダム攻撃が成功する確率より高くなる可能性がある．

## 5 まとめ

本研究では，携帯電話におけるパスワード入力に対して覗き見攻撃されても安全性を確保できる入力方法を検討した．本手法では，従来研究で用いられた偽の入力行為を含めることにより覗き見攻撃に対する耐性を向上させることに加えて，ユーザにパスワードと各記号の位置の組を記憶させ，入力時に入力したい記号が決められた位置にある記号列を選択させることで，正しいパスワードが入力されたものと判断する手法を提案した．

## 参考文献


[1] R. Raguram, A.M. White, D. Goswami, F. Monrose, and J. Frahm. ispy: automatic reconstruction of typed input from compromising reflections. In *Proc. 18th ACM conference on Computer and communications security*, pp. 527–536, Oct. 2011.

[2] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proc. 3rd symposium on Usable privacy and security*, pp. 13–19, Jul. 2007.

[3] J. San Agustin, H. Skovsgaard, E. Mollenbach, M. Barret, M. Tall, D. W. Hansen, and J. P. Hansen. Evaluation of a low-cost open-source gaze tracker. In *Proc. the 2010 Symposium on Eye-Tracking Research & 38; Applications*, ETRA '10, pp. 77–80, 2010.

[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, Vol. 109, No. 115, pp. 21–26, Jun. 2009.