Computer Security Symposium 2014
22 - 24 October 2014

背景色と偽入力を用いた覗き見耐性を持つパスワード認証方式の提案

杉本 洋介 †　　稲葉 宏幸 ‡

† 京都工芸繊維大学 大学院工芸科学研究科 情報工学専攻
〒 606-8585 京都府京都市左京区松ケ崎橋上町
sugimoto09@sec.is.kit.ac.jp†, inaba@kit.ac.jp ‡

あらまし　携帯端末や ATM で利用される個人認証には、暗証番号やパスワードを用いたものが最も利用されている。しかし、既存の認証方式では, 認証動作の覗き見や録画攻撃への耐性がほとんどないものが多く、認証情報が他人に知られてしまう危険性がある。既存のパスワードによるチャレンジレスポンス型の認証方式として、文字の背後に色の配列を表示した認証画面に対して、利用者がパスワードを基に背景配列を移動させることで認証を行うものがある。本論文ではこの方式に改良を加え、入力に本来のパスワードとは無関係の偽入力を混じえ、利用者が使用する色を指示することで、覗き見に対する安全性を高めた認証方式を提案し、その安全性の評価を行う。

Proposal on Password Authentication Using Fake Input Sequence and Background Color Array Against Iterative Shoulder Surfing

Yosuke Sugimoto†　　Hiroyuki INABA‡

†Kyoto Institute of Technology　Matsugasaki, Sakyo-ku, Kyotoshi, Kyoto, 606-8585 Japan.
sugimoto09@sec.is.kit.ac.jp†, inaba@kit.ac.jp ‡

Abstract　Password authentication is widely used in various IT systems like cell phones, ATM, etc. However,it has a weakness for shoulder surfing at input operation. A conventional method that displays an array of colors or figure behind characters does not have tolerance for iterative shoulder surfing. In order to improve this method, we introduce an unrelated input sequence and specify color chart for user's choice. We show that the proposed method is better in the tolerance for iterative shoulder surfing than a conventional method.

1　はじめに

現在，最も一般的な個人認証方式として普及しているものとして，パスワードや暗証番号による認証方式がある．この方式は，あらかじめ利用者が決めておいたパスワードをシステムに伝えておき，認証を必要とする際にシステムが利用者にパスワードが何であったかを確認するものである．この方式は，パスワード認証を行う二者の間で秘密に行われ，第三者はそのパスワードを知り得ないという前提の下に成立する．しかし，利用者がシステムにパスワードを伝えるという作業が必ず行われるわけであるから，パスワードが第三者に漏洩する危険性が存在する．この入力動作は目に見える形で行われることが多く，第三者が目視することが可能である．第三者が攻撃者であった場合，故意に入力動作を覗き見ようとすることが考えられる．この時，

パスワードを直接入力する方式では，攻撃者は容易にパスワードを特定することができる．実際に銀行 ATM に隠しカメラが設置され，盗撮されるという事件が発生している．利用者側でできる対策として，覗き見されないように注意を払ったり，パスワードの文字数を多くするなどの対策が挙げられるが，利用者の負担も増大してしまう．また一度の覗き見で正確に特定されなかったとしても，複数回にわたって入力を覗き見られるとパスワードを特定されてしまう可能性は高くなる．このため現在，覗き見攻撃を考慮した様々な認証手法が提案されている [1][2] が，複数回の覗き見に対する安全性への対処が十分でないことも多い．したがって本論文では，認証行為を複数回覗き見られれても一定の安全性を確保可能にする認証手法を提案し，その安全性評価を行った．

2　既存手法の概要

2.1　背景配列の移動量を用いたパスワード認証方式

パスワードによるチャレンジレスポンス型の認証方式の既存手法として，背景に異なる色や図形の配列（背景配列と呼ぶ）を表示し，背景配列を動かすことで認証を行うものがある．[2] この方式の認証画面は上部のパスワード選択部と，下部の確定表示部から構成される．パスワード選択部は文字配列と背景配列で構成され，パスワードの選択に使用される．文字配列はパスワードに使用できる文字を要素とする二次元配列である．背景配列は個々の文字の背景として使用される図形と色を要素とする二次元配列である．背景配列には同じ背景が均等に含まれている．認証画面に対しての操作には上下左右の方向キーと入力キーおよびクリアキーの計 6 つがある．上下左右いずれかの方向キーを押すと，背景配列の要素だけが押されたキーの方向に移動する．この時，例えば上方向キーを押して背景配列の要素を上に移動させると最上段にあった要素が最下段に移動する．入力キーを押すと，その時点での背景と文字の要素の対応を確定し，確定表示部に”＊”が 1 つ追加される．また，この時同時に背景配列がランダムに移動する．所定の回数だけ確定された後に，認証を行う．認証では，パスワードの各文字について順に，背景を全て同じ種類の背景に合わせることができていれば利用者がパスワードを正しく記憶している正規の利用者であると判定する．使用する背景の種類は利用者がパスワードの最初の文字の背景を合わせる際に任意に選択してよい．したがって，使用する背景の種類は予め決めて覚えておく必要がなく，認証の度に変えることができる．さらに，パスワードを細かなフレーズに分割し，それぞれのフレーズの中で背景を統一することで，パスワード全体では複数の背景を使用し，よりパスワードを特定されにくくする方式も提案されている．

2.2　既存手法の認証手順

既存手法の入力手順を以下に示す．まず利用者は事前にシステム側にパスワードを伝えておく．仮にここでは，パスワードを $(W_0,W_1,\cdots,W_N-1$ として説明する．

Step1 i=0 とする　認証に用いる背景を決定する

Step2 背景色をランダムに配置する

Step3 W_i の背景色が認証に用いる色になるように背景色の配列を動かし，Step4 へ

Step4 入力ボタンを押して背景色と文字の対応を確定させる　Step5 へ

Step5 i=i+1 とする．
$i < N$ ならば Step2 へ
i=N ならば終了し，認証を行う

3　提案手法

本研究では，前述した”背景配列の移動量を用いたパスワード認証方式”を改良し，覗き見攻撃に対する耐性を高めた認証方式の提案を行う．提案手法では，2 つの改良点を設ける．まず 1 つ目に，本来のパスワードに必要な入力（真入

力と呼ぶ）と関係のない偽の入力（偽入力と呼ぶ）を挿入する．偽入力を導入するにあたって重要な点は，どのような手段で利用者側とシステム側が偽入力のタイミングを共有するかという点である．提案方式では，利用者はパスワードを決定する時に，偽入力のタイミングを共有するための 1 つの色 (偽入力判別色と呼ぶ) を予め決定しておく． 2.2 節の Step2 において，背景の色がランダムに入れ替わった時に，偽入力判別色が次に入力したいパスワードの文字の背景として表示されていた場合，その入力を偽入力と判断する．その時利用者は，背景を任意に動かして入力すればよいものとする．次に，2 つ目の改良点は，利用者が使用する色の系列を表示することである．既存手法では利用者が認証開始時に認証に用いる色を任意に選択するが，その後の入力では同じ色を使用する必要がある．提案手法では，図 1 における右上のように色の配列 (系列配列と呼ぶ) が表示されており，そこから 1 マスを選択しそのマスに表示されている色を認証に用いる．系列配列は 2.2 節の Step2 において，背景配列と同様にランダムに色の再配置が行われるが，利用者は次の文字を入力する際にも先ほどと同じマスに表示されている色を最後まで用いる．図 1 の上段の画面が 1 文字目の入力であったとすると，利用者は右側にある 16 マスから好きなマスを選択し，その色を使用する．例えば一番左上の青色を選択した場合，次の 2 文字目の入力もその一番左上のマスに表示された黄緑色を入力に使用する．

4　提案手法の安全性評価

4.1　評価シミュレーション

安全性を評価するにあたって，パスワードの入力と覗き見に関する計算機シミュレーションを行った．シミュレーションにおける条件を以下のように設定する．

1. 文字種
   0 から 9 の数字 10 種，A から Z のアルファベット 26 種，記号 4 種の合計 40 種
2. 文字数
   5 文字，6 文字
3. 系列配列
   0 マス，16 マス，32 マスの 3 通り
4. 偽入力
   0 箇所　 2 箇所の 2 通り

文字数，系列配列，偽入力のそれぞれの組み合わせによる 12 通りの条件においてシミュレーションを行った．

4.2　ランダム入力攻撃に対する安全性

パスワードについての情報を何も得ていない攻撃者がランダムに入力を行った場合に認証が成功してしまう確率を求める．例えば 10 進数の暗証番号 M 桁では

$$P = \frac{1}{10^M} \tag{1}$$

である．既存手法においては，最初の入力でパスワードの 1 文字目の背景色となった色と残りの文字の背景の色が全て一致する必要がある．また，提案手法においては，パスワードの 1 文字目の背景色となった色が系列配列のマスにあった場合，それ以降同じマスの色を使用する必要がある．ここで，使用する色の種類数を b，同じ色が 1 画面に表示される数を c，パスワードの文字数を λ とすると，ランダム入力攻撃が成功する確率は

$$P = \frac{1}{b^{\lambda-1}} \tag{2}$$

である．これは偽入力，系列配列の数によって一切変化しないものである．パスワードが 5 文字の場合は 10 色以上，6 文字の場合は 7 色以上を表示することで同じ長さの PIN と同等のランダム入力攻撃への耐性が得られる．

5　覗き見に対する安全性

5.1　1 回の覗き見に対する安全性

偽入力を用いない場合，1 回の覗き見によって攻撃者が想定するパスワード候補の数は以下

のように求めることができる．系列配列のサイズを N とするとパスワード候補の総数 S は

$$S = N \times b \times c^{\lambda} \tag{3}$$

となる．
偽入力を用いた場合，攻撃者はどこが偽入力の箇所なのかを想定する必要がある．シミュレーションのの条件では，5+2 回，もしくは 6+2 回の入力から偽入力の箇所を想定して同様の計算を行うことになる．したがって偽入力がある場合に 1 回覗き見た攻撃者が想定するパスワード候補数 S は，偽入力の数を d とすると最大で

$$S = \begin{pmatrix} \lambda + d \\ d \end{pmatrix} \times b \times c^{\lambda} \tag{4}$$

と見積もることが出来る．
式 (4) で示されるパスワード候補の中には一般に同じものが含まれるので，真の S の値は式 (4) よりも小さくなる．

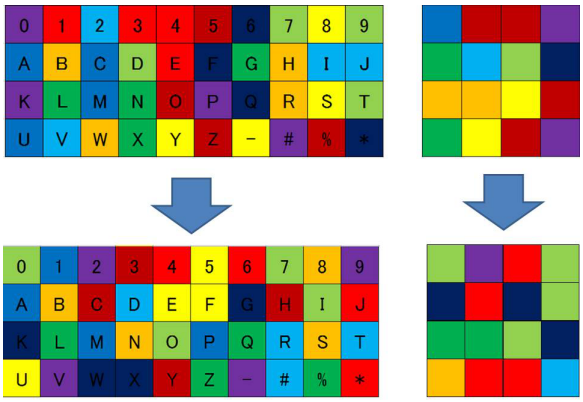

図 1: 色の系列表示を含めた認証画面

5.2 複数回の覗き見に対する安全性

複数回の覗き見に対する安全性を評価するために，シミュレーションでは 4.1 節の各条件のもと，で同じパスワードについて 5 回の認証動作を行い，それらの認証動作を覗き見されたという仮定で推測されるパスワード候補を求める．このパスワード候補の数は覗き見回数 (1〜5 回) が増加すると減少することが明らかである．ここで，パスワードの候補数 S を情報量 I で表すために

$$I = log_2 S \tag{5}$$

と定義する．一般に，銀行 ATM などのシステムでは暗証番号の入力を 3 回間違えるとシステムが利用できなくなるものが多い．つまり，このようなシステムでは，覗き見後の情報量が 2(bit) を下回った時点で認証システムが破られると考えることができる．
図 2 にパスワード長が 6 文字の場合の各手法の複数回の覗き見による情報量の推移を示す．図中の 6 本のグラフを比較すると，情報量の低下が小さいものと大きいものには明らかな隔たりがあることがわかる．下側の 3 本のグラフは

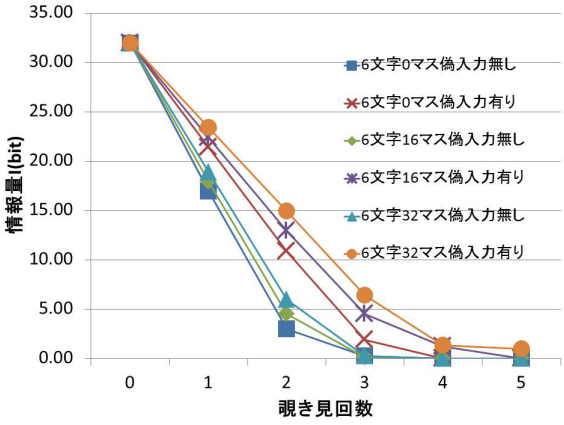

図 2: 複数回の覗き見に対する安全性

系列配列のサイズこそ違うものの，偽入力を用いていないものであり，安全性を向上させるためには系列配列よりも偽入力の効果が大きいことが見て取れる．また，覗き見に耐えうる回数については，2 回までは全ての条件で 2bit 以上の情報量を持ち，覗き見への耐性を有している．しかし，3 回以降は耐性を有しているのは「系列配列 32 マス，偽入力有り」,「系列配列 16 マス，偽入力有り」の 2 つの条件のみであった．

6　まとめと今後の課題

パスワード，暗証番号による認証方式は銀行 ATM やコンピュータ端末，さらに近年では急速に普及の進む，スマートフォン，タブレット端末において個人を認証する方式として，導入の容易さや利用者の利便性から広く用いられている．しかし，パスワード認証方式は入力操作時の覗き見や盗撮に対して脆弱であるという欠点があり，実際に隠しカメラを用いた情報漏洩の事件も発生している．そこで本論文では，パスワードの入力に本来の入力とは無関係な偽の入力を含ませ，さらに利用者が使用する色を系列配列によって指示することにより，複数回の覗き見への耐性を強化した認証方式を提案した．提案手法では，3 回までの覗き見に耐性を持つことを示したが，使用状況の画面サイズに応じて系列配列のサイズを変更すればより安全性を高めることができると考えられる．また，偽入力は安全性の向上において高い効果を示したが，入力回数の増加という点もあり，利用者の利便性とトレードオフの関係にあることを留意し，今後被験者による入力実験を実施したいと考えている．

参考文献

[1] V. Roth, K. Richer, and R. Freidinger,“A pin-entry method resilient against shoulder surfing,”In Proc. of 11th ACM Conference on Computer and Communication Security, pp.236-245, 2004.

[2] 櫻井鐘治，撫中達司,“背景配列の移動寮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.