2022 年 3 月 15 日

報道関係者各位

国立大学法人筑波大学

歪み画像を用いるパスワードシステムを提案
～個人の記憶を活用して盗み見が不可能に～

日常生活において、パスワードによって個人認証をするサービスがたくさんあります。パスワード以外の個人認証システムとして、画像認証を用いるものもありますが、いずれも盗み見の危険性があります。これを防ぐために、これまで覚えづらい画像を用いる個人認証システムがいくつか提案されているものの、スクリーンの録画攻撃を防ぐことは困難です。

そこで本研究では、歪み画像を用いる個人認証システム EYEDi（Estimating Your Encodable Distorted images）を提案しました。これにより、たとえパスワード入力画面を録画されても、盗み見を防ぐことが可能になります。

EYEDi は、ユーザーが用意した画像に画像処理フィルターを適応して歪んだ画像を生成します。ユーザーは、記憶に基づき、多くの歪んだ画像から自分が用意した画像を選択することで個人認証を行います。この歪み画像は元に戻すことができない上、歪みの強度が調整可能なので、元の画像を知っている正規ユーザーのみが判別できます。また、一つの画像から何通りもの歪み画像を生成することができるため、スクリーンを録画されても、盗み見の心配がありません。

本システムの有効性を検証するため、既存手法と EYEDi を用いて、20 名の参加者が、3 種類の攻撃（肩越し撮影、カメラ録画、スクリーン録画）を、それぞれ 300 回実施し、正規ユーザーと攻撃者の分類誤り率を調べたところ、EYEDi の方が優れていることが分かりました。特に、最も深刻な脅威モデルであるスクリーン録画に対する高い防御性能が示され、EYEDi は、スクリーンショット攻撃者の排除に効果的であることが明らかになりました。

研究代表者
筑波大学システム情報系
善甫 啓一　助教

研究の背景

パスワードや暗証番号などの個人認証システムは、今日の IT システムを利用する上で必要不可欠です。この個人認証システムは大きく 3 つに分けられ、金属や IC カードの鍵など「何を持っているか」、文字列（パスワード）や画像など「何を知っているか」、指紋や虹彩など「何者であるか」などによる認証方法が提案されています。このうち、「何者であるか」は、指紋や虹彩などユーザーの生体情報に基づくため、漏洩・複製リスクを考えると、安易に使うことは困難です。また、「何を持っているか」は容易に紛失・複製してしまうことが多く、実際には、パスワードや画像など「何を知っているか」に基づく個人認証が広く使われています。しかし、パスワードは複雑にすれば記憶しておくことが困難であり、画像は盗み見のリスクに対して弱いという問題点がありました。

研究内容と成果

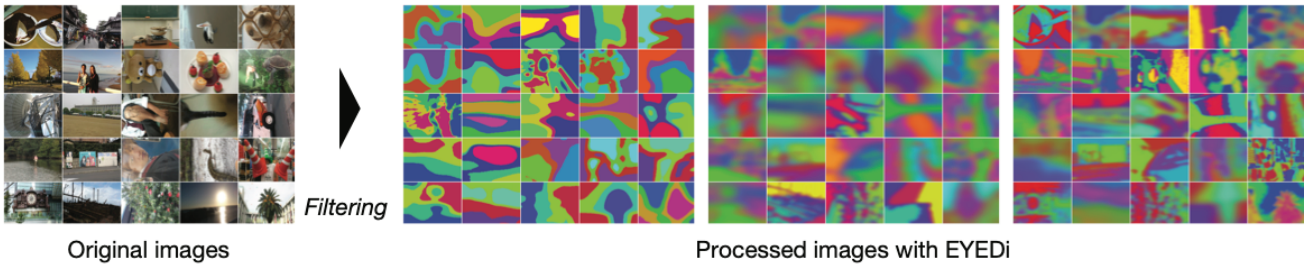
本研究チームは、ユーザーが用意した画像に画像処理フィルターをかけることで、元画像を知っている本人にしか分からない歪み画像を生成し、認証画面で提示する個人認証システム「EYEDi（Estimating Your Encodable Distorted images）」を開発しました。この画像処理フィルターは、歪み強度の調節が可能で、元の画像を知っている正規ユーザーのみが判別できる画像を作ることができます（参考図）。また、この画像処理フィルターは不可逆な処理を行っているため、スクリーンの録画をされても、元の画像に復元することはできません。また、一つの画像から何通りもの歪み画像を生成することができ、フィルターの強度を適切に調節することで、スクリーンを録画されたとしても、盗み見を防止することが可能です。

このシステムの有効性を検証するため、20 名の参加者（IT 機器の操作に慣れている学生など）が攻撃者となって、3 種類の攻撃（肩越し撮影、カメラ録画、スクリーン録画）を、既存手法で用いる覚えづらく工夫した画像パスワードと EYEDi で作成した歪み画像に対して、それぞれ 300 回実施しました。3 種類の攻撃の分類誤り率[注1)]を調べたところ、EYEDi の方が、正規ユーザーと攻撃者を正しく認識する割合が高いことが分かりました。具体的には，盗み見攻撃には 17.3 倍、盗撮攻撃には 10.4 倍、スクリーン録画攻撃には 6.25 倍程度、セキュリティー性能が向上しました。特に、最も深刻な脅威モデルであるスクリーン録画については、既存手法では完全に突破されたのに対し、EYEDi では 10%程度の分類誤り率で攻撃を防ぐことができました。さらに、攻撃者がログインするために要する時間も増加したことから、EYEDi は効果的にスクリーンショット攻撃者を排除できることが明らかになりました。

今後の展開

研究チームは、今後さらに、EYEDi のマルチモーダル化[注2)]や、ユーザー認証にかかる時間の短縮など、より使い勝手の良いシステム開発に取り組みます。

参考図



図：EYEDi によって、本人にしか分からないレベルまで歪ませた画像群

用語解説

注１）　分類誤り率

システムが正規ユーザーを誤って非正規ユーザーと分類してしまいログインできない、あるいは、悪意ある攻撃者（非正規ユーザー）を誤って正規ユーザーと分類してログインさせてしまう割合のこと。

注２）　マルチモーダル化

コンピューターやシステムと人間がやり取りを行う方法を複数にすること。例えば、パスワードに加えて 2 段階認証の要素を加えたり、映像に加えて音響の要素を足すなど。

掲載論文

【題　名】 EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to Prevent Screenshot Attacks
（EYEDi: スクリーンショット攻撃を防止する歪んだ画像を用いる個人認証システム）

【著者名】 Takayuki Kawamura[1], Tadashi Ebihara[2], Naoto Wakatsuki[2], and Keiichi Zempo[2]

[1] 筑波大学 理工情報生命学術院 システム情報工学研究群 知能機能システム学位プログラム

[2] 筑波大学 システム情報系 知能機能工学域

【掲載誌】 IEEE Access

【掲載日】 2022 年 1 月 7 日

【DOI】　10.1109/ACCESS.2021.3138093

問合わせ先

【研究に関すること】

善甫 啓一（ぜんぽ けいいち）

筑波大学 システム情報系 知能機能工学域 助教

URL: http://www.xpercept.aclab.esys.tsukuba.ac.jp

【取材・報道に関すること】

筑波大学広報室

TEL: 029-853-2040

E-mail: kohositu@un.tsukuba.ac.jp