**SCIS 2007** The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

# fakePointer 2: 個人認証における覗き見攻撃への安全性を向上させるユーザインタフェースの提案

# fakePointer 2: A Proposal of User Interface for 4-digit PIN authentication to make shoulder surfing attack hard

高田哲司 *
Tetsuji TAKADA

**あらまし** 本論文では，個人認証における覗き見攻撃に対する改善策として，fakePointer を提案する．銀行 ATM を代表とする暗証番号認証において覗き見攻撃が成立してしまう原因は，秘密情報を直接選択させるユーザインタフェースにあると言える．そこで我々は，二層式の表示による画面を提案する．この画面では，上層に数字キーが表示され，下層には図形群が数字キーの背景となるように表示される．ユーザは，事前に指定される特定の図形を入力したい数字キーの背景になるように操作することで回答を行う．これにより，攻撃者が認証行為を覗き見ていても秘密情報の特定を困難にするともに，Challenge and Response の仕組みを応用し，回答に使用する図形を認証のたびに変化させることで，仮に認証行為をビデオ撮影されたとしても一定の安全性を担保可能にするインタフェースを実現した．

**キーワード** 個人認証，ユーザインタフェース，覗き見攻撃，チャレンジアンドレスポンス

## 1 はじめに

個人認証における脅威の一つとして，覗き見攻撃[1] がある．これは認証行為を第三者に覗き見られることにより，秘密情報 (パスワードや暗証番号など) が第三者に奪取されるという攻撃である．日本では 2005 年末から 2006 年初頭にかけて銀行 ATM にビデオカメラを設置し，暗証番号を盗もうとする盗撮事件が発生したことも記憶に新しい．

この攻撃手法に対する基本的な対策は，認証行為を第三者に覗かれない環境で行うことであるが，その実現は現実的に困難であると言わざるをえない．またユビキタス環境の普及にともない，他人の目のある環境下で認証を行わなければならない状況も今後起こりうると推測する．これらの状況を考慮すると,「覗かれないようにする」という方針に基づく既存の対策方法だけでは不十分であると考える．

そこで本論文では，他人に覗き見られても，それが即座に秘密情報の漏洩につながらないような個人認証のためのユーザインタフェースとして “fakePointer” を提案する．fakePointer は，認証を行っているユーザが回答として何を入力したのかを一見しただけでは半別不能にするとともに，Challenge and Response の仕組みを応用し，回答方法を毎回変更することによって，認証行為がビデオ撮影されたとしても，その記録から秘密情報が即座に特定されない仕組みを提供する．

以降，本論文では既存の銀行 ATM で使用されている四桁数字による暗証番号認証を対象とし，覗き見攻撃に関する関連研究を挙げ，その問題点を明らかにするとともに，fakePointer の仕組みとその安全性および利便性に関する考察を述べる．

## 2 覗き見攻撃に対する既存の対策とその問題点

覗き見攻撃に対する対策手法はいくつか提案されている．本章では，既存の対策手法とその問題点について整理する．既存の対策手法は,「第三者による認証行為の覗き見を困難にする」手法と,「覗き見を想定し，見られても秘密情報の特定を困難にする」手法の二種類がある．そのそれぞれについて述べていく．

### 2.1 覗き見を困難にする手法

1. 遮蔽板: 覗き見攻撃に対する物理的な防御方法として，覗き見を困難にするための遮蔽板を設置する方法である．トマト銀行では，銀行 ATM に「盗

* 産業技術総合研究所, 東京都千代田区外神田 1-18-13 秋葉原ダイビル 10F, Advanced Industrial Science and Technology, Dai bldg 10F, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo, JAPAN (zetaka @ computer . org)

[1] Shoulder surfing, Shoulder hacking, Observation attack とも呼ばれる

撮防止カバー」を設置し，第三者による認証画面の覗き見を困難にしている [7]．また遮蔽板の応用として，正規ユーザのみが操作画面を見られるようにする遮蔽箱 [8] といった技術も存在する．

2. 視野角制御機能付き液晶パネル: 液晶パネルの視野角を制御することによって第三者による覗き見を困難にする技術であり，携帯電話ではすでに実用化されている．著名な技術としては，シャープ社の VeilView 液晶 [11] がある．

3. プライバシーフィルタ: 液晶パネルに貼り付けるフィルタで，液晶パネル同様，視野角を制御することにより覗き見を困難にする．

これらの対策手法における問題点は，認証を行う全ての機器への対応が困難であることと，これらの対策を施しても，覗き見攻撃の脅威を完全には排除できないことである．

### 2.2 覗き見を前提に，秘密情報の特定を困難にする技術

第三者に認証行為を覗き見られたとしても，それによって秘密情報が即座に特定されないようにする技術は，大きく 2 つあると考える．本節では，そのそれぞれについて述べる．

まず 1 つめの枠組みは，部分的に覗かれる可能性を想定した対策手法である．この想定に基づく代表的な対策技術は，数字キーの配列をランダムにする方法である．また暗証番号入力用の画面を拡張し，10 x 5 のキー配列の中の任意の位置に 3 x 4 のテンキーを配列することで，入力行為の覗き見による暗証番号の推測を困難にする手法 [9] や，各数字キーを複数組用意する手法 [10] なども提案されている．

もう 1 つの枠組みは，認証行為が人間によって覗き見られることを想定した対策手法である．この想定では，通常の人間が持ちうる能力において覗き見をしたとしても秘密情報の特定を困難にすることであり，攻撃者が秘密情報を特定するために必要な情報量を増やしたり手順を複雑にすることで，その攻撃達成を困難にする手法である．

Volker ら [3] は，テンキーの背景に白黒の色をつけ，入力したい数値の背景色を 4 回回答させることで覗き見攻撃を困難にしている．つまり図 1 の場合，数字の 3 を入力するためには画面の状況に応じて「白，黒，白，黒」と回答することになる．しかし 1 つの数字を入力するのに 4 回回答する必要があり，操作時の手間は増えることになる．

Desney ら [2] は，公共の場にあるディスプレイを使用して認証を行うことを想定し，その環境下で認証行為を第三者に覗き見られてもパスワードが特定されないようする手法として，特殊なキーボードによる入力方法を提

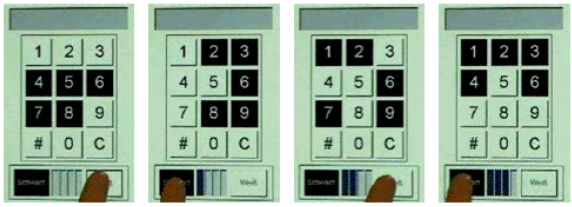

図 1: Volker らによる PIN Entry Method

案している．各キーには 3 種類の文字が表示されており，シフトキーを使ってその 3 種類のうちのどのキーを入力するかを決定した上で，選択シンボルを該当するキーへドラッグすることで一つの文字を入力する．選択シンボルをドラッグし始めると，キートップに表示されていた文字が消えるようになっており，結果として第三者が認証行為を見ていたとしても入力した文字の特定を困難にしている．

また画像認証の分野では，その認証手法に特化した覗き見対策手法がいくつか提案されている．

原田ら [4] は，画像記憶のスキーマを利用し，画像をモザイク処理化することで，認証行為を覗き見られても秘密情報の特定を困難にする手法を提案している．

L.Sobrado ら [6] が提案している手法は，画面内にアイコンがランダムに配置されている状況で，ユーザが事前に決定しておいた 3 つのアイコンによって囲まれている領域にあるアイコンを複数回選択させることで認証を行う手法である (図 2)．この手法は，ユーザの秘密情報を直接選択しないので，その特定が困難になっている．

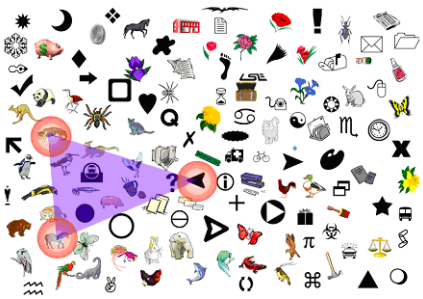

図 2: L.Sobrado らによる囲い込み回答法

これらの対策手法の問題点は，現実に発生しているビデオ撮影による覗き見攻撃の脅威に対応できない点である．前述したが，覗き見攻撃は人間が行うだけでなく，ビデオ撮影によって行われるようになってきている．また Desney ら [2] が想定するように，公共の場にあるディスプレイを使用するような状況であれば，第三者が認証行為をビデオで撮影していても不思議ではないだろう．

既存の研究では，Volker ら [3] が認証行為をビデオで撮影されることを想定した場合の対策を提案している．

その方法とは，Volker らの認証方法では，1 つの数字を入力する際に 4 回の回答を必要とするが，その 4 回の回答で特定される数値を 1 つから 2 つになるようにすることである．つまり，仮に攻撃者がビデオ撮影のデータを元に解析しても，2 個の数字の組が 4 桁分揃うことになり，結果として 16 個 ($=2^4$) の暗証番号候補が攻撃者の手に渡ることになる．したがって認証行為をビデオ撮影されたとしても，それにより即座に秘密情報が特定されることにはならないというものである．しかし，この方法でも攻撃者に渡る暗証番号候補の数は十分多いとは言えず，その安全性に疑問が残るといわざるを得ない．

よって本論文では，暗証番号認証において認証行為をビデオで撮影されたとしても一定の安全性を保証しうる手法として “fakePointer” を提案する．次章では，fakePointer の仕組みと認証方法について述べる．

## 3 fakePointer

### 3.1 基本コンセプト

なぜ個人認証において覗き見攻撃が成立してしまうのか? 我々は，その原因はユーザインタフェースにあると考える．秘密情報が攻撃者に知られてしまう理由は，個人認証におけるユーザインタフェースがユーザに正解を直接指し示すことを強制しているからである．

したがって，ユーザが秘密情報を直接選択しなくても秘密情報を入力可能にするインタフェースが実現できれば，この脅威に対する対策になると考える．そこで我々は，二層の表示からなる回答インタフェースを提案する．図 3 は，fakePointer の画面例である．


図 3: fakePointer の回答画面例

この画面は二層構造になっている．上の層は数字キーが表示されており，その配置はテンキーと同様で固定である．下の層は，各数字の背景として 10 種類の図形がランダムに表示される．この図形群の各数字キーへの割り当ては，回答入力のたびにランダムに行われる．またこの割り当ては，ユーザのキー操作により変更可能になっており，現在の実装では，左右の矢印キーが割り当てられている．

このインタフェースにおける回答方法は，入力したい数値キーの背景に，事前に指定された図形が描画されるよう背景の図形群の配置をキー操作で変更し，決定キーを押すことで行う．つまり，入力したい数値キーを特定の図形で選択するという仕組みである．この数値を指定するための図形を，選択図形と呼ぶことにする．例を挙げて説明すると，図 3 の状態は，選択図形が白い円で，ユーザが入力したい数値が “3” である場合の回答例となる．この回答方法により，攻撃者は数値キーを指定する選択図形を知らない限り，この画面を覗き見ただけではどの数字が回答として入力されたが不明となり，覗き見攻撃が困難になるという仕組みである．

しかし，これだけでは認証行為をビデオ撮影された場合に対する安全性が確保できない．理由は簡単である．ビデオによる記録があれば，各選択図形が選択した数値をたどることで，10 個の暗証番号候補が特定可能だからである (図 4).

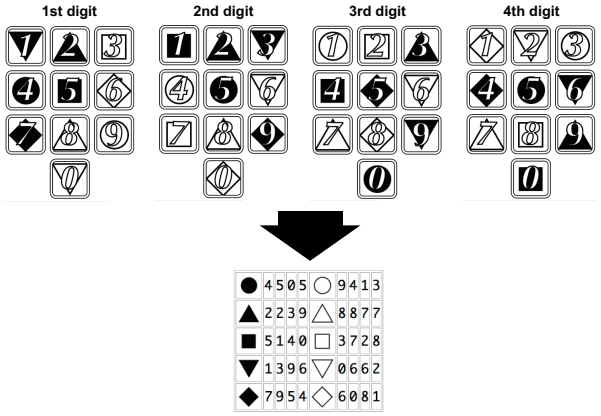


図 4: ビデオ撮影による秘密情報の特定

これでは現実に存在する脅威に対して安全性が確保されているとは言えない．よって攻撃者が認証行為のビデオを手にしたとしても，秘密情報が容易に特定されないような工夫が必要である．

図 4 が意味することは，仮に秘密情報の入力方法が間接的になったとしても，その入力方法が固定されているならば，それは覗き見攻撃への対策にはならないということである．つまり回答方法が一定ならば，入力方法が間接的であっても，認証行為のビデオから秘密情報を特定しうるということであり，その対策としては，回答選択方法を可変化する必要がある．

そこで我々は，回答方法に Challenge and Response

を導入することにより，この問題に対応する．この回答方法の説明も含めた fakePointer の認証方法については次節で説明する．

### 3.2 認証方法

fakePointer における認証方法を説明する．まず認証を行う前提として，ユーザは 4 桁の暗証番号を事前に決定し，記憶しているものとする．この状況において，fakePointer による認証を行おうとする者は，認証を行う前に選択図形に関する Challenge を取得しなければならない．図 5 は，チャレンジの一例である．

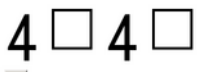


図 5: 選択図形を示すチャレンジの例

このチャレンジは，4 桁の暗証番号を入力するのに必要な選択図形に関する情報を与えている．チャレンジは，1 つの図形と 1 つの数字から構成される．この解釈方法を説明する．暗証番号の 2 桁目と 4 桁目の選択図形は白い四角形であり，選択図形を直接指定している．つまりユーザは，白い四角形を 2 桁目と 4 桁目の選択時に各暗証番号の背景に白い四角形が描画されるように背景図形を操作して回答を行う．図 6 は，選択図形が白四角形である場合に 1 を入力している回答例である．

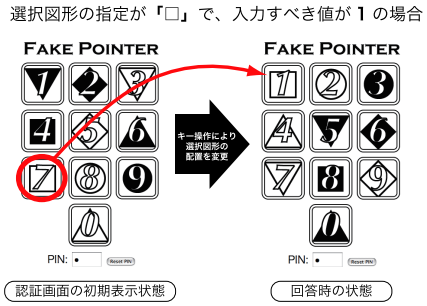


図 6: 選択図形の指定が図形だった場合の回答法

問題は 1 桁目と 3 桁目の選択図形が数字で指定されている点である．これは間接的に選択図形を指示しており，この数字から選択図形を得るのに認証画面を利用する．詳細を図 7 を用いて説明する．

Challenge 内の数字から選択図形を得るには，認証画面の初期状態を利用する．図 7 の左の認証画面は，1 桁目の回答をするためにシステムがユーザに提示した認証画面の初期状態，すなわちユーザが操作をする前の状態である．Challenge 内の 4 という数値は，この画面内の数字キー “4” を意味し，認証画面の初期状態で指定の数字キーの背景になっている図形を選択図形として使

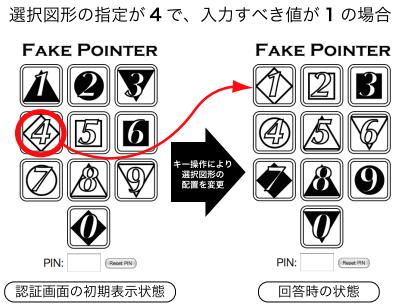


図 7: 選択図形の指定が数字だった場合の回答法

用することを意味している．したがって図 7 の例では，Challenge の 1 桁目の値が 4 なので「白のダイヤ」が選択図形になる．よって 1 桁目の暗証番号を 1 とした場合，ユーザは選択図形の配置を変更し，図 7 右の状態にした上で決定キーを押すことで回答を行う．

このようにして，回答を指示する選択図形は Challenge により指示される．この Challenge によって一意に決定される選択図形を使用し，ユーザは 4 桁の数字を入力する．入力された数字が，ユーザの事前に決定していた暗証番号と一致すればその認証は成功となる．

選択図形を示す Challenge はランダムに生成される．したがって，暗証番号のどの桁の回答に使用する選択図形が図形による直接指定になり，また数値による間接指定になるかもランダムである．また，どの図形や数値が指定されるかもランダムとなる．それゆえ，Challenge の内容は認証の毎に毎回異なるものになる．またこの Challenge は一回の認証でのみ有効であり，ユーザは認証を行うたびに Challenge を取得するものとする．

これらの仕組みにより，攻撃者が認証行為のビデオ記録を取得したとしても，その認証に使われた選択図形の Challenge と認証行為の双方が揃わない限り，秘密情報の特定は困難になる．

## 4 考察

本章では，fakePointer の安全性と利便性について述べる．

### 4.1 安全性

fakePointer における安全性について考察する．まず想定される攻撃に対する安全性について述べる．

1. Brute-force 攻撃
   本手法における Brute-force 攻撃の安全性は 1/10000 であり，既存の四桁数字による暗証番号認証と同等の安全性である．

2. 人間による覗き見攻撃
   人間による覗き見攻撃とは，処理能力と記憶能力

に制約がある場合を指す．fakePointer の場合，暗証番号を特定するためには各照合画面の最初と最後の状態を記憶する必要があるが，大多数の人はこれを実行できないと推測する．また仮にすべての状態を記憶できたとしても，fakePointer はビデオ撮影を想定した安全性を確保しているので問題はない．安全性の詳細については，次の「ビデオ撮影による覗き見攻撃」で述べる．

3. ビデオ撮影による覗き見攻撃
   ビデオ撮影による覗き見攻撃とは，処理能力と記憶能力に制約がない場合を指す．この場合，認証行為を撮影したビデオから Challenge の情報なしに秘密情報の特定が可能かという問題に帰着する．選択方法に関して既知であることは，4 回の回答のうち 2 回は同一の図形で，残りの 2 回は同一数字キーの背景になっていた図形により数値を選択しているということである．よって，この条件において攻撃者が得ることのできる秘密情報の候補数は以下の式より 600 個となる (図 8).

$$\underbrace{6\,({}_4C_2)}_{\text{図形により選択図形を指示する桁の組み合わせ数}} \times \underbrace{10}_{\text{選択図形の種類数}} \times \underbrace{10}_{\text{選択図形を指示する位置の数}} = 600$$

図 8: ビデオ撮影によって攻撃者が得る秘密情報の候補数

したがって，仮に認証行為がビデオで撮影されたとしても，それによって秘密情報が即座に特定されることはない．また Volker らが提案している方法よりも安全性は高いと言える．

もう一つ起こりうる脅威として，選択図形に関する Challenge が攻撃者に知られた場合の安全性について述べる．

当然だが，Challenge を知られただけでは秘密情報の特定にはつながらない．しかし，Challenge を知られた上で，かつ認証行為をビデオで撮影された場合は秘密情報が特定されることになる．したがって Challenge は，第三者に知られないようにすることが強く望まれる．Challenge の発行については，一定の制限があることが望ましいであろう．例えば，銀行のキャッシュカードがなければ，そのユーザの認証に必要な Challenge は取得できないといった仕組みが考えられる．また Challenge と認証行為の双方をビデオで撮影されないよう，Challenge を発行する機器と認証を行う機器は別にすべきである．

なお正規ユーザが認証する前に Challenge が第三者に知られたことに気づいたならば，その脅威は回避可能である．なぜならば，第三者に知られてしまった Challenge を認証に使用せずに破棄し，新たに Challenge を再取得してから認証を行えばよいからである．

また別の脅威として，共有値探索攻撃が考えられる．この攻撃は，攻撃者が該当ユーザの認証行為を撮影したビデオを複数所持していることが前提となる攻撃であり，一回のビデオで攻撃者が得る秘密情報の候補は 600 個であるが，その候補群が複数あった場合には，その群の中に存在する共有値を抽出することで秘密情報が特定可能になるという攻撃方法である．この攻撃方法を使用すると，秘密情報の候補が 600 個よりもはるかに少ない数に絞りこまれていく可能性があり，その脅威評価と対策は今後の課題である．

### 4.2 利便性

fakePointer の利便性について，3 つの観点から述べる．

1. 記憶負担
   fakePointer における記憶負担について述べる．本手法においてユーザが長期記憶として保持しなければならない情報は 4 桁数字のみであり，既存の暗証番号認証と同じである．ただし fakePointer では，認証時には暗証番号に加えて選択シンボルに関する Challenge を記憶する必要がある．このため記憶負担が増しているのは確かである．しかし，それは長期記憶として保持する必要はなく，認証時にのみ記憶しなければならない情報であるため，その負担増は必要最小限に抑えられていると考える．

2. 回答入力方法
   次は入力方法である．打鍵数について考えると，通常の暗証番号認証は多くても 5 回の打鍵で暗証番号の入力が完了するが，fakePointer の場合は，それ以上の回数になる．よって打鍵数について見れば，その手間は増大する．しかし fakePointer は 3 種類のキーだけで回答入力が可能であり，キーボードや画面に表示されている数値の位置を気にしなくても入力操作は可能である．したがって打鍵数は増えるものの，入力操作自体は平易になると言える．またこの特徴ゆえ，キーボードは必須要件ではなく，PDA や携帯電話でも操作は可能である．

3. 操作時間
   fakePointer の操作にかかる時間をユーザ実験により測定した．ユーザ実験は，大学院生の男性 6 名で行った．fakePointer の仕組みについて説明し，事前に 3 回ほど練習したあと認証実験を 3 度実施し，その操作時間を測定した．結果は平均で 17.35 秒となり，最小ならびに最大値はそれぞれ，9.84 秒と 29.75 秒であった．操作時間は暗証番号認証より長くなることに疑いの余地はないが，操作に習熟するにしたがい 15 秒前後で操作できる可能性は十分あると考えている．

### 4.3 今後の課題

今後の課題は，Challenge の記憶を容易にすることと，安全性を維持しつつ回答方法の容易にしうる手法の探求である．操作時間の測定実験後に被験者に対して本手法の意見を求めたが，その結果はどれもネガティブなものであった．その内容を要約すると，以下の通りになる．

- 選択図形の Challenge が覚えられない
- 数字による選択図形の指定は混乱を招く
- 照合画面の初期画面を見忘れてしまい，数字から選択図形を得られなくなった
- 似ている図形があって混乱しやすい

したがって，本手法の実用化に向けて Challenge の記憶と回答方法を平易にすることは急務である．

本手法において，選択図形に関する Challenge を 1 つの図形と 1 つの数値で構成している理由は，安全性と利便性のバランスを考慮した結果である．理想的には，4 つの図形をランダムに組み合わせて使用することが望ましいが，それでは選択図形に関する Challenge の記憶は極めて困難になる．そこで 2 種類の図形を 2 回ずつ使用することを考えたが，これでは安全性が低下する．そこで折衷案として 1 つの図形で 2 回分の選択を指示し，あとの 2 回は数値で指定することで，結果として 3 種類の図形を使うことを可能にしつつ，記憶すべき情報としては 2 種類に抑えるという手法を採用したのである．

しかしながら，現在の実装では Challenge の記憶は困難であり，かつ操作方法も複雑であることは明らかである．今後は選択図形として図形のかわりに文字や写真の利用も考慮に入れ，ユーザ評価を実施する予定である．

## 5 おわりに

本論文では，個人認証，特に暗証番号認証における覗き見攻撃に注目し，その攻撃を困難にする方法として fakePointer を提案した．覗き見攻撃の原因は秘密情報をユーザに直接回答させるユーザインタフェースにあるとし，攻撃を困難にする方法として二層式の表示による認証画面を提案した．

このインタフェースにおける回答入力方法は，特定の図形を入力したい数字キーの背景にするという方法である．fakePointer では，画面上の全ての数字キーが背景になんらかの図形をもつ表示になっているため，どの図形が回答選択に使用されているかが不明であり，攻撃者が認証行為を覗き見たとしても，ユーザの入力値を特定することが困難になっている．

また Challenge and Response の仕組みを応用し，回答に使用する選択図形を認証の毎に変更することにより，仮に攻撃者が認証行為をビデオで撮影していたとしても，秘密情報の特定を困難にし，一定の安全性を担保可能にしている．しかしその一方で，操作方法が複雑であり，また設計時の想定以上にユーザの記憶負担が大きいことがユーザのアンケート結果から明らかになっており，その改善が今後の課題である．

## 参考文献


[1] 高田哲司，増井俊之,“fakePointer: 回答候補の複数同時選択による” 覗き見攻撃” への安全性改善法, DICOMO2006, pp.77-80, July 2006.

[2] Desney S. Tan, Pedram Keyani and Mary Czerwinsky,“Spy-resistant keyboard: more secure password entry on public touch screen displays, Proceeding of OZCHI 2005, 2005.

[3] Volker Roth, Kai Richter and Rene Freidinger“A PIN entry method resilient against shoulder surfing. In Proc. 11th ACM Conference on Computer and Communication Security, pp.236–245, Oct 2004.

[4] 原田篤史，漁田武雄，水野忠則，西垣正勝，画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013, 2005.

[5] 徐強，西垣正勝，ニーモニックに基づくワンタイムパスワード型画像認証の実現可能性に関する検討，情報処理学会研究会報告，2006-CSEC-32，pp.275–280, 2006

[6] L.Sobrado and J.C.Birget,“Graphical passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm,

[7] トマト銀行,“操作画面をすっぽり覆う「盗撮防止カバー」を ATM に設置, 日経 BP, March 27, 2006. http://www.nikkeibp.co.jp/archives/425/425911.html, site accessed at Dec 07, 2006

[8] 東洋通信機, 暗証番号入力装置, 特開 2001-147763, 2001.

[9] 三菱電機，暗証番号入力装置，特開平 05-334334, 1993.

[10] 日本信号，暗証番号を入力する装置，特開平 09-297875，1997.

[11] シャープ， VeilView モバイル ASV 液晶, http://www.sharp.co.jp/products/sh851i/text/veilview.html, site accessed at Dec 07, 2006.