UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE
Wydział Matematyki, Fizyki i Informatyki

dr hab. Bogdan Księżopolski, prof. uczelni | Kierownik Katedry Cyberbezpieczeństwa

Lublin, 21.12.2020 r.

Sekretariat Rady Dyscypliny
Informatyka Techniczna i Telekomunikacja

15 -01- 2021
data wpływu

Recenzja rozprawy doktorskiej

Tytuł: Percepcyjne techniki zabezpieczania danych i weryfikacji użytkowników

Autor: mgr inż. Natalia Krzyworzeka

1. **Jaki zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

Rozprawa doktorska dotyczy opracowania nowych algorytmów tworzenia wizualnych kodów oraz metod percepcyjnych służących do uwierzytelnienia użytkownika. Metody te polegają na potwierdzeniu, czy strona, która próbuje uzyskać dostęp do systemu, jest człowiekiem, czy też inteligentnym programem komputerowym (botem). Techniki percepcyjne wykorzystują takie zdolności człowieka, z których naśladowaniem nie są jeszcze w stanie poradzić sobie zaawansowane algorytmy informatyczne. Metody percepcyjne w uwierzytelnieniu stosuje się wszędzie tam, gdzie kluczową cechą metody ma być jej łatwość użycia oraz implementacja. Kluczowym aspektem jest tutaj zachowanie odpowiedniego poziomu bezpieczeństwa.

Autor postawił następującą tezę badawczą: **Możliwe jest opracowanie nowych algorytmów wykorzystujących wizualne kody CAPTCHA, a także technik percepcyjnych do zabezpieczania danych i weryfikacji użytkowników.**

Do zdefiniowanej tezy głównej pracy zaproponowano następujące cele szczegółowe:

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.

Postawiona teza została sformułowana poprawnie, a jej wykazanie implikowało konieczność rozwiązania sformułowanych celów szczegółowych oraz implementacji stosowych rozwiązań o stopniu złożoności adekwatnym do oczekiwanego poziomu prac doktorskich.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczącą o dostatecznej wiedzy autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Analiza źródeł została zawarta w rozdziale 2 oraz 3 rozprawy. W rozdziale 2 Autor wprowadził w tematykę technik kognitywnych stosowanych w zabezpieczeniach. W tej części definiowane są wizualne metody CAPTCHA (ang. Completely Automated Public Turing test to tell Computers and Humans Apart) oraz omawiane są najważniejsze jej modele. W rozdziale 3 poruszona jest tematyka ochrony danych z wykorzystaniem technik percepcyjnych. W tej części zostały zdefiniowane wymagania dotyczące bezpieczeństwa i użyteczności technik percepcyjnych. Zaprezentowany w rozdziałach 2 i 3 stan wiedzy prezentuje kolejno istotne zagadnienia dotyczące zadań badawczych określonych w rozprawie.

Przedłożona rozprawa doktorska obejmuje 63 pozycje bibliograficzne, które reprezentują poruszaną tematykę. Jest ona uporządkowana w kolejności alfabetycznej. Pewną słabością wykonanej analizy są dobrane źródła, ponieważ wśród wybranych prac ponad połowa datowana jest na rok 2010 lub wcześniejszy. Pomimo tego faktu, uważam, że analiza źródeł została wykonana w sposób wystarczający i świadczy o dostatecznej wiedzy Autora o porusza tematyce poruszanej w rozprawie.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**

W mojej ocenie postawiony w pracy problem opracowania nowych algorytmów wykorzystujących wizualne kody CAPTCHA, a także techniki percepcyjne do zabezpieczania danych i weryfikacji użytkowników, został rozwiązany. W pracy zaprezentowano cztery autorskie implementacje nowych modeli CAPCHA opartych o zastosowanie technik percepcyjnych:

1. CAPTCHA Reminder;
2. CAPTCHA personalna wykorzystująca dane lokalizacyjne;
3. CAPTCHA tekstowa;
4. Percepcyjny protokół autentykacji.

CAPTCHA Reminder jest rozwiązaniem, które ma stanowić alternatywną propozycję do aplikacji zarządzającej hasłami (ang. password manager). Głównym celem proponowanego rozwiązania jest ułatwienie użytkownikowi przypomnienia sobie danych logowania, poprzez przedstawienie mu znanego już obrazu, mającego wymusić skojarzenia, które wcześniej sam stworzył. Hasła są dzisiaj wykorzystywane jako najbardziej popularny mechanizm uwierzytelnienia typu „to, co wiesz", jest to spowodowane głównie prostotą ich użycia. Złożoność haseł jest bardzo istotna, ponieważ dzisiaj bardzo popularnymi atakami są ataki typu „słownikowego" oraz ich modyfikacje. Wprowadzanie mechanizmu percepcyjnego w celu zbudowania skojarzenia dla użytkownika dotyczącego hasła, pozwoli użytkownikowi utworzyć bardziej złożone hasło. Metoda odwołuje się do faktu, iż ludzki mózg znacznie lepiej radzi sobie z zapamiętywaniem i kojarzeniem obrazów niż słów. Pewną słabością zaproponowanej metody jest to, że skojarzenia oparte na obrazach będą miały postać wyrazów słownikowych (przykłady s.58 - QuoVadis238Kolejka, HarryPotter2007Horyzont, ImieRozyGory15), które mogą zostać wzbogacone lub połączone cyframi. W takim przypadku entropia hasła będzie niższa niż w przypadku, gdyby hasło nie było zbudowane w oparciu o wyrazy słownikowe.

CAPTCHA personalna wykorzystująca dane lokalizacyjne ma na celu zwiększenie bezpieczeństwa aplikacji na etapie przydzielania dostępu do jej zasobów, nie podnosząc jednocześnie poziomu trudności logowania dla docelowej grupy użytkowników. Proponowane rozwiązanie bazuje na wykorzystaniu pewnej wiedzy dobrze znanej przez użytkownika, która dla

osoby trzeciej będzie trudna do odgadnięcia. W pracy został przedstawiony przykład ulicy jako miejsca, które dobrze zna użytkownik, a które będzie trudne do odgadnięcia przez osoby trzecie. Jest to uwierzytelnienie typu „to co wiesz". Zaproponowany mechanizm zakłada pobieranie obrazu ulicy z Google Street View oraz wymazywanie z tego obrazu nazwy ulicy. W pracy zaproponowano kilka metod wymazywania nazwy ulicy z obrazu i uzyskane efekty są dobre. Sama idea wydaje mi się ciekawa i warta analizy. Zaletą przedstawionego podejścia jest to, że użytkownik w szybki sposób może wykonać weryfikację ulicy oraz to, że w przypadku wybrania znanej ulicy w sposób automatyczny będzie znał jej nazwę. Warto postawić pytanie, czy zaproponowana metoda jest bezpieczna? Czy liczba możliwych kombinacji ulic jest wystarczająca duża, żeby metoda była odporna np. na przeszukiwanie wyczerpujące? Metoda zakłada, że użytkownik sam przysyła obraz ulicy i ulica ta ma nie być blisko miejsca zamieszkania lub miejsca pracy. To słuszne założenie, ale w jaki sposób system będzie weryfikował ten fakt? Słabością zaproponowanej metody jest brak wykonania szerszej analizy bezpieczeństwa.

Trzecim zaproponowanym rozwiązaniem jest **CAPTCHA tekstowa**. Ze względu na sposób implementacji jest to metoda najbardziej popularna na świecie, pomimo faktu, że rozwój algorytmów sztucznej inteligencji znacznie zmniejszył bezpieczeństwo jej użycia. W pracy zaproponowane nowe rozwiązanie, które zakłada łączenie kilku różnych metod przetwarzania obrazów. Zwiększenie trudności opiera się na umieszczeniu na obrazie kilku liter wizualnie znacząco różniących się od siebie, co ma na celu uniemożliwienie szybkiego rozpoznania każdego ze znaków, jak również zwiększenie szansy na fałszywie ujemne i fałszywie pozytywne detekcje. Tworzenie tekstu odbywa się wieloetapowo i zakłada takie operacje jak: losowanie liter i cyfr, losowanie algorytmu przetwarzania, losowanie umieszczenia znaków na obrazie oraz losowe generowanie tła. Dodatkowo zaproponowana metoda została wzbogacona o dodatkowe modyfikacje liter. Wśród nich można wymienić: zaszumienie tekstury, pogrubienie konturu, wykorzystanie różnej skali szarości, efekt cienia, modyfikacja konturu litery oraz erozje szkieletu. Wykorzystane metody tworzenia i modyfikacji tekstu są zgodne z tymi wykorzystywanymi w literaturze i zwiększają bezpieczeństwo rozwiązania. W opisie metod zabrakło mi analizy ilościowej, w jakim stopniu poszczególne modyfikacje wpływają na zwiększenie bezpieczeństwa rozwiązania (poprzez zwiększenie złożoności dla algorytmów rozpoznawania obrazów), przy jednoczesnym zachowaniu wymagań wydajności metody.

Ostatnim zaproponowanym rozwiązaniem jest **percepcyjny protokół autentykacji.** Protokół ten polega na pobraniu od użytkownika hasła w postaci obrazu i zapisanie go w systemie. Proces uwierzytelnienie będzie polegał na tym, że użytkownik zamiast podania klasycznego hasła tekstowego będzie musiał wysłać do systemu obraz, którego poprawność system zweryfikuje. Zaproponowana metoda ma ciekawą cechę, która polega na tym, że wprowadzany jako hasło obraz nie musi być całkowicie zgodny z tym zapisanym w systemie obrazem. Przedstawione rozwiązanie wyznaczona stopień podobieństwa względem oryginalnego obrazu i w przypadku uzyskania odpowiednio wysokiej wartości pozytywnie weryfikuje użytkownika. Głównym zagadnieniem badawczym jest tutaj oszacowanie podobieństwa obrazów oraz określenie, kiedy system będzie przyjmował weryfikacją użytkownika jako pomyślną, a kiedy nie. Zaproponowane rozwiązanie polega 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. W pracy wykonano analizę kilku wybranych przykładów, które ilustrują zaproponowany proces logowania przy pomocy obrazów. Zawarta w pracy analiza potwierdza poprawność zastosowanych metod oraz poprawność działania zaproponowanego rozwiązania. Pewną słabością analizy jest brak wykonania testów, które wykazałyby, jaka jest zależność między modyfikacją przedstawianego do uwierzytelniania obrazu a wskaźnikami false possitive oraz false negative.

4. **Na czym polega problem oryginalności rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?**

Najważniejszym oryginalnym osiągnięciem Autora jest opracowanie czterech nowych modeli CAPCHA opartych o zastosowanie technik percepcyjnych. Omawiane modele nie stanowią kopii istniejących już CAPTCHA, lecz prezentują autorskie podejście do rozwijanych wcześniej zagadnień kognitywnych i sposobów autentykacji opartych o percepcyjne zdolności człowieka.

W przypadku CAPTCHA Reminder oryginalne wkładem Autora jest zaproponowanie mechanizmu, który będzie ułatwiał użytkownikowi przypomnienie danych logowania poprzez przedstawienie mu znanego obrazu, mającego wymusić skojarzenia, które wcześniej sam stworzył. Dzięki takiemu mechanizmowi użytkownik może zastosować bardzie złożone hasło, ponieważ nie będzie miał problemów z przypomnieniem sobie hasła w chwili uwierzytelnienia. Przedstawiona koncepcja jest nowatorska i może stanowić inspirację do dalszych badań w tym zakresie.

Bardzo ciekawym i oryginalnym rozwiązaniem jest utworzenie CAPTCHA personalnej z wykorzystaniem danych lokalizacji. Zaproponowanie obrazu ulic jako typu „to, co wiesz" jest oryginalną koncepcja. Oprócz tego zaproponowane mechanizmy wymazywania nazw ulic działa bardzo dobrze i również jest ważnym wkładem do badań w dziedzinie. CAPTCHA Personalna wykorzystująca dane lokalizacyjne może stanowić alternatywę do tradycyjnie generowane tokena w celu resetowania hasła.

Kolejną propozycją w zestawie zaproponowanych metod percepcyjnych jest CAPTCHA tekstowa. W tym przypadku za oryginalną część rozprawy można uznać liczbę zaproponowanych modyfikacji znaków, które będą stanowić CAPTCHE tekstową. Stosowanie wielu odmiennych stylów transformacji liter do tworzenia schematu CAPTCHA tekstowej nie będzie utrudniało użytkownikowi odczytania informacji, ale będzie stanowić wyzwanie dla algorytmów detekcyjnych.

Ostatnim zaproponowanym rozwiązaniem jest percepcyjny protokół autentykacji. Oryginalnym rozwiązaniem jest zaproponowanie dwuelementowego uwierzytelnienia typu „to, co wiesz" i „to, co masz" opartego na obrazach. Elementem „to, co wiesz", jest tutaj wiedza na temat rodzaju załączonego obrazu (np. zegarek na ręku) oraz elementu „to, co masz", ponieważ w procesie uwierzytelnienia należy przedstawić zdjęcie tego zegarka.

Podsumowując, zaproponowane cztery propozycje stanowią zestaw nowych koncepcji wykorzystania metod percepcyjnych do zabezpieczania danych i weryfikacji użytkowników i można uznać j jako oryginalny wkład autora do dziedziny.

5. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?**

Praca została napisana w języku polskim. Język jest na dobrym poziomie, nie zauważyłem większych problemów językowych. Praca została zredagowana w sposób dobry. Autor wykazał się umiejętnością poprawnego przedstawienia uzyskanych przez siebie wyników. Zaproponowane rozwiązania zostały poprawnie zilustrowane grafikami oraz przykładami. Moim zdaniem poziom redakcyjny rozprawy doktorskiej jest na dobrym poziomie.

6. **Jakie są słabe strony rozprawy i jej główne wady?**

Przedstawione przez Autora wyniki mają duży aspekt praktyczny, inżynierski, co w moim odczuciu jest zaletą pracy. Przy pracach o charakterze praktycznym warto zadbać o weryfikację zaproponowanego system w środowisku rzeczywistym. Według mnie, minusem pracy jest brak przeprowadzenia eksperymentów zaproponowanych rozwiązań dla rzeczywistych odbiorców, czyli potencjalnych użytkowników systemu. W pracy nie znalazłem badań, które określiłyby doświadczenia użytkownika końcowego (ang. user experience), co w przypadku metod percepcyjnych jest bardzo ważne.

Brakuje mi w pracy również ilościowej oceny bezpieczeństwa zaproponowanych rozwiązań. W przypadku metod wizualnych opartych o analizę obrazów, kluczowym aspektem jest ich analiza pod względem odporności na automatyczne algorytmy rozpoznawania obrazów. W pracy można spotkać często stwierdzenia jakościowe, które mówią, że im więcej stosowanych metod modyfikujących obraz, tym większa będzie ich ochrona przeciwko automatycznym algorytmom rozpoznawania obrazów. Po pierwsze, takie stwierdzenie nie zawsze musi być prawdą, a po drugie istotnym elementem jest określenie, jak konkretne modyfikację wpływają na czas wymagany na wykonanie poprawnej analizy obrazu.

Innym aspektem, którego mi zabrakło, to analiza wydajnościowa zaproponowanych rozwiązań. Potencjalne zastosowanie w bieżących systemach jest ściśle związane z wymaganym czasem przetwarzania poszczególnych kroków zaprezentowanych modułów.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Moim zdaniem, zaproponowane rozwiązania mają duży walor praktyczny i wykazują spory potencjał wykorzystania w naukach technicznych. Opracowane nowe wizualne techniki weryfikacji użytkowników z zastosowaniem metod transformacji obrazów są ciekawym wykorzystaniem zagadnień kognitywnych opartych o percepcyjne zdolności człowieka. Innowacyjność rozwiązania oraz potencjał zastosowania w naukach technicznych będzie mógł być lepiej określony, w przypadku, gdy zostanie wykonana szersza analiza zaproponowanych metod, myślę tutaj o porównaniu ilościowym, które określi np. bezpieczeństwo nowej metody, wydajność czy aspekt użyteczności technik przez końcowych użytkowników (UX).

8. Do której z następujących kategorii Recenzent zalicza rozprawę:

a) **nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy,**
b) **wymagająca wprowadzenia poprawek i ponownego recenzowania,**
c) **spełniająca wymagania,**
d) **spełniająca wymagania z wyraźnym nadmiarem,**
e) **wybitnie dobra, zasługująca na wyróżnienie.**

Uważam, że rozprawa doktorska magister inżynier Natalii Krzyworzeki spełnia wymogi stawiane rozprawom doktorskim przez obowiązujące przepisy. Warto podkreślić, że część wyników rozprawy została już opublikowana w literaturze międzynarodowej.