L-005

画像を用いた個人認証手法の提案
Proposal of personal authentication technique based on images

安斎 太基†
Taiki Anzai

伊與田光宏†
Mitsuhiro Iyoda

1. はじめに

暗証番号やパスワード等、文字を用いた個人認証手法が様々な場面で用いられ、多くのユーザが生年月日や電話番号等推測されやすい文字列を使用している。そのため、第三者が容易に推測することが可能であり、その対策としてランダムな文字列を使用することが推奨されている。しかし、忘却の危険が高くなる等記憶負担が増加してしまう。

そこで記憶負担を軽減させるために、画像を用いた個人認証手法（以下、画像認証と呼称）が研究されている画像は文字列に比べ、想起,連想が可能であるため記憶負担が小さいという利点がある。本研究では既存の画像認証の手法を調査し、新しい手法の提案を試みる。

2. 現状・目的

以下に、既存の画像認証に関する研究を簡単に紹介する。

・Deja Vu[1]

システムが提示する画像の中から秘密情報とする画像（以下、パス画像と呼称）を記憶する。提示される画像はランダムアートと呼ばれる画像で、画像そのものに意味はない。認証時は、複数の画像の中からパス画像を選択するという手法である。用いる画像にランダムアートを用いる利点は、推測されにくくロ伝やメモによる漏洩の危険が低いからである。しかし、画像自体に意味はないので、記憶負担が高くなっている。

・あわせ絵[3],[4]

Deja Vu同様、複数の画像の中からパス画像を選択する手法である。認証に使用する画像はユーザが自分で登録することができる。これにより、ユーザの記憶負担は軽減するが、正規ユーザに関する情報を持つ第三者に推測される危険も高くなる。

・スキーマ[6]

他の手法同様、複数の画像の中からパス画像を選択する手法であるが、提示される画像にはモザイク化等の不鮮明化処理が施されている。正規のユーザはパス画像登録時にオリジナルの画像を記憶するため、不鮮明化されてもパス画像を判別することができる。一方、第三者は一見しただけでは提示された画像の判別ができないので記憶するのは困難であり、覗き見に耐性を有することができる。しかし、正規のユーザにも判別する時に負担がかかったり、カメラなどに撮影されてしまうと非常に脆弱という問題がある。。

以上のように、現在研究されている画像認証の手法では、認証時に提示される複数の画像の中からパス画像を直接選択する方式が多く用いられている。簡単に言うと銀行のATMにおける暗証番号を画像に置き換えたものである。

しかし、この手法だと覗き見されたときにパス画像が漏洩する危険がある。現実に、ATMでの認証作業をカメラで盗撮することにより、悪意のある第三者が暗証番号を不正に入手し、本人に成りすます事件が起きている。

そこで、本研究では覗き見に対して耐性を有する画像認証の手法を提案する。既存の画像認証の手法では、直接パス画像を選択するため、覗き見されたときにパス画像が特定されてしまう。そこで、パス画像を間接的に選択することで、覗き見されてもパス画像が特定されるのを防ぐ手法を提案する。

3. 提案手法

事前準備として、ユーザに異なる画像を64枚提示し、その中から3枚の画像を登録、記憶してもらう。この3枚の画像がパス画像となる。認証時は、図1のように64枚の画像を升目上に表示する。この時画像はランダムに配置され、4つのグループに分割して表示される。すなわち、1ブロックあたり16枚の画像で構成されている。

ユーザは4つのグループの中からパス画像が最も多く含まれているグループを選択する。この時、最も多くパス画像が含まれているブロックが複数ある場合、逆に最もパス画像が含まれていないブロックを選択する。具体的には、ブロック1,ブロック2,ブロック3にパス画像が1枚ずつ含まれているときは、パス画像が1枚も含まれていないブロック4を選択する。この作業を7回繰り返すことで認証を行う。これにより、ユーザはパス画像を直接選択せず、ブロックを用いて間接的に選択することが可能となる。

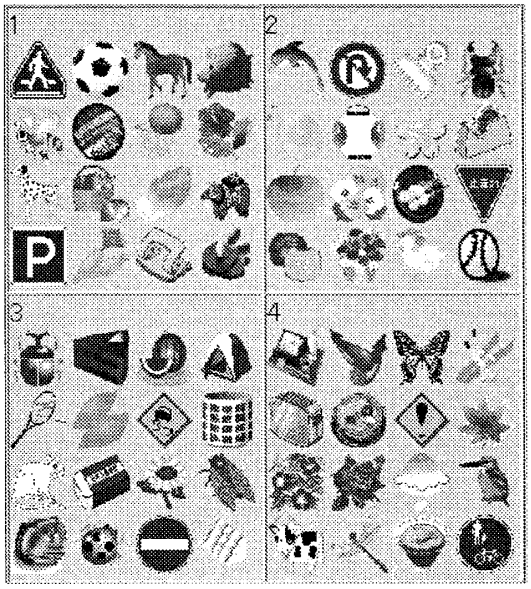

図1. 画像の表示

†千葉工業大学情報科学研究科
Graduate School of Computer Science, Chiba Institute of Technology

4. 攻撃に対する耐性

以下に、提案した画像認証に対して行われると考えられる攻撃方法と安全性について示す。

・Brute-force攻撃

総当り攻撃とも呼ばれ、考えられる秘密情報の組み合わせを全て試行する攻撃方法のことである。

提案手法では毎回表示される画像の並びはランダムであるため、全ての組み合わせを試すのは困難だと考えられる。また、4つのブロックから1つのブロックを選択することを7回繰り返すことから、選択するブロックの組み合わせはと $4^7=16384$通り なり、確率的には既存の暗証番号より安全性は高いと考えられる。

・Educated Guess攻撃

これはある特定の正規ユーザに関する情報を持つ攻撃者がその情報を用いてパス画像を推測し、成りすましを行う攻撃手法である。

提案手法では、使用する画像はシステムが提示するものを使用し、ユーザが自分で好みの画像を登録することはできないため、ユーザに関する情報が入り込む余地は少ないと考えられる。よって、第三者に推測される危険は低いと考えられる。

・Intersection攻撃

これは「パス画像が必ず表示される」という前提を悪用する攻撃手法である。特に複数の画像の中からパス画像を選択する手法の一種で、パス画像以外の画像が認証毎に入れ替わる方式に対して使われる攻撃である。パス画像以外の囮画像が毎回ランダムに変化した場合、表示された画像の積集合を求めることで、最悪2回の認証試行でパス画像が特定されてしまう。

提案手法では表示される画像は毎回同じであるので、この攻撃方法を無効とすることが可能である。

・Observation攻撃

この攻撃は認証作業を覗き見ることでパス画像を特定するものである。最近ではカメラを用いて認証作業を盗撮するケースも存在する。

提案手法において認証作業が覗き見されたときに漏洩する情報は、選択したブロックとそのブロックに含まれている画像のみである。そのため、選択したブロック内のどの画像がパス画像なのか攻撃者に特定されにくいと考えられる。この時、漏洩する画像の組み合わせは

$$ {}_{16}C_3 \quad + \quad {}_{16}C_2 \quad = \quad 680\text{通り} $$

↑ パス画像が3枚の場合　↑ パス画像が2枚の場合

となる。また、パス画像が最も多く含まれているブロックが複数存在するときは、パス画像が最も含まれていない、すなわちパス画像が0枚のブロックを選択する。これにより、選択したブロックに必ずパス画像が含まれているとは限らない。以上から、認証作業を肩越しや横から覗き見された時だけではなく、ビデオで盗撮されたとしてもパス画像の特定は困難であると考えられる。

5. 評価方法

既存の画像認証の研究では、各攻撃方法に対する安全性を考察するとともに、ユーザビリティについても考察されている。ユーザビリティとして、長期記憶の可能性や認証にかかる時間等を調査していた。そこで、本研究でも攻撃方法に対する考察以外に長期記憶の可能性や認証にかかる時間の調査を行う。

攻撃方法に関する考察は上述したものの他に、実際にユーザと攻撃者を用意して耐性を調査する。ユーザビリティに関しては、認証にかかる時間の計測やランダムな文字列と画像の記憶性を比較する。

6. おわりに

本稿では覗き見に対して耐性を有する画像認証の手法を提案した。秘密情報である画像を直接選択するのではなく間接的に選択することで、覗き見をされたときに漏洩する画像が特定されにくくなった。これにより、覗き身される危険の高い駅や街中といった公共性の高い場所でも使用できるのではないかと考えられる。

参考文献

[1] Rachna Dhamia and Adrian Perrig “Deja Vu:A user Study Using Images for Authentication”, 9th Usenix Security Symposium, pp.45-88,(Aug. 2000)

[2] 株式会社ニーモニックセキュリティ “ニーモニックガード”, http://www.mneme.co.jp/index net.html

[3] 高田哲司,小池英樹 “あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法”, 情報処理学会論文誌, Vol.44, No.8, pp. 2002-2012, (Aug. 2003)

[4] 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, Vol.47, No.8, pp.2602-2612, (Aug.2006)

[5] 鹿島一紀 “画像の位置情報による本人認証方式の開発 画像パスワードGATESCENE(ゲートシーン)”, 電子情報通信学会技術研究報告ISEC 情報セキュリティ, Vol.100, No.213, pp.121-127, (2000)

[6] 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, pp1997-2013, (Aug.2005)

[7] 高田哲司 “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(Revisedversion)”, マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2006), pp.77-80, (Jul.2006)

[8] 高田哲司 “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”, 暗号と情報セキュリティシンポジウム(SCIS2007), (Jan. 2007)