画像選択型認証方式における改善策

石原 彰人† 小柳 和子†
†情報セキュリティ大学院大学

1．はじめに

情報システムでは利用者を判別し適切な権限を付与するため認証作業が行われる．広く利用される認証技術に PIN やパスワードがあるが，記憶負荷の低いと考えられる画像を利用することで，記憶を容易にする研究が行われている．しかし，画像を利用した認証技術においても，いくつかの問題がある．本稿では，問題点のうち推測攻撃と呼ばれるものについて，改善策を提案した．改善内容と改善内容を適用したシステムでの実験結果について述べる．

2．画像認証について

広く利用されている認証技術に記憶に基づく認証がある．しかし，人間には記憶を忘れるという問題点がある．特に秘密情報としてよく利用されるランダムな英数字はその文字列自体に意味が無いため記憶することが困難である．そこで，利用者の記憶負荷が少ない認証技術として画像を利用した認証が提案されている．

画像選択型認証方式では，認証時に提示された画像群の中から予め決めておいた正解画像を選択することで，本人確認を行う認証方式である．無意味な文字列ではなく画像を利用することにより容易に覚えることが出来る，正解画像が提示されるため正解を思い出せる等の利点が期待出来る．

しかし，以下のような欠点が発生する．提示された画像群から正解を選びだす方式のため，必ず正解が表示される．このため，攻撃者は攻撃対象の利用者の情報（趣味，嗜好等）と提示された画像群から答えを推測できる可能性がある．また，似た画像を正解にしてしまうと，正解画像間の関連性から推測される可能性がある．利用者が画像を登録可能であれば，画像に関するエピソード等を含めて覚えることが可能になり，記憶負荷が減少する利点が考えられる．しかし，利用者が登録する画像が色合い，ピント等において特徴的であった場合等に，特徴から正解を推測できてしまう可能性がある．このような攻撃が推測攻撃である．

Improvement in authentication method of image selection
Akito Ishihara†
Kazuko OYANAGI†
†Institute of Information Security

また，利用者の正解の画像を選択する動作を観察することにより正解を知ることが出来，覗き見攻撃と呼ばれる．

この方式では利用者は正解画像を選択する必要があるため，システムは必ず正解画像を提示する必要がある．攻撃者は認証試行を繰り返すことで表示された画像を集め，毎回必ず表示される画像を特定することが出来ればそれが正解であると推測可能である．この攻撃を積集合攻撃とする．

3．本研究での改善策

本研究では，推測攻撃に注目をした．1．利用者の情報から正解と推測できる画像が少ない場合，2．関連性のある画像が正解画像数とほぼ同じ枚数表示された場合，3．特徴的な画像が表示されている場合等に攻撃可能である．

1，2のような問題を解決するため，関連性のある画像を囮として表示することで攻撃を難しくすることが考えられる．非正解画像を利用者が選択出来るシステムであれば，利用者が関連性のある画像を登録することで実現出来る．しかし，利用者に対する負担が高いと考えられる．4 桁 PIN と同等の確率にするために，10 枚から 1 枚の画像を 4 回繰り返す認証システムでは，36 枚おとり画像を設定する必要が発生する．

本研究では，この作業を自動で行うシステムを構築した．通常，人間はどのような意味を持った画像であるかを判断することが可能である．情報システムにおいても画像の意味を判断することが出来れば，正解画像に関連性のある囮の画像群を選び出すことが可能である．画像から意味を抽出する，画像に意味を付与しておくなどの方法が考えられる．本研究では，予め意味を付与された画像を利用した．Web 上で公開されているショッピングサイトの Web Service API を利用し，商品 DB にアクセスすることによって，商品の画像と，どのようなジャンルの商品であるかを取得した．ショッピングサイトの画像を利用することによる利点として，画像に特徴が出にくいということがあり 3 の問題の改善が期待できる．このように，1 から 3 の問題を改善し，推測攻撃を困難にすることが期待出来る．

4．テストシステムの概要

改善策の評価を行うためにプロトタイプを作成し実験を行った．そのシステムの概要を述べる．今回のシステムは，認証のみで，PC 上のアプリケーションとして作成した．

利用者は最初，ID と正解画像を 4 枚指定する．画像は Web Service API を通して検索を行い，指定する．システムは指定された画像から，API 経由で関連性のある画像を取得する．

試行時，利用者は ID を指定する．認証画面が表示され，画像が 10 枚ずつ 4 回，全部で 40 枚ランダムな順序で表示される．利用者は 10 枚の中に正解画像があれば選択する．40 枚を表示した後正解画像を 4 枚選択することが出来ていれば認証成功とする．

今回のシステムでは，1 回の表示で出現する正解画像を 1 枚ではなくランダムにし，全体として 4 枚選択とした．これは，10 枚に 1 枚正解がある場合，$(1/10)^4 = 1/10000$ の確立で正解するが，40 枚から 4 枚を選ぶ操作に変更され，$1/{}_{40}C_4 = 1/91390$ で正解するため，安全性の向上が期待出来る為である．

また，画像の変更が行われることにより積集合をとられることを防ぐため，囮の画像は最初に取得した画像から変更を行わない．

5．評価実験

研究室の 7 名に対して，ユーザビリティについて実験を行った．認証は正解画像の設定直後，1 日後，8 日後，22 日後に行い，それぞれの間隔は，1 日，1 週間，2 週間である．何回目の試行で認証成功したか，認証にかかった時間を調査した．認証は 3 回目までに成功できれば認証成功とした．

表 1 に成功までの試行数を示す．画像設定直後や翌日の試行では，2 回目以降での成功や認証の失敗があったが，回数を重ねることで短い試行回数で認証を通過できていた．

表 2 に認証成功時の試行にかかった時間を示す．最大値ではばらつきがあるが最小値ではほぼ 20 秒で認証ができるという結果を得た．

次に，推測攻撃に関する実験を行った．あるユーザーの認証に使われた画像 40 枚を一度に提示した上で正解画像を推測してもらう．誰の認証に使用された画像であるかは教えておく．攻撃の全正解画像を言い当てることで成功とする．

表 3 に 4 枚中何枚推測することが出来たかを示す．4 枚全てを正解し攻撃に成功した者はいなかった．最大でも 4 枚中 2 枚正解という結果であった．全体として，38 回×4 枚=152 枚の画像中 25 枚が攻撃されており，約 16%が推測されている．

表 1．認証成功までの試行回数

	1 回	2 回	3 回	失敗
設定直後	5	1	0	1
1 日後	5	2	0	0
8 日後	6	1	0	0
22 日後	7	0	0	0

表 2．認証成功時の認証時間(s)

	min	ave	max
設定直後	00:23.1	00:52.2	02:19.3
1 日後	00:20.8	00:42.7	02:02.0
8 日後	00:21.3	01:05.3	04:18.7
22 日後	00:22.9	00:38.3	00:57.2

表 3．推測攻撃での正解数

正解数(枚)	0	1	2	3	4
攻撃数(回)	18	15	5	0	0

被験者へのアンケート結果について述べる．非正解画像に関連する画像が提示されるため，関連画像が正解画像とほぼ同じようなものが出てきた場合に分かりにくいといった意見が出た．

6．考察

[2]において暗証番号などにおける認証成功率と認証時間の実験，正解画像間に共通性が無い画像を知人に提示し推測攻撃を行う実験が行われている．暗証番号や[1]において提案されているあわせ絵方式では，8 週経過後でもほとんどの被験者が認証に成功している．認証時間の平均値は，暗証番号が 1 5 秒以下，あわせ絵が 2 4．6 秒であった．推測攻撃の成功率は 25%以上であった．

[2]と比較し，ほぼ同様の認証成功率で推測攻撃の成功率を低下させた．しかし認証時間が平均で 40 秒以上かかってしまう結果になった．これは，各画面で正解画像が出るか不明であったためすぐに思い出すことが出来なかったことが原因として考えられる．想起しやすい条件での評価が今後の課題である．

参考文献

[1]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，(2003)．

[2]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，(2006)．