Vol.2013-CSEC-62 No.1
Vol.2013-SPT-6 No.1
2013/7/18

覗き見攻撃耐性を考慮した加算型 PIN 認証方式に関する一検討

磯貝尚明[†1]　長谷川まどか[†1]　篠田一馬[†1]　加藤茂夫[†1]

現在，携帯電話やスマートフォンでは，暗証番号による認証方式(PIN 方式)が最もよく利用されているが，覗き見によって秘密情報が漏えいする危険性が存在する．このため，覗き見による秘密情報の漏えいを防止可能な認証方式の確立が望まれている．本稿では，ユーザが予め設定した PIN に，システムからランダムに提示される数字を加算して入力を行う認証方式を提案する．提案方式では，加算するランダムな数字を，音や画像でユーザのみに提示する．先行研究方式とのユーザビリティの比較を行ったので報告する．

A Study on a PIN Authentication based on Digit Addition for Preventing Shoulder-Surfing

Naoaki ISOGAI[†1]　Madoka HASEGAWA[†1]
Kazuma SHINODA[†1]　Shigeo KATO[†1]

Currently, PIN code is commonly used for the user authentication in cell phones and smartphones. However, the user's PIN may be stolen by a person standing behind the user and observing the screen. A usable authentication method deterring shoulder-surfing is highly desired. In this paper, we propose a new PIN entry method that adds a random number for each digit of PIN. The random number is presented as a sound or an image to the user by the system through a secret channel. We compared usability of this method with the other methods.

1. はじめに

昨今，広く普及した携帯電話やスマートフォンでは，端末内に保存された情報へのアクセスの際に本人認証が欠かせない．この本人認証プロセスで用いられる認証方式としては，暗証番号による認証(PIN 方式)が主流である．PIN 方式の特徴として，ユーザにとって秘密情報の記憶が容易である点や，認証方法がシンプルであるため認証時間が短い点が挙げられる．しかし一方で，入力操作の覗き見やカメラによる盗撮によって，秘密情報が容易に漏えいし，正規ユーザに成りすまされる危険性も存在する．この欠点はディスプレイが大きい傾向にあるスマートフォンでは特に注意が必要である．このような欠点への対策として，ユーザが何を入力しているのかを周囲からは容易には判断できない認証方式の確立が望まれている．

覗き見攻撃に耐性を持つ認証方式のひとつに生体認証がある．生体認証は，指紋や静脈などの身体的特徴を秘密情報として利用する方式[1]と，歩行動作やジェスチャなどの行動的特徴を秘密情報として利用する方式[2]の 2 つに分類することができる．これらの認証ではユーザの生体情報を秘密情報として利用するため，ユーザ自身が秘密情報を記憶する必要がない反面，広いスペースを必要とするなど認証を行える場所の制約や，認証を行う上で特殊な機材が必要となるなどの制約があり，利用可能な場面が限られている．また，覗き見攻撃を考慮した認証方式の 1 つに PIN の代わりに画像を秘密情報として用いる，グラフィカルパスワード方式が研究されている[3]-[5]．一般にグラフィカルパスワード方式は覗き見攻撃に対して脆弱であるとされているが，認証方法を複雑にすることで秘密情報の漏えいを防ぐ方式[6]や，画像自体に不鮮明化処理を加えることで正規ユーザ本人以外には画像の認識や記憶を困難にする方式[7]など，覗き見攻撃に対して耐性を持たせる研究が行われている．しかし，これらの方式を用いても，複数回の認証行為から秘密情報の推測を行う Intersection 攻撃によって秘密情報が漏えいする可能性がある．

このため，これらの攻撃に対して耐性のある認証方式が求められている．覗き見攻撃に強く，Intersection 攻撃に対しても耐性を持つ認証方式の一つとして，ユーザに対して複数の知覚情報を与え，これをもとに入力方法を毎回変化させることで秘密情報の漏えいを防止するマルチセンソリー認証方式[8]-[11]がある．マルチセンソリー認証方式では，ユーザ本人にしか知覚できない情報を含む複数の知覚情報を認証に利用するため，認証行為の覗き見攻撃に強く，また，毎回提示する情報が異なるため Intersection 攻撃にも強いという特徴がある．

マルチセンソリー認証方式の利用ケースとして，文献[8],[9]では ATM のような比較的大型の専用機器，文献[10],[11]ではスマートフォンなどのタッチパネル搭載端末での使用を前提とした検討が進められている．これらの検討において，マルチセンソリー認証方式は認証手順が複雑なため認証操作に要する時間が長く，PIN 方式に比べてユーザビリティが低い傾向にあることが分かっている．

そこで本稿では，覗き見に頑健で，認証操作もシンプル

†1 宇都宮大学大学院工学研究科情報システム科学専攻
Graduate School of Engineering, Utsunomiya University

Vol.2013-CSEC-62 No.1
Vol.2013-SPT-6 No.1
2013/7/18

な認証方式として，ユーザ本人にしかわからないようにランダムな数字を提示し，PIN との加算結果を入力する，タッチパネル搭載端末向けの認証方式を提案し，そのユーザビリティ評価を行ったので報告する．

2. 先行研究の概要

2.1 マルチセンソリー認証

マルチセンソリー認証方式とは，複数の知覚要素を利用して認証を行う認証方式である．なお本方式は，システムが提示するチャレンジと呼ばれる入力のルールに対して，ユーザが一定の規則を踏まえてレスポンスを返すことで認証の可否判定を行っているため，チャレンジ&レスポンス方式の一種と考えることができる．チャレンジ&レスポンス方式では，まずシステムが，チャレンジと呼ばれる，秘密情報を入力するための規則を毎回ランダムに提示する．これに対してユーザは，提示されたチャレンジを考慮して秘密情報を入力し，システム側にレスポンスとして応答する．このときシステムは，あらかじめユーザが登録したパスワードと提示したチャレンジをもとに演算を行い，演算結果とユーザからのレスポンスを検証して認証の成否を判定する．マルチセンソリー認証方式におけるチャレンジは周囲からも見ることが可能な Visible チャレンジと，正規ユーザ本人にしか知り得ない Invisible チャレンジとで構成されている．認証を行う際，ユーザは与えられた Visible チャレンジと Invisible チャレンジを総合的に考慮した上でレスポンスを行うため，両方のチャレンジが同時に漏えいしない限り，第三者が正規ユーザの秘密情報を盗むことは困難である．

マルチセンソリー認証方式の概要を図 1 に示す．まず，認証システムは，視覚的な入力インターフェース画面と，正規ユーザ以外は知覚不可能な聴覚的情報（または不鮮明化した画像情報など）とをユーザに提示する．後者の情報は，システムが認証のたびごとにランダムに決定して出力する．ユーザは，これらの与えられた情報と，PIN などの自分の認証トークンとにもとづいて応答を決定し，システムに入力する．

その後，システムは，ユーザの応答と認証システム内で算出した正解とを検証し，認証の可否を判定する．この方式では，視覚的な情報に加えて，正規ユーザ以外には知り得ない（または認識できない）情報も利用して生成した応答を入力するため，第三者によって入力操作を覗き見られた場合においても，秘密情報である認証トークンが漏えいすることはない．

2.2 マルチセンソリー認証における認証操作の手順

先行研究で用いられているインターフェースを図 2 に示す．この研究では，テストモードと認証モードとを用意しており，図 2 は後者の例である．テストモードでは，円の内側の 4 つのチェックボックスに，入力された PIN の数

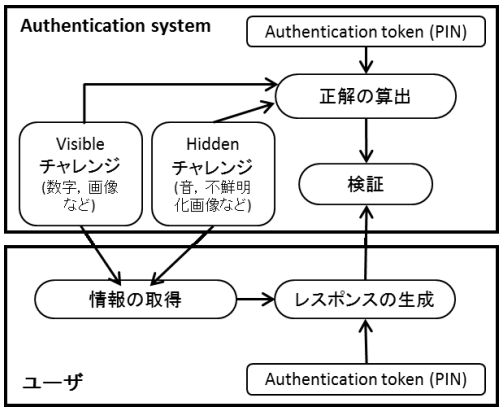


図 1　マルチセンソリー認証の概要

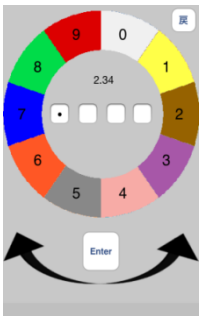


図 2　先行研究のインターフェース(認証モード)

字が一桁ずつ表示されるが，認証モードでは，入力した PIN は黒点で表示される．なお，円の内側の数字は操作開始からの経過時間を表しており，画面右上のボタンは進行中の認証処理を中止し認証開始画面に戻るためのボタンである．

先行研究では，Visible チャレンジとして，White，Yellow，Brown，Purple，Pink，Gray，Orange，Blue，Green，Red の 10 色に分割された円環を用い，分割された各ブロック上には 0 から 9 までの数字をそれぞれ配置している．画面下部の矢印が表示されている領域において，指を左方向に 1 回スワイプさせることで時計回りに数字が 1 回ずつ移動し，右方向に 1 回スワイプさせることで反時計回りに数字が 1 回ずつ移動する．スワイプ操作を用いて数字の移動を行った後，円環の下に表示されている Enter ボタンをタップすることで PIN の 1 桁分の入力を行う．これを 4 回繰り返して全 4 桁の入力を行うことになる．

第三者が，Visible チャレンジの視覚情報から，入力された PIN の数字を判断できないようにするため，PIN の数字をどの色のブロックに移動するかを Invisible チャレンジの聴覚情報としてユーザに提示する．本方式の Invisible チャレンジでは，Visible チャレンジに用いる 10 色のうちの 1 色がランダムに選択され，その色名の音声がヘッドホンを介して出力される．この音声情報は Visible チャレンジで示される色のブロックと対応しており，Enter ボタンをタップすることで入力される数字は，音声によって提示された色のブロック上に表示されている数字となる．そのため，認証を行う場合に，Invisible チャレンジによって指定された

Vol.2013-CSEC-62 No.1
Vol.2013-SPT-6 No.1
2013/7/18

色のブロックまで，数字を移動する操作が必要となる．各知覚情報は認証開始と同時に出力され，PIN の 1 桁の入力毎に，次の新しい Invisible チャレンジが提示される．

2.3 認証の操作例

本方式における認証操作の例を図 3 に示す．図では，説明のため，テストモードの画面を示している．ここでは，PIN が「1234」，Invisible チャレンジが「Blue, Red, Gray, Blue」の場合の例を説明する．なお，色名の音声は実際にはシステムが毎回ランダムに決定する．ユーザは，ヘッドホンを装着して音声を聞き取るものとする．

ステップ 1：認証開始と同時にヘッドホンから「Blue」と音声が出力される．

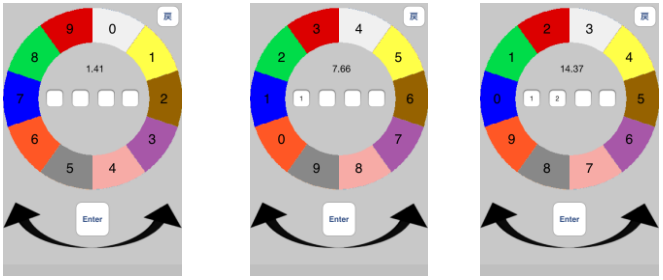
ステップ 2：青色で着色されたブロックまで，PIN の 1 桁目である「1」を移動する．その後，Enter ボタンを押すことで入力を行う．

ステップ 3：次の Invisible チャレンジとして「Red」の音声が出力される．PIN の 2 桁目である「2」を赤色で着色されたブロックに移動し，Enter ボタンを押すことで 2 桁目の入力を行う．

ステップ 4：次の Invisible チャレンジとして「Gray」の音声が出力される．PIN の 3 桁目である「3」を灰色で着色されたブロックに移動し，Enter ボタンを押すことで PIN の入力を行う．

ステップ 5：次の Invisible チャレンジとして「Blue」の音声が出力される．PIN の 4 桁目である「4」を青色で着色されたブロックに移動し，Enter ボタンを押すことで PIN の入力を行う．

ステップ 6：全桁の入力後，PIN が正しいかどうかをシステムが判定し，認証の成否が表示される．



(a) ステップ 1　(b) ステップ 2 (Blue の上に 1 を移動)　(c) ステップ 3 (Red の上に 2 を移動)

(d) ステップ 4 (Gray の上に 3 を移動)　(e) ステップ 5 (Blue の上に 4 を移動)　(f)ステップ 6 (認証の成否判定)

図 3　先行研究における認証例(テストモード)

3. 加算型 PIN 方式の提案

3.1 概要

先行研究方式は覗き見攻撃に頑健ではあるものの，認証手順が複雑なため認証時間が長く，結果的にユーザビリティが低い．そこで本研究では，ユーザビリティの向上を目指し，通常の PIN 方式に近いインターフェースを採用した．本方式においても正規ユーザ以外には知り得ない知覚情報を同時に利用して認証を行うため，第三者によって認証行為を除き見られた場合においても，入力操作から秘密情報が漏えいすることはない．本方式では Invisible チャレンジとして 0~9 までの数字のうち 1 つをランダムに出力する．ユーザは，あらかじめ決定した PIN と提示された数字とを加算し，その和を入力することで認証を行う．和が 10 を超えた場合は，1 の位の値だけを入力する．例えば，提示された数字が「8」で入力したい PIN の値が「9」の場合，和の 17 のうち，1 の位の値である「7」を入力する．これを PIN4 桁すべてに対して行うことで認証の成否判定をする．Invisible チャレンジは音声または重畳画像によって提示され，PIN を 1 桁入力するごとに新しい数字が提示される．

本研究では，Invisible チャレンジを，ヘッドホンを介した音声で提示する方式と，重畳画像で提示する方式について検討を行った．次節で各方式の詳細を説明する．

3.2 音声を用いた加算型 PIN 方式

音声を用いた場合のインターフェースを図 4 に示す．本方式のインターフェースは通常の PIN 方式と同じである．先行研究と同様に，本方式でも，ユーザはヘッドホンを装着して認証を行う．ヘッドホンからは Zero，One，Two，Three，Four，Five，Six，Seven，Eight，Nine の音声のうち 1 つが出力される．入力を行う場合は，PIN と提示された数字との和の 1 の位を 0~9 のボタンを押すことで入力する．

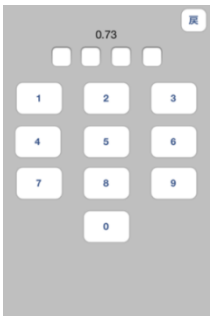


図 4　音声を用いた加算型 PIN 方式のインターフェース

3.3 重畳画像を用いた加算型 PIN 方式

重畳画像を用いた場合のインターフェースを図 5 に示す．本方式では画面右下に数字とテクスチャとを重畳して不鮮明化した画像が提示されている．重畳画像の例を図 6 に示す．図 6 は，説明のため，文字部を強調しているが，実際には図 5 に示すように，画面から離れた第三者には見えない程度に不鮮明化されている．用意した数字のフォントは MS ゴシックおよび，Bauhaus 93 の 2 種類である．本

方式において背景にテクスチャ画像を使用しているのは，重畳画像が画面の右下に提示されていることを第三者からわかりにくくするためである．数字の入力を行う場合は，音声を用いた加算型 PIN 方式と同様に，PIN と提示された数字との和の 1 の位を 0~9 のボタンを押すことで入力する．

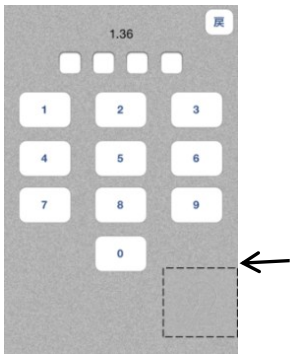


図 5　画像を用いた加算型 PIN 方式のインターフェース

図 6　重畳画像の例

3.4 認証の操作例

本方式における認証の流れを図 7 に示す. PIN が「1234」，システムによって提示された数字が「2497」の場合を例として説明する．ここでは 3.3 節の重畳画像を用いた方式の例を説明する．なお，先行研究の認証例と同様，実際の認証画面では入力した PIN は黒点で表示されるが，ここでは例として数字をそのまま表示するテストモードの画面を示している．テストモードでは，入力した PIN が可視状態となり，入力時間が詳細表示されるなどの差異がある．

ステップ 1: 認証開始と同時に, 画面右下に重畳画像で「2」が提示される．

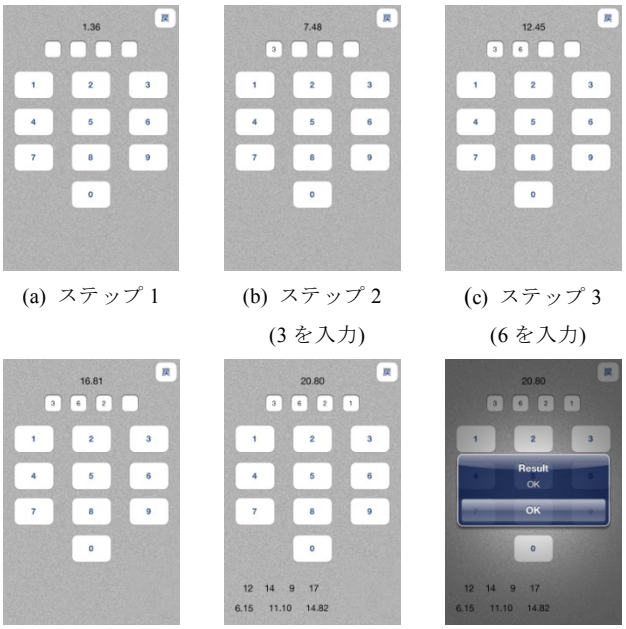
ステップ 2 : 提示された「2」と，入力したい PIN の 1 桁目である「1」との和の「3」を PIN の 1 桁目として入力する．

ステップ 3 : 重畳画像で「4」が提示される．PIN の 2 桁目である「2」と，提示された「4」との和の「6」を PIN の 2 桁目として入力する．

ステップ 4 : 重畳画像で「9」が提示される．PIN の 3 桁目である「3」と，提示された「9」との和の「12」のうち 1 の位の値である「2」を PIN の 3 桁目として入力する．

ステップ 5 : 重畳画像で「7」が提示される．PIN の 4 桁目である「4」と，提示された「7」との和の「11」のうち 1 の位の値である「1」を PIN の 4 桁目として入力する．

ステップ 6 : 全桁の入力完了後，PIN が正しいかどうかをシステムが判定し，認証の成否が示される．



(a) ステップ 1　(b) ステップ 2 (3 を入力)　(c) ステップ 3 (6 を入力)

(d) ステップ 4 (2 を入力)　(e) ステップ 5 (1 を入力)　(f) ステップ 6 (認証の成否判定)

図 7　加算型 PIN 方式の認証例

4. 比較実験

4.1 実験概要

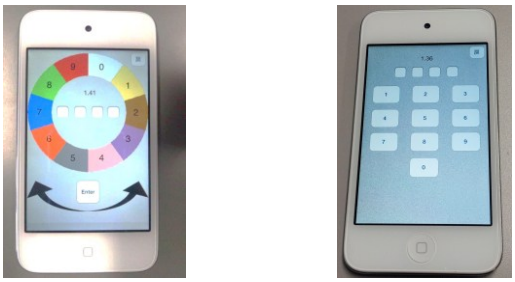
PIN 方式，先行研究で提案されている色を用いたマルチセンソリー方式(以下，先行研究(色))，提案方式である音声を用いた加算型 PIN 方式(以下，加算型 PIN 方式(音声))，および，重畳画像を用いた加算型 PIN 方式(以下，加算型 PIN 方式(画像))の全 4 方式について，ユーザ実験を行い，認証時間および認証成功率を測定した．なお，認証時間とは，認証の操作が開始されてから 4 桁目の PIN の入力が完了するまでの時間である．また，認証成功率とは，認証試行回数に対して認証が成功した回数の割合である．ユーザビリティが高く，使い易い方式ほど，認証時間が短く，認証成功率が高くなると考えられる．先行研究(色)に比べて，提案方式は認証方法がシンプルであるため，ユーザビリティが高い評価となることが期待される．

4.2 実験環境

実験には，図 8 に示す第 4 世代 iPod touch を使用する．ソフトウェアの開発には Xcode を使用した．

実験の参加者は，20 代の理系学生 12 名である．実験結果に順序効果が表れないようにするため，A~F の 6 つのグループに参加者を割り振り，データを取得した．表 1 に各グループの実験順序を示す．なお，表 1 中の数字は各グループが実験を行った方式の順序を表している．ただし, PIN 方式は参加者全員が普段から慣れていると考えられるため，すべてのグループで最初に実験を行った．

Vol.2013-CSEC-62 No.1
Vol.2013-SPT-6 No.1
2013/7/18



(a) 先行研究(色)　　(b) 加算型 PIN 方式(画像)

図 8　実験に使用した端末

実験の流れは以下の通りである．まず，実験の概要説明を行い，音声を使用する先行研究(色)と加算型 PIN 方式(音声)では使用する 10 種の音を，画像を使用する加算型 PIN 方式(画像)では 20 枚の重畳画像を一通り見せ，意味が分からない音声や画像が無いかを確認した．なお，先行研究(色)と加算型 PIN 方式(音声)では，参加者のみが音声を聴取できるように，参加者にヘッドホンを装着させた．音量は，実験者が提示される音声の説明をした後に参加者に確認させ，参加者自身が聴きとり可能な音量に調整させた．その後，実際の認証手順について説明を行った．

次に，各方式について，テストモードを用いた練習後に本実験を行った．練習は，PIN 方式では 2 回，それ以外の 3 方式においてはそれぞれ 7 回とし，本実験では 5 回の認証操作を行った．実験順序は表 1 の通りである．

なお，入力する PIN は実験者が選定して参加者に与えた数字であり，参加者ごとに異なっている．

表 1　グループごとの実験順序

グループ	PIN	先行研究(色)	加算型 PIN (音声)	加算型 PIN (画像)
A	1	2	3	4
B	1	2	4	3
C	1	3	2	4
D	1	3	4	2
E	1	4	2	3
F	1	4	3	2

4.3 実験結果

参加者 12 名分の認証試行回数 5 回のデータ，計 60 回の認証に関するデータを，方式ごとに集計を行った．図 9 に認証時間ならびにその標準偏差を，表 2 に認証成功率ならびにその標準偏差をそれぞれ示す．なお，図表のデータは全参加者の結果を平均したものであり，図中のバーは標準偏差を示す．

まず，図 9 に示す認証時間について考察する．PIN 方式が最も時間が短く 1.72 秒であった．続いて加算型 PIN 方式(画像)が 5.77 秒，加算型 PIN 方式(音声)が 7.21 秒，そして認証時間が最長であったのが先行研究(色)で 11.34 秒であった．このことから今回提案した 2 種の加算型 PIN 方式は，PIN 方式と比べると認証時間が長いが，先行研究(色)よりは優位であることがわかる．続いて，認証時間の標準偏差について着目すると，加算型 PIN 方式(画像)は 1.60，加算型 PIN 方式(音声)が 2.12，先行研究(色)が 2.20 となっており，加算型 PIN 方式(音声)と先行研究(色)の間にはあまり差がないが，加算型 PIN 方式(画像)は，先行研究と比べても標準偏差が小さく，参加者による認証時間の差が小さいことがわかる．このことからより多くのユーザに受け入れられる方式である可能性がある．

次に，表 2 に示す認証成功率について考察する．認証成功率も認証時間と同様で PIN 方式が最も高く，98.3%であった．続いて高かったのが加算型 PIN 方式(画像)で 96.7%，先行研究(色)が 93.3%，加算型 PIN 方式(音声)が最も悪く 86.7%であった．このことから，加算型 PIN 方式(画像)は，PIN 方式と同程度の認証成功率であり，先行研究から比べても高い成功率となっていることから，加算型 PIN 方式(画像)が先行研究(色)よりも優位であることがわかる．しかし，加算型 PIN 方式(音声)においては，先行研究(色)と比べても成功率が低いことがわかる．続いて，認証成功率の標準偏差に着目すると，加算型 PIN 方式(画像)は 7.45，先行研究(色)が 9.43，加算型 PIN 方式(音声)が 17.00 となっており，加算型 PIN 方式(画像)は，先行研究(色)と比べても標準偏差が小さく，参加者による認証時間の差が小さいことがわかる．また加算型 PIN 方式(音声)は，ほかの方式と比べて標準偏差が大きくなっていることから，ユーザによっては，使いにくいと感じる方式である可能性がある．

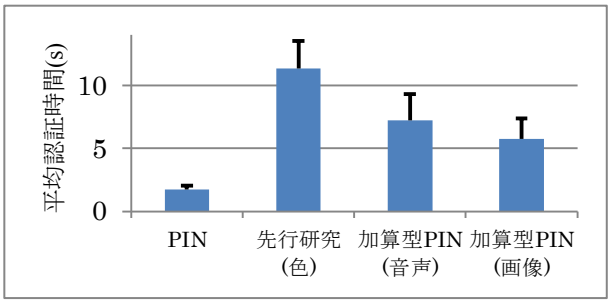


図 9　平均認証時間(s)および標準偏差

表 2　平均認証成功率(%)および標準偏差

	PIN	先行研究 (色)	加算型 PIN (音声)	加算型 PIN (画像)
平均認証成功率(%)	98.3	93.3	86.7	96.7
(S.D.)	5.53	9.43	17.0	7.45

次に認証時間と認証成功率それぞれに対して Tukey 法を用いて各方式間の有意差検定を行った．認証時間の p 値を表 3 に，認証成功率の p 値を表 4 にそれぞれ示す．認証時間について着目すると PIN 方式とそれ以外の 3 方式それぞれ，先行研究(色)と加算型 PIN 方式(音声)，加算型 PIN 方式(画像)のそれぞれ間において有意水準 5%で有意差が確認され，加算型 PIN 方式(音声)と重加算型 PIN 方式(画像)間のみ有意水準 5%で有意差は確認できなかった．次に認証成功率について着目してみるとすべての方式間において有意水準 5%では有意差が確認できなかった．

表 3　認証時間の有意差

	PIN	先行研究(色)	加算型 PIN (音声)	加算型 PIN (画像)
PIN		8.28×10^{-13}	1.58×10^{-8}	1.15×10^{-5}
先行研究(色)	8.28×10^{-13}		8.02×10^{-6}	1.11×10^{-8}
加算型 PIN (音声)	1.58×10^{-8}	8.02×10^{-6}		0.22
加算型 PIN (画像)	1.15×10^{-5}	1.11×10^{-8}	0.22	

表 4　認証成功率の有意差

	PIN	先行研究(色)	加算型 PIN (音声)	加算型 PIN (画像)
PIN		0.69	0.07	0.98
先行研究(色)	0.69		0.47	0.89
加算型 PIN (音声)	0.07	0.47		0.15
加算型 PIN (画像)	0.98	0.89	0.15	

表 5　各方式の平均順位

	平均順位
先行研究(色)	2.17
加算型 PIN (音声)	2.50
加算型 PIN (画像)	1.33

4.4 実験結果とユーザビリティの相関

まず，認証時間の短さに着目すると，PIN 方式，加算型 PIN 方式(画像), 加算型 PIN 方式(音声), そして先行研究(色)の順となった．次に，認証成功率の高いものから降順に並べた場合では，PIN 方式，加算型 PIN 方式(画像)，先行研究(色), 加算型 PIN 方式(音声)の順となった. このことから，上位の PIN 方式，加算型 PIN 方式(画像)の順序は一致するものの，3 位以下は入れ替わっており，認証時間と認証成功率の間には必ずしも相関がないと考えられる．

次に，実験後のアンケート結果について考察する．アンケートでは，PIN 方式を除く 3 方式について，使いやすいと感じた方式の順に完全順位法で 1 位から 3 位までの順位付けを行う項目を用意した．各方式に対して参加者が付けた順位を平均した結果を表 5 に示す．集計結果より，認証時間が最短で，認証成功率が最高であった加算型 PIN 方式(画像)の平均順位が最も高いことが分かる．次いで，先行研究(色)，加算型 PIN 方式(音声)の順となっている．この順番は認証成功率と同じであることがわかる．このことからユーザにとっての使いやすさは，認証時間よりも，認証成功率との相関が高いと考えられる．

加算型 PIN 方式(音声)では，加算型 PIN 方式(画像)に比べ認証成功率が 10%程度低下した理由としては，加算型 PIN 方式(画像)では，認証を行う画面上に常に数字が提示されているのに対して，加算型 PIN 方式(音声)では，数字の音声は 1 度再生されてしまうと聞き直せないこと，および, 今回は実験者から与えられた PIN を使用したため, PIN を復唱しながら数字の音声を耳で聞くユーザが多く，ユーザの負担が増大した結果，操作ミスや計算ミスが生じたのではないかと考えられる．

また，今回行ったユーザ実験では参加者が理系学生のみであり，比較的計算が得意な参加者が集まったと考えられるため，提案手法が先行研究(色)と比べて良好な結果が得られた可能性がある．そこで，今後，文系の学生を含めたより大きな規模のユーザ実験を行う予定である．

5. おわりに

本論文では，覗き見攻撃への耐性を考慮した加算型 PIN 方式を提案し 2 種類の数字の方法を提案した．PIN 方式と先行研究(色)を含めた 4 種類の方式に関するユーザ実験を行った結果，加算型 PIN 方式(画像)の認証時間が 5.77 秒と先行研究の 11.34 秒の約半分の時間で認証を完了することができた．また認証成功率においても先行研究の 93.3%よりも 3.4%高い 96.7%であり, PIN 方式との差も 1.6%と小さく良好な結果が得られた．このことから提案手法のユーザビリティが高いことを確認した．

今後の課題としては，文系学生を対象にしたユーザ実験により，計算能力がユーザビリティの評価に与える影響の調査や，アンケートで得られた意見にもとづいたインターフェースの改善などが挙げられる．

参考文献

1) 鷲見 和彦, “指紋認証システム,” 映像情報メディア学会誌," Vol.58, No.6, pp.759-762, June, 2006.
2) D. Gafurov, K. Helkala, T. Soendrol, “Gait Recognition Using Acceleration from MEMS,” The First International Conference on Availability, Reliability and Security, pp.432-439, 2006.
3) R. Dhamija, A. Perrig, "Déjà vu: A user study, using images for authentication," Proc. 9th USENIX Security Symposium, 2000.
4) 小島 悠子, 山本 匠, 西垣 正勝, “覗き見攻撃耐性と利便性を有する画像認証方式に関する一検討,” 情報処理学会研究報告, CSEC, No.44, pp.91-96, 2009.
5) 高田 哲司, 大貫 岳人, 小池 英樹, “個人認証システム「あわせ絵」の安全性と利便性に関する評価実験,” 情報処理学会論文誌, Vol47, No.8, pp.2602-2612, Aug., 2006.
6) 安斎 太基, 伊與田 光宏, “画像を用いた個人認証手法の提案,” 画像電子学会誌, Vol.38, No. 5, pp.608-613, 2009.
7) E. Hayashi, J. Hong, N. Christin, “Security through a Different Kind of Obscurity: Evaluating Distortion in Graphical Authentication Schemes,” Proc. of the 2011 ACM Conference on Human Factors in Computing Systems, 2011.
8) M. Hasegawa, N. Christin, E. Hayashi, “New Directions in Multisensory Authentication,” Pervasive 2009 Adjunct Proceedings, pp.103-106, May, 2009.
9) H. Sasamoto, N. Christin, E. Hayashi, “Undercover: Authentication Usable in Front of Prying Eyes,” Proc. of the 2008 ACM Conference on Human Factors in Computing Systems, Apr., 2008.
10) M. Hasegawa, N. Isogai, S. Kato, “On Design of Audio Instructions for Multisensory Authentication for Portable Touchscreen Device,” SOUPS2012, USA, July, 2012.
11) 磯貝 尚明, 長谷川 まどか, 加藤 茂夫, “マルチセンソリー認証方式のための聴覚情報の提示法について,” 2013 年電子情報通信学会総合大会予稿集, A-7-9, p.144, Mar. 2013.