Percepcyjne techniki zabezpieczania danych i weryfikacji użytkowników

mgr inż. Natalia Krzyworzeka

Promotor: dr hab. Lidia Ogiela prof. nadzw.

Dyscyplina: **informatyka**

Postępujący rozwój technologii informacyjnych w niemal wszystkich dziedzinach życia sprawia, że coraz większa ilość danych podlega cyfryzacji. Proces uwierzytelniania dostępu użytkowników do zasobów determinuje zwykle rodzaj chronionej informacji oraz stopień poufności, jaki został jej nadany. Jednym z najczęstszych i najbardziej uciążliwych problemów, z jakim przeciętny użytkownik spotyka się na etapie logowania do systemów, jest problem z zapamiętaniem hasła oraz problem z szybką i skuteczną weryfikacją.

Według badań przeprowadzonych w Stanach Zjednoczonych w 2020 roku przez digitalguardian.com, przeciętny adres mailowy każdego z nas jest powiązany ze średnio 130 personalnymi kontami w różnych aplikacjach [1]. Według securitymagazine.com, bazując na danych z 2017 roku, średnia liczba kont osobistych dla użytkownika biznesowego wynosi natomiast 191 [2]. Pamiętanie tak wielu kombinacji haseł oraz loginów jest niezwykle trudne, a ustawienie takich samych danych logowania dla kilku kont lub nie zmienianie ich przez dłuższy okres czasu, jest naruszeniem podstawowych zasad bezpieczeństwa.

Na podstawie ankiety wykonanej na zlecenie NordPass, 54% mężczyzn i 46% kobiet w Stanach zjednoczonych w przedziale wieku od 25 do 44 lat padło ofiarą ataku hackerskiego [3]. W większości przypadków wynikało to ze zbyt łatwego do złamania hasła. Dostępne od jakiegoś czasu na rynku aplikacje tzw. *Password Manager* służące jako pomoc w logowaniu i uwierzytelnianiu kont oraz przechowujące hasła, są płatne i pomimo zabezpieczeń mogą również stanowić cel ataku.

Najpopularniejszą obecnie komercyjną techniką percepcyjną stosowaną w celu ulepszania zabezpieczeń aplikacji jest CAPTCHA. Wykorzystuje ona zdolność człowieka do intuicyjnej, wzrokowej interpretacji informacji, jak również jego umiejętność

w rozpoznawaniu kształtów i rozumieniu schematów, opartą w dużej mierze na wiedzy oraz doświadczeniu obserwatora. Techniki wizualne są najbardziej popularnymi technikami percepcyjnymi ze względu na fakt, iż postrzeganie i analiza obrazu stanowi niezwykle skomplikowany proces nawet dla wyspecjalizowanych programów komputerowych i wymaga odpowiedniej bazy danych, będąc jednocześnie prostym do realizacji zadaniem dla przeciętnego użytkownika.

Ciągły postęp technologiczny ma istotny wpływ na funkcjonowanie CAPTCHA w przestrzeni internetowej sprawiając, że coraz większa ilość jej schematów jest łamana. Wymusza to w konsekwencji konieczność implementacji coraz trudniejszych, również dla człowieka, zadań percepcyjnych. Granica, przy której rozwiązanie zadania CAPTCHA będzie trudniejsze dla człowieka niż maszyny, może zostać lub została już przekroczona.

W prezentowanej pracy starano się przedstawić najbardziej istotne problemy, z którymi mierzy się w internecie przeciętny użytkownik oraz jak zdolności kognitywne człowieka mogą posłużyć w ich rozwiązaniu. Omówione zostały również mocne i słabe strony technik percepcyjnych. W pracy poświęcono także uwagę temu, jak ciągły rozwój technologiczny może wpłynąć zarówno w pozytywny jak i w negatywny sposób na znane rozwiązania CAPTCHA. Głównym celem pracy są cztery autorskie modele autentykacji: CAPTCHA Password Reminder, CAPTCHA tekstowa, CAPTCHA personalna wykorzystująca dane lokalizacyjne oraz percepcyjny protokół autentykacji. Każde z rozwiązań przedstawia inne wykorzystanie technik percepcyjnych jako elementu zabezpieczeń.

Cel i teza pracy

W niniejszej pracy główną uwagę postanowiono skupić na technikach percepcyjnych wykorzystujących pamięć wzrokową użytkowników oraz na zdolności człowieka do rozpoznawania obiektów na obrazach. Starano się przybliżyć również następujące zagadnieniach z zakresu ochrony danych, tj. trudność w zapamiętaniu przez użytkownika wielu haseł, personalizacja pytania przypominającego, autoryzacja w oparciu o konkretny przedmiot lub lokalizację oraz próba ulepszenia najpopularniejszej techniki służącej odróżnianiu człowieka od komputera, jaką jest CAPTCHA tekstowa.

Głównym celem pracy było udzielenie odpowiedzi na pytanie, czy możliwe jest opracowanie nowych algorytmów wykorzystujących wizualne kody CAPTCHA, a także

technik percepcyjnych do zabezpieczania danych i weryfikacji użytkowników. Tym samym w niniejszej pracy podjęta została próba wykazania następującej tezy badawczej:

„*Możliwe jest opracowanie nowych algorytmów wykorzystujących wizualne kody CAPTCHA, a także technik percepcyjnych do zabezpieczania danych i weryfikacji użytkowników*".

W pracy zostały podjęte następujące cele badań:

1. Opracowanie nowych wizualnych technik weryfikacji użytkowników z zastosowaniem metod transformacji obrazów.
2. Opracowanie metodologii wykorzystania technik percepcyjnych i behawioralnych w procesach weryfikacji użytkowników.
3. Zaproponowanie nowej klasy personalnej CAPTCHA bazującej na pamięci wzrokowej oraz na indywidualnych preferencjach użytkownika.
4. Próba udoskonalenia technik oraz zidentyfikowania słabych stron algorytmów rozpoznawania obrazów na podstawie analizy cech schematów CAPTCHA, wykazujących największą skuteczność podczas procesu implementacji.

Wszystkie omawiane rozwiązania zostały opracowane specjalnie na potrzeby niniejszej pracy jako próba zaproponowania potencjalnych rozwiązań lub możliwych dalszych kierunków rozwoju percepcyjnych techniki zabezpieczania danych i weryfikacji użytkowników. Głównym zadaniem prezentowanych algorytmów jest przetwarzanie obrazów, z uwagi na ten fakt zostały one napisane z użyciem programu Matlab wersja 2010a. Język ten wybrano ze względu na dużą ilość pomocnych funkcji do przetwarzania oraz podglądu plików graficznych. Autorskie funkcje, które posłużyły do stworzenia wspomnianych czterech rozwiązań, wykorzystują m.in. następujące techniki przetwarzania i analizy obrazów: filtrację, segmentację, dylatację oraz erozję kształtów, analizę histogramu, skalowanie obrazu, watermarking, rozpoznawanie konturów oraz inne.

Tworząc programy wzięto pod uwagę nieustanną ewolucję technologii i rozwój algorytmów detekcyjnych. We wszystkich czterech rozwiązaniach starano się uwzględnić przede wszystkim ich praktyczność, łatwość w implementacji oraz intuicyjność w obsłudze, szybkość działania, efektywność i skuteczność, jak również potencjalne szanse na komercyjne zastosowanie.

Struktura pracy

W pierwszych rozdziałach pracy został dokonany m.in. przegląd literaturowy najpopularniejszych modeli CAPTCHA wraz z omówieniem ich wad i zalet. Przedstawione zostały również realne zagrożenia czyhające zarówno na użytkowników, jak i twórców stron internetowych ze strony złośliwego oprogramowania. W kolejnym rozdziale omówione zostały wspomniane wcześniej autorskie modele CAPTCHA. Zaprezentowano również przykładowe algorytmy przedstawiające ich wykorzystanie w praktyce. W dalszej części pracy omówiono sposoby działania nowych metod wraz ze szczegółową charakterystyką ich mocnych i słabych stron, skupiono się również na potencjalnych dalszych kierunkach rozwoju opisanych autorskich modeli CAPTCHA.

Niniejsza rozprawa zawiera 5 głównych rozdziałów. Rozdział pierwszy stanowi wstęp, który wprowadza w tematykę rozprawy oraz obrazuje celowość stosowania CAPTCHA wizualnej w systemach zabezpieczeń. W rozdziale tym przedstawiono także tezę rozprawy doktorskiej.

W rozdziale drugim przedstawiono aktualny stan wiedzy i przegląd literaturowy najpopularniejszych modeli CAPTCHA. Ponadto omówiono wady i zalety każdego z rozwiązań.

Rozdział trzeci został poświęcony zobrazowaniu realnych zagrożeń czyhających zarówno na użytkowników jak i twórców stron internetowych ze strony złośliwego oprogramowania. Ponieważ zagrożenia te wymagają ciągłego podnoszenia jakości zabezpieczeń, podjęta została próba omówienia najlepszych, dostępnych obecnie na rynku implementacji CAPTCHA.

W rozdziale czwartym przedstawiono cztery autorskie modele CAPTCHA. Każdy z nich prezentuje odmienne wykorzystanie technik percepcyjnych jako elementu zabezpieczeń. W rozdziale tym omówione zostały sposoby działania wspomnianych metod wraz ze szczegółową charakterystyką ich mocnych i słabych stron.

Rozdział piąty stanowi podsumowanie pracy, w którym przedstawione zostały otrzymane wyniki, potencjalne zastosowania oraz wskazano dalsze kierunków rozwoju zaproponowanych rozwiązań.

Wyniki badań

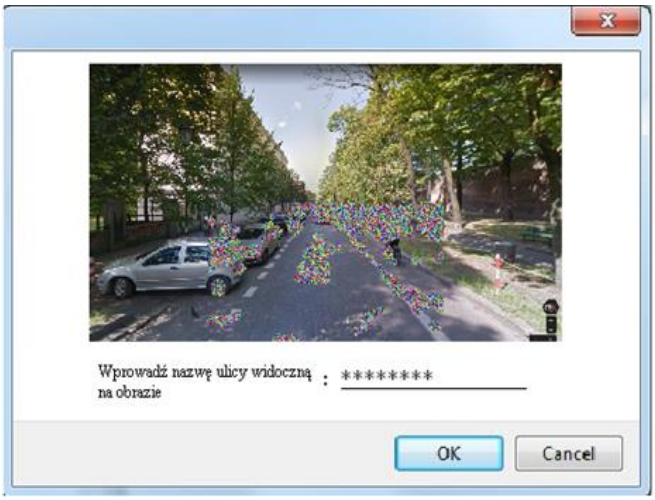
Metody opracowano z nadzieją na ich przyszłe zastosowanie w protokołach autentykacji stron i weryfikacji uprawnionych użytkowników, a także wykorzystanie do zabezpieczania (oznaczania) danych w sposób zbliżony do sposobu działania znaków wodnych. Zaproponowane w rozprawie modele mogą wpłynąć na rozwinięcie niezwykle aktualnej dziedziny, jaką jest informatyka w zakresie zapewniania bezpieczeństwa danych.

Jako pierwszy zaproponowany został program CAPTCHA Password Reminder. Metoda ta uwzględnia wprowadzenie dodatkowego kroku na etapie rejestracji konta. Użytkownik zostaje najpierw poproszony o wgranie lub wylosowanie dowolnego obrazu np. ze zbioru grafiki Google, oraz o udzielenie odpowiedzi na jedno ze standardowych pytań używanych do odzyskiwania konta, np: *podaj imię psa z dzieciństwa*, *jak brzmiało nazwisko panieńskie Twojej matki*, *ulubiona postać z kreskówki*, etc. Po zatwierdzeniu przez aplikację odpowiedzi na pytanie przypominające, jak również po zweryfikowaniu poprawności rozszerzenia i rozmiaru obrazu, algorytm generuje CAPTCHA Password Reminder. Jest to obraz przedstawiający wybraną wcześniej przez użytkownika grafikę wraz z wkomponowanym w nią pytaniem, na które została już uprzednio udzielona odpowiedź. Styl liter pytania przypominającego ma być przedstawiany w formie znaków CAPTCHA, tak aby dodatkowo utrudnić botom ich rozszyfrowanie.

Rysunek 1. Przykładowa implementacja CAPTCHA Password Reminder.

Kolejnym proponowanym rozwiązaniem jest tzw. CAPTCHA personalna wykorzystująca dane lokalizacyjne. W tym rozwiązaniu odniesiono się do bardzo dobrze znanej użytkownikowi informacji, która dla innej przypadkowej osoby mogłaby być niemożliwa do uzyskania. Dzięki niezbywalnej zdolność człowieka do pamiętania miejsc,

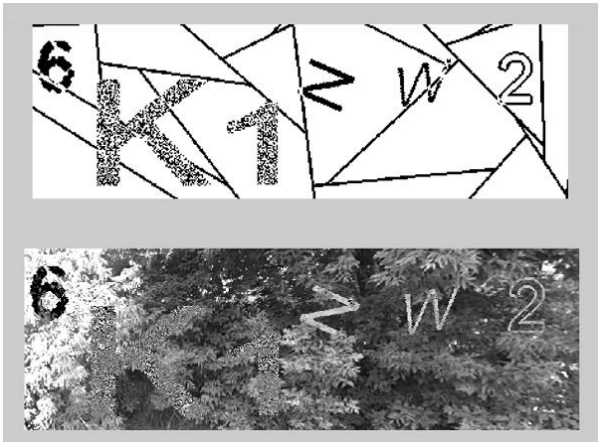
w tym także ulic, szczególnie dla nas ważnych, możliwe jest opracowanie bazy danych, która nie będzie wymagać od użytkownika pamiętania hasła, a mimo to pozwoli pozytywnie przejść weryfikację i zagwarantuje potencjalnie dużą skuteczność (w zależności od doboru ulicy i jej popularności). Opracowany algorytm ma za zadanie głównie przycięcia grafiki do pożądanych rozmiarów oraz usunięcia komputerowo naniesionej przez Google Street View nazwy ulicy przy pomocy algorytmów przetwarzania obrazów.



Rysunek 2. Przykładowa implementacja autorskiego percepcyjnego protokołu autentykacji.

Trzecie z kolei rozwiązanie stanowi autorska CAPTCHA tekstowa. Jest to propozycja tworzenia CAPTCHA w oparciu o równoczesne łączenie kilku różnych metod przetwarzania obrazów. Celem niniejszego rozwiązania jest stworzenie efektywnego i łatwego w interpretacji dla człowieka schematu, będącego równocześnie potencjalnie trudniejszym do złamania w porównaniu do standardowej CAPTCHA. Kombinacja na jednym obrazie kilku liter, wizualnie znacząco różniących się od siebie, ma na celu uniemożliwienie szybkiego rozpoznania każdego ze znaków, jak również zwiększenie szansy na fałszywie ujemne i fałszywie pozytywne detekcje. Do stworzenia CAPTCHA posłużono się tylko jedną wersją liter o konkretnej czcionce, wykorzystano szereg metod przetwarzania obrazów oraz wprowadzono możliwość wstawiania komplementarnego tła, mającego za zadania jeszcze bardziej utrudnić detekcję liter botom.

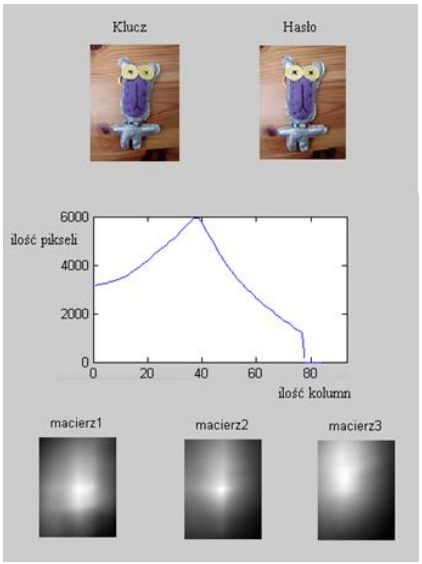
Rysunek 3. Przykładowe działanie autorskiej CAPTCHA tekstowej.



Rysunek 4. Przykładowe działanie autorskiej CAPTCHA tekstowej wraz z automatycznym naniesieniem tła.

Ostatnim opracowanym rozwiązaniem jest nowy percepcyjny protokołu autentykacji. Model ten ma na celu wykrywanie oraz porównywanie obiektów na obrazie ze wzorcem. Opisywany algorytm jest w stanie nadać lub odmówić użytkownikowi autoryzacji na etapie logowania w oparciu o stopień podobieństwa przesłanego zdjęcia do oryginału znajdującego się w bazie danych. Działanie programu opiera się początkowo na wyznaczeniu jak najlepszego dopasowania względem oryginalnego zdjęcia, w tym przeskalowaniu obrazu oraz doborze optymalnego przesunięcia względem osi pionowej i poziomej, a następnie na nadaniu stopnia podobieństwa.

Podobieństwo obiektu do wzorca jest wyznaczane metodą piksel do piksela. W celu uproszczenia obliczeń zdecydowano się nie wykorzystywać korelacji, a jedynie próg zgodności na poziomie wyższym niż 95% wartości składowych macierzy RGB. Głównym zadaniem omawianego rozwiązania jest jego przedstawienie jako kolejnej alternatywy do standardowego procesu logowania.



Rysunek 5. Przykładowy efekt działania percepcyjnego protokołu autentykacji.

Zaproponowane w pracy nowe schematy CAPTCHA działają w oparciu o całkowicie zautomatyzowane algorytmy przetwarzania obrazów. Strona techniczna oparta na kodzie jest stosunkowo prosta i nie wymaga dużej ilości obliczeń (z wyłączeniem percepcyjnego protokołu autentykacji, wykorzystującej standardowe metody korelacji), co daje szanse na utrzymanie płynności w działaniu aplikacji i ich dużą użyteczność rozumianą jako łatwość rozwiązania przez użytkownika konkretnego zadania przy jednoczesnej zwiększonej trudności przełamania kodu przez boty lub inne urządzenia.

Prezentowane w niniejszej pracy modele nie powinny też wymagać częstej wymiany haseł, chyba że na wyraźne życzenie użytkownika. Rozmiar danych przechowywanych na serwerach, potrzebny do ich implementacji, również nie zwiększa się znacząco dla CAPTCHA personalnej wykorzystującej dane lokalizacyjne oraz CAPTCHA tekstowej w odniesieniu do standardowych metod. Przy implementacji CAPTCHA Password Reminder należałoby przeznaczyć jednak kilka dodatkowych MB pamięci na osobę, tak aby można było zachować przesłane przez nią zdjęcia w odpowiedniej jakość. W przypadku percepcyjnego protokołu autentykacji przechowywane informacje miałyby natomiast dotyczyć punktów charakterystycznych tylko tych obiektów, które dany użytkownik ustawił jako swoje aktualne hasło.

CAPTCHA tekstowa stanowi przykład algorytmu, który jest w stanie generować za każdym razem subiektywnie czytelne i pożądane schematy. W praktyce można by dodatkowo zrandomizować lub automatycznie generować bardziej adekwatne tło oraz wprowadzić nowe style liter, jednak otrzymany rezultat działania tej techniki wydaje się być zadowalający.

Kod opracowany do CAPTCHA personalnej wykorzystującej dane lokalizacyjne jest rozwiązaniem prototypowym, a jego główne działanie ogranicza się do usuwania nazwy ulicy z obrazu. Aby w pełni przełożyć ideę proponowanej metody na praktykę, należałoby opracować aplikację będącą w stanie połączyć się zdalnie z losowym podglądem Google Street View® danej ulicy (przynajmniej raz na kilka logowań danego użytkownika), oraz zrobić screen.

Opisany percepcyjny protokół autentykacji ma szansę zostać wykorzystywany przede wszystkim na aplikacjach mobilnych. Rozwój CAPTCHA Password Reminder w przyszłość można rozszerzyć o komercyjne zastosowania, np. jako tło CAPTCHA wprowadzić zdjęcie promowanego produktu i poprosić użytkownika o wkomponowanie jego nazwy w hasło. Takie podejście mogłoby przynieść komercyjny zysk, a w przypadku gdyby produkt był „ukryty" na zdjęciu, wprowadzić dodatkową trudność dla algorytmów deszyfrujących CAPTCHA.

Rozwój technik CAPTCHA wydaje się być nieunikniony, a jedynym wyznacznikiem jego kierunku są dalsze obszary zastosowań. Obecnie CAPTCHA jest wykorzystywana do autoryzacji procesów logowania, ale może być ona także stosowana w procesach zabezpieczania danych. Algorytmy CAPTCHA tekstowej mogą również posłużyć, jak zaprezentowano to w niniejszej pracy, stworzeniu innych algorytmów autentykacji, takich jak CAPTCHA Password Reminder. Ilość haseł, jakie jesteśmy zmuszeni każdego dnia pamiętać wymuszą stosowanie ulepszeń oraz pomocnych rozwiązań w tym zakresie. Omijanie dodatkowych kosztów (płatne aplikacje typu password reminder) oraz unikanie przechowywania danych logowania w miejscach innych niż nasza pamięć, zawsze powinno być jednym z celów tworzenia protokołów autentykacji.

Przypisy:

[1] https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-i-improving-infographic
[2] https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
[3] https://nordpass.com/blog/password-habits-statistics/

Ważniejsze publikacje doktorantki:

1. M.R. Ogiela, **N. Krzyworzeka**, *Heuristic approach for computer-aided lesion detection in mammograms*, Soft Computing, vol. 20 (10), 2016, pp. 4193–4202
2. **N. Krzyworzeka**, *Asymmetric cryptography and trapdoor one- way functions*, Automatyka/Automatics, vol. 20 (2), Wydawnictwa AGH, 2016, pp. 39-51
3. **N. Krzyworzeka**, L. Ogiela, *Security and Understanding Techniques for Visual CAPTCHA Interpretation*, in: Xhafa F. at all (Eds.), Advances on P2P, Parallel, Grid, Cloud and Internet

Computing, Lecture Notes on Data Engineering and Communications Technologies, vol. 13, Springer International Publishing AG, 2018, pp. 277-283

4. **N. Krzyworzeka**, L. Ogiela, *Visual CAPTCHA for Data Understanding and Cognitive Management*, in: Barolli L. at all (Eds.), Advances on Broad-Band Wireless Computing, Communication and Applications, Lecture Notes on Data Engineering and Communications Technologies, vol. 12, Springer International Publishing AG, 2018, pp. 249-255
5. M.R. Ogiela, **N. Krzyworzeka**, L. Ogiela, *Application of knowledge-based cognitive CAPTCHA in Cloud of Things security*, Concurrency and Computation: Practice and Experience, vol. 30 (21), 2018, e4769