3W-03

ショルダーハック耐性とユーザの想起性を両立する類似画像を用いた認証手法の提案

A Proposal of Authentication Method Using Similar Images with Shoulder Hack Tolerance and User's Memorability

津谷和紀[†1]　小倉加奈代[†1]　Bhed Bahadur Bista[†1]　高田豊雄[†1]
岩手県立大学[†1]

1. はじめに

近年，スマートフォン（以下スマホ）の普及や PC 端末の小型化が進み，電車など人目につく場所での認証利用機会が増え，肩越しから入力中の認証情報を盗み見るショルダーハック攻撃の危険性が増大している[1]．この攻撃に対し，複雑で推測困難な認証情報を利用する対策が有効であるが，認証情報を忘れやすいという問題がある．

本稿では，ショルダーハック攻撃に耐性があり，ユーザの認証情報に対する記憶保持性を有する類似画像を用いた認証手法を提案し，そのショルダーハック耐性と記憶保持性を評価する．

2. 関連研究

Dhamija et al.[2]は，Deja vu と呼ばれる画像認証システムを提案した．提案システムでは，ユーザはシステムが自動的に生成する幾何学模様の中から認証用画像 5 枚を選択する．認証時にシステムは，認証用画像 5 枚を含む 25 枚の画像を表示する．ユーザが 5 枚の認証用画像を正しく選択することで，認証成功となる．このシステムは，4 桁の PIN 認証同様の強度を持つことが確認されているが，ユーザは，自動生成された幾何学模様を記憶しにくく，記憶保持性の点で問題点があると考えられる．

Hayashi ら[3]は，Use your illusion と呼ばれる画像認証システムを提案した．提案システムは，ユーザが保持している画像を歪ませた画像を認証用画像に設定し，ログインする認証方法である．ユーザは，最初に 3 枚の画像を認証用画像として記憶する．認証時には，ランダムに表示された 27 枚の画像から 3 枚の認証用画像を選択する．記憶保持性に関する評価では，加工が施された画像でも，1 日後，2 日後，1 週間後，1 か月後の時点で問題なく認証できることが確認されている．このシステムは，記憶保持性に長けているものの，ショルダーハック耐性への考慮がなされていないという問題がある．

3. 提案システム

本提案では，ユーザが自身のスマホや PC に保存している画像を利用することで記憶保持性の向上を実現し，ダミー用画像に類似画像を使用し，さらに画像加工を行うことでショルダーハック耐性の向上を実現する．

提案システムでは，認証用画像を登録する登録フェーズ，認証を実施する認証フェーズの大きく 2 つのフェーズが存在する．次節よりそれぞれのフェーズについて説明する．

3.1 登録フェーズ

(1) 初期登録時に，ユーザは，自身の端末に保存されている画像を認証用画像として 4 枚選択する．

(2) (1)の各選択画像に対し，google 類似画像検索を実施し，検索結果上位 8 枚の画像をダミー用画像として設定する．

3.2 認証フェーズ

認証フェーズは以下 2 つの手順からなる．

(1) 認証実行時にシステム側で認証用画像，ダミー用画像すべてに 5 種類の画像処理をランダムに施す．画像加工のパターンは，グレースケール変換，2 値化変換，ネガポジ変換，スタンドガラス処理，色変換の 5 種類である．

(2) ログイン画面上に(1)で画像処理済みの認証用画像とダミー画像をランダムな並びで 9 枚表示する．ユーザは 9 枚から登録フェーズで登録した認証用画像を選択する．この作業が 4 回繰り返される．本認証の流れを図 1 に示す．ユーザが認証用画像を 4 回連続で選択した場合に認証成功とし，ダミー用画像を 1 回でも選択した場合，認証失敗とする．

4. 評価実験

本章では，提案手法のショルダーハック耐性及び記憶保持性に関する実験とその結果について述べる．

4.1 ショルダーハック耐性の評価実験

提案システムを用いて情報系学部所属大学生 3 名に対し，ショルダーハック耐性の評価実験を行った．

4.1.1 実験手順

被験者は最大 10 回までログイン試行する．なお，ビデオ映像は好きな位置のものを何度でも視聴可能とする．

認証動画は，実験者が提案システムを使いログインしている様子をスマホで撮影したもので，右 90 度，右 45 度，真後ろ，左 45 度，左 90 度の 5 つの位置から撮影した．ログイン画面には 4.2 節で述べる実験被験者 5 名の認証用画像を使用した．認証動画の視聴について，被験者は，好きな位置のものを何度でも視聴可能とする．

†1 Iwate Prefectural University

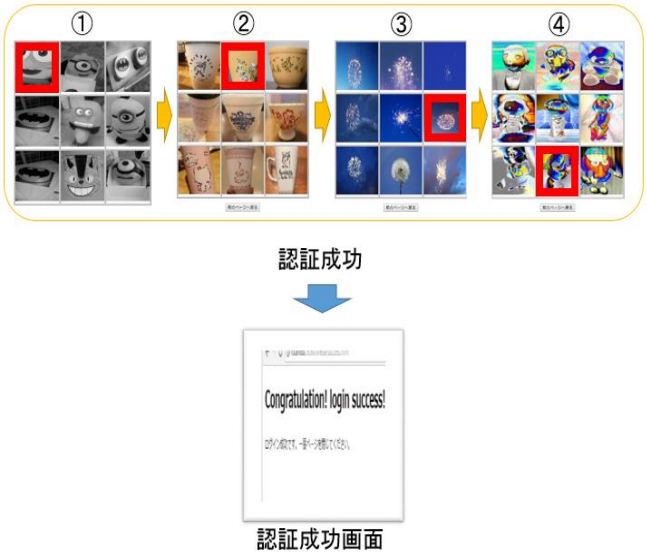

図 1：認証の流れ
（正解時．赤い□が認証用画像）

4.1.2 ショルダーハック耐性の評価実験の結果

3 名中 2 名の被験者がログインに成功した．ログイン成功した 2 名の学生は 4 回目のログインで成功した．また，攻撃者の視聴回数の平均回数は 10.3 回である．

使用した認証画像等の分析の結果，攻撃が成功した場合について，認証用画像とダミー用画像の違いがわかりやすかったことが考えられる．これに対し，画像加工の種類を変える，使用する認証用画像の種類を風景のような違いがでにくい画像に限定するといった改良を行う必要がある．

4.2 記憶保持性に対する実験

提案システムを用いて，情報系学部所属大学生 10 名に対し，記憶保持性の評価実験を行った．

4.2.1 想起性テストの手順

実験は以下の 3 つの手順からなる．

(1)被験者が用意した画像を認証用画像として登録する．

(2)被験者は，回数の制限を設けず実験者側で用意した画像によるログイン画面を使用してログイン成功を 5 回，同様に前述の被験者が用意した画像によるログイン画面を使って，5 回ログイン成功できるまでログイン試行してもらう．

(3)1 日後，2 日後，1 週間後と被験者は，(2)同様にログイン試行する．ただし，ログインの制限回数は関連研究[2]と同様の条件にするため，3 回までとする．

4.2.2 想起性テストの結果

1 日後，2 日後，1 週間後のすべてについて全被験者が 3 回までのログイン試行のうちにログインに成功した．1 日後の試行で，1 名の被験者が二値化画像変換された画像を 1 度間違えたが 2 回目のログイン試行で問題なくログインできた．このことから，1 週間後までは，問題なく記憶保持性が保たれるといえる．

また，実験終了後にアンケートを記入してもらった．表 1 は本システムが文字パスワードと比べて使いやすいかのアンケート結果である．

Q. 文字パスワードと比べて本システムは使いやすかったですか．	
A. とても使いやすかった	1
B. やや使いやすかった	6
C. どちらも変わらなかった	0
D. やや使いにくかった	3
E. とても使いにくかった	0

表 1:文字パスワードと比べたシステムの使いやすさに関するアンケート結果

4.2.3 想起性テストの考察

被験者全員ログイン成功することができた．このことから，1 週間後までは，問題なく記憶保持性が保たれることが分かった．

アンケートの結果から，本システムの使いやすさにおいては文字パスワードより，優位性があると分析した．

また，実験終了後に被験者に意見を伺ったところ，システムの意見として 2 値化変換と色変換した画像が覚えるのが難しいという意見があったので，この画像処理パターンを無くすか，別の画像処理パターンに変えれば，より想起性の向上が見込めると考えられる．

5. まとめ

本研究では，ショルダーハック耐性と記憶保持性を有する認証方式として，ユーザの所有する画像を利用することで記憶保持性を高め，類似画像と画像処理を併用することでショルダーハック耐性を高めることを可能とする類似画像認証手法を提案した．また，評価実験では，提案手法を利用した際，少なくとも 1 週間後までの記憶保持性を達成できることを確認した．ショルダーハック耐性については，今後は，1 か月後まで，記憶保持性が保たれるか調査し，画像加工種類のパターンを変えるといったシステムの改良を行い，ショルダーハックの耐性の向上を試みる予定である．

参考文献

[1] 情報を盗み取る手段「ショルダーハック」とは？ http://asci.jp/elem/000/001/225/1225322/ (最終閲覧日：2017-5-24)

[2] R. Dhamija and A. Perrig: Déjà vu–A User Study: Using Images for Authentication, Proc. of the 9th Conference on USENIX Security Symposium, Vol.9, pp.45-58, 2000.

[3] E. Hayashi, R. Dhamija, N. Christin and A. Perrig: Use Your Illusion: secure authentication usable anywhere, SOUPS '08 Proc. of the 4th symposium on Usable privacy and security, pp. 35-45, 2008.