

複数回の盗撮に耐性を持つパスワード認証手法の検討

伊藤 拓己[†] 大関 和夫[‡] 平川 豊[‡]

芝浦工業大学大学院 理工学研究科 電気電子情報工学専攻[†] 芝浦工業大学 工学部 情報工学科[‡]

1. 背景と目的

現在、銀行等 ATM での認証は 4 桁の暗証番号によるものが主流である。しかし、認証時に暗証番号である数字を直接入力するため、覗き見やビデオカメラによる盗撮で、他者に簡単にパスワードを知られる危険性がある。実際に、ビデオカメラによる盗撮事件も発生している。

現在、盗撮に耐性を持つ様々な認証方式が提案されている。しかし、これらは複数回の盗撮に対する対処は十分ではない。

本研究では複数回の盗撮が行われても暗証番号が判明しないような認証手法を検討する。

2. 関連研究

先行研究[1]では、絵柄を使い捨て(ワнтаイム)パスワードとして入手し、認証時に暗証番号に正しい絵柄を合わせ入力する手法が提案されている。しかし、この手法は絵柄の安全な入手方法は記述されていない。

先行研究[2]ではユーザに予め最低 2 つの暗証番号を登録させ、認証時に暗証番号の最初の文字で背景の種類を選択し、残りの文字の背景を最初の文字で選んだ背景と同じものに合わせることで認証を行う手法が提案されている。しかし、この手法は複数の暗証番号を登録する必要があり、暗証番号が数字のみの場合には最低でも 12 桁必要となるため、ユーザに多大な記憶負荷がかかる。

3. 提案手法

3.1 ワнтаイムパスワードの生成

1	2			
	3			
4				

(a) パターン

★	■	@	♥	●
◆	=	♣	●	♥
×	▲	@	▲	×
●	■	=	×	■
◆	♣	▲	@	★

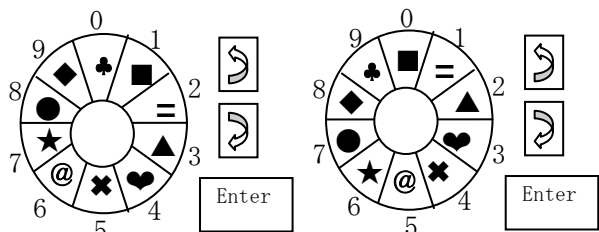
(b) 背景絵柄の表

図 1. ワнтаイムパスワード

ユーザは予め 8 桁の暗証番号とパターン長 2～4 のいずれかのパターンを登録する。パターンとは暗証番号の各桁に対応するワнтаイムパスワードとして用いる背景絵柄の位置を決めるものであり、パターン長とは登録するパターンの長さのことである。図 1(a)はパターン長 4 のパターンの例である。認証時には図 1(b)の様な背景絵柄の表が表示されるので、そこに登録したパターンを合わせることでワнтаイムパスワードの生成を行う。また、登録したパターンの開始位置をずらしてワнтаイムパスワードの生成を行う事が可能なものとする。

例えば暗証番号を 67894321、ワнтаイムパスワードのパターンを図 1(a)の様にした時、初めに暗証番号 6789 に対応するワнтаイムパスワードの生成を行う。パターンの開始位置を背景絵柄の表の 1 行 1 列目に合わせた場合は暗証番号 1 桁目の背景絵柄は「★」、2 桁目の背景絵柄は「■」、3 桁目の背景絵柄は「=」、4 桁目の背景絵柄は「×

3.2 暗証番号の入力



(a) 操作前

(b) 操作後

図 2. 暗証番号入力画面

図 2(a)に暗証番号入力画面を示す。「➡」を押せばワнтаイムパスワードが 1 文字分左回りに回転し、「➡」を押せば 1 文字分右回りに回転する。ここで暗証番号「6」を入力する場合、

それに対応する位置にワнтаイムパスワード「★」が来るように操作し(図 2(b))、”Enter”で入力を確定する。また、提案手法では入力する暗証番号の 1 つ右の数字にワнтаイムパスワードを合わせても良いものとする。よって、暗証番号「6」ではなく「7」に「★」を合わせて入力を行う事も可能である。この操作を残りの暗証番号 7894321 に対しても行う。

4. 評価

ランダム攻撃に対する耐性と 2 回の盗撮に対する耐性について評価を行う。セキュリティ強度は既存の 4 桁の数字による暗証番号の認証と同等の 10000 の候補があることを目標とする。

4.1 パターン長 2 の耐性

図 3 にパターン長が 2、背景絵柄の表が 8 行 8 列、暗証番号の入力時に 1 桁までずらして入力を行える場合のセキュリティ強度を示す。

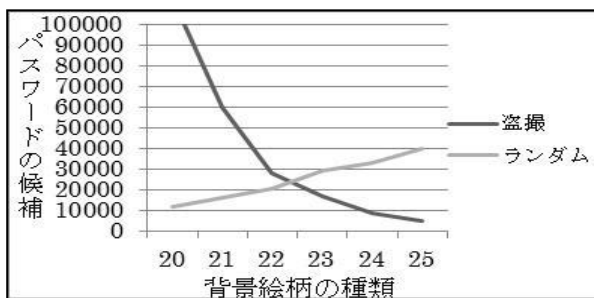


図 3. パターン長 2 のセキュリティ強度

ランダム攻撃に対する耐性は背景絵柄の種類が 20 から 25 の範囲では 10000 以上の候補があるためセキュリティ強度は十分な値となる。

2 回の盗撮に対する耐性は背景絵柄の種類が 20 から 23 の範囲では 10000 以上の候補があるが、24、25 の場合は 10000 以下となる。

したがって、背景絵柄の種類が 20 から 23 の範囲ではランダム攻撃及び 2 回の盗撮に対する耐性があるという結果を得た。

4.2 パターン長 3 の耐性

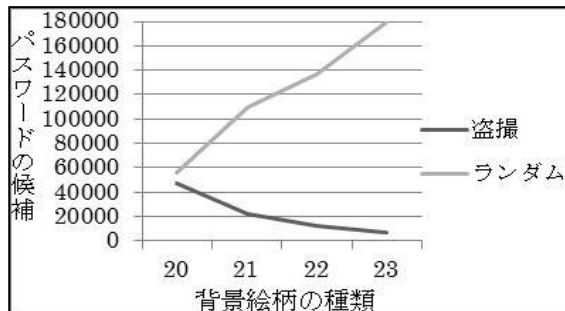


図 4. パターン長 3 のセキュリティ強度

図 4 にパターン長が 3、背景絵柄の表が 8 行 8 列、暗証番号の入力時に 2 桁までずらして入力を行える場合のセキュリティ強度を示す。

背景絵柄の種類が 20 から 22 の範囲ではランダム攻撃及び 2 回の盗撮に対する耐性があるという結果を得た。

4.3 パターン長 4 の耐性

図 5 にパターン長が 4、背景絵柄の表が 8 行 8 列、暗証番号の入力時に 4 桁までずらして入力を行える場合のセキュリティ強度を示す。

背景絵柄の種類が 20 から 21 の範囲ではランダム攻撃及び 2 回の盗撮に対する耐性があるという結果を得た。

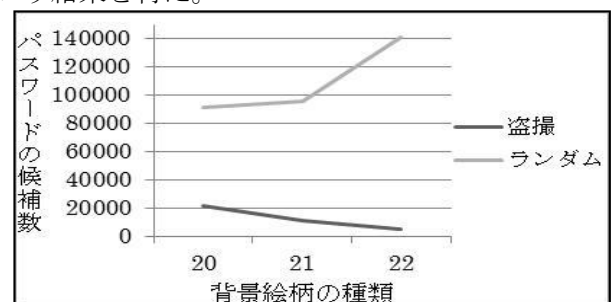


図 5. パターン長 4 のセキュリティ強度

5. まとめと考察

本稿では、ランダム攻撃と複数回の盗撮に対する耐性を持つ暗証番号の入力方式を提案し、システムの構築と評価を行った。提案手法では先行研究よりも暗証番号の桁数を減らすことができ、ランダム攻撃と 2 回までの盗撮に耐性があるという結果を得ることができた。

背景絵柄の種類を増やした場合にはランダム攻撃に対する耐性が上昇するが、盗撮に対する耐性が低下する。ランダム攻撃に対する耐性が上昇する理由としては背景絵柄の種類が増えるにつれ、背景絵柄の表に出現する絵柄は異なるものが増えるので、曖昧性が減り、登録してあるパターンと偶然に一致する確率が減少するためである。盗撮に対する耐性が低下する理由は曖昧性が減るため、想定しえるパターンの総数が減少するためである。

6. 参考文献

- [1] 高田哲司, “fakepointer: 映像記録による覗き見攻撃にも安全な認証手法”, 情報処理学会論文誌, Vol.49, No.9, pp.3051-3061 (2008)
- [2] 桜井鐘治, 撫中達司, “背景配列の移動量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)