Kraków, 22 czerwca 2015 r.

Prof. dr hab. Wiesław Lubaszewski
Katedra Informatyki, IEiT AGH

Recenzja rozprawy doktorskiej Wioletty Wojtowicz:
Wykorzystanie technik biometrycznych do tworzenia cyfrowych znaków wodnych

Analizowana i stosowana w pracy mgr Wioletty Wójtowicz cyfrowa technologia znaków wodnych stanowi funkcjonalny odpowiednik dwu różnych technologii stosowanych od dawna do papierowego nośnika informacji. Pierwsza z nich to „tajnopis" czyli technologia ukrywania informacji, w taki sposób by informacja właściwa była niewidoczna na nośniku, na który naniesiono także informację widoczną, tj. tekst lub obraz – ukrytą informację właściwą można uwidocznić z pomocą określonego procesu chemicznego. Druga to właściwy znak wodny, czyli informacja widoczna w tle informacji właściwej naniesionej na ten sam nośnik, mająca potwierdzić autentyczność informacji właściwej, np. znak wodny na dokumencie, banknocie itp. Analizowana w pracy cyfrowa technologia znaków wodnych może pełnić obie z wymienionych funkcji, ale od technologii tradycyjnych odróżnia ją trwałość i bezpieczeństwo zapisanej za jej pomocą informacji. Zarówno tajnopis jak i znak wodny są w sposób trwały zintegrowane z nośnikiem, którym jest papier i nie można ich modyfikować lub usunąć bez trwałego, widocznego uszkodzenia nośnika. Natomiast cyfrowy znak wodny jest z założenia zintegrowany z obrazem, gdyż musi być zbudowany z punktów (pikseli), które są umieszczane w tej samej matrycy co obraz opatrywany znakiem wodnym. W rezultacie współczesna technologia cyfrowego znaku wodnego może być zawodna i ma kilka istotnych niedoskonałości, tj.

- nawet przypadkowa modyfikacja obrazu, w który wbudowano znak wodny, np. modyfikacja wprowadzona przez algorytm kompresji stratnej może spowodować nieodwracalne uszkodzenie znaku wodnego – uszkodzenie może uniemożliwić rozpoznanie znaku lub informacji zakodowanej w znaku wodnym,
- znak wodny można wyekstrahować z opatrzonego znakiem obrazu, np. porównując obraz opatrzony znakiem z obrazem oryginalnym – wyekstrahowany znak wodny może być używany niezgodnie z intencją twórcy lub właściciela znaku,
- ukrywanie znaku wodnego przed wzrokiem ludzkim uzależnia rozmiar informacji przekazywanej przez znak wodny – np. punkty (piksele) składowe znaku wodnego staną się niewidoczne dla oka dopiero wtedy, gdy umieścimy je w tych sekcjach obrazu, w których występuje duże zagęszczenie punktów (pikseli).

Wszystkie wymienione niedoskonałości technologii znaków wodnych są omawiane i badane w recenzowanej rozprawie doktorskiej, co pozwala na stwierdzenie, że recenzowana rozprawa aktywnie wpisuje się w szeroki i intensywny nurt badań zmierzających do usunięcia wymienionych niedoskonałości. Innymi słowy, problematyka rozprawy jest ważna i aktualna, a Autorka zajmuje się problemami, które nie znalazły dotąd zadowalającego rozwiązania.

Doktorantka stawia tezę, że *„Możliwe jest opracowanie nowej klasy cyfrowego znakowania obrazów, wykorzystujących personalne cechy biometryczne i gwarantujących integralność danych obrazowych. Algorytmy takie mają istotne zalety w porównaniu z innymi dotychczas powszechnie stosowanymi rozwiązaniami."* (s.5)

Rozprawa składa się ze wstępu, dwu rozdziałów wprowadzających, dwu rozdziałów analitycznych, podsumowania, bibliografii i dwu dodatków.

Rozdziały wprowadzające to: Rozdział 1. **Charakterystyka metod cyfrowego znakowania wodnego**, poświęcony omówieniu technologii cyfrowych znaków wodnych oraz wykorzystaniu technik biometrycznych do tworzenia znaków wodnych oraz Rozdział 2. **State of the art badań nad biometrycznymi znakami wodnymi**, omawiający stan badań nad biometrycznymi znakami wodnymi. Treść obu rozdziałów wprowadzających jest spójna i dobrze sproblematyzowana – tekst pokazuje, że Autorka dobrze rozumie opisywaną problematykę. Tak więc występująca w tytule rozdziału drugiego niefortunna zbitka terminów: angielskiego *State of the Art* i polskiego *stan badań* niepotrzebnie psuje dobre wrażenie.

Rozdziały analityczne tworzą zasadniczą część rozprawy doktorskiej wymagają więc dokładniejszego omówienia. Rozdział 3 **Algorytmy znakowania wodnego wykorzystujące obrazy twarzy do konstrukcji znaków wodnych oraz sieci neuronowe do identyfikacji właścicieli obrazów**. W rozdziale tym Autorka analizuje sytuację, w której znak wodny jest pochodną obrazu, który zostanie opatrzony znakiem wodnym. Materiałową podstawą analizy był opracowany przez AT&T zbiór obrazów twarzy. Mówiąc najogólniej, zawierający 64 punkty (piksele) znak wodny jest ekstrahowany z obrazu za pomocą algorytmów PCA i ERE i jest zapisywany jako wektor 64 punktów (pikseli).
Do badania odporności znaku wodnego Autorka proponuje następującą procedurę. Najpierw wyekstrahowany znak wodny jest integrowany z obrazem z którego został wyekstrahowany. Autorka testuje 5 różnych algorytmów integrujących znak wodny z obrazem. Następnie oznakowany obraz zostaje poddany 5 różnym przekształceniom: skalowanie, obrót, filtrowanie, wycinanie i kompresja. W kolejnym kroku znak wodny zostaje wyekstrahowany z oznakowanego obrazu za pomocą tego samego algorytmu, którego użyto do zintegrowania znaku wodnego z obrazem. Wyekstrahowany znak wodny zostaje ponownie zapisany jako wektor 64 pikseli. W ostatnim kroku rozpoznawalność wyekstrahowanego znaku bada sieć neuronowa. Autorka przeprowadziła dwa eksperymenty służące badaniu rozpoznawalności znaku wodnego. EX1 to eksperyment, w którym danymi treningowymi sieci neuronowej były znaki wodne w postaci oryginalnej, tj. przed integracją z obrazem, a danymi testowymi były znaki wyekstrahowane z obrazów poddanych modyfikacjom. EX2 to eksperyment, w którym danymi treningowymi były znaki wodne wyekstrahowane z oznakowanych obrazów, których nie poddano żadnym modyfikacjom, a danymi testowymi – tak jak poprzednio – były znaki wodne wyekstrahowane z obrazów poddanych modyfikacjom. Oba eksperymenty przeprowadzono odrębnie dla każdego z pięciu opisanych w pracy algorytmów integrujących znak wodny z obrazem. Zbiorcze wyniki testów dla znaków wodnych tworzonych za pomocą algorytmu PCA pokazuje tabela 3.1, a dla znaków tworzonych za pomocą algorytmu ERE tabela 3.2. Testy pokazują, że odporność znaku wodnego, który jest pochodną znakowanego obrazu zależy od sposobu (algorytmu) integracji znaku wodnego z obrazem oraz to, że odporność znaku wodnego zmienia się w zależności od sposobu modyfikacji oznakowanego obrazu. Najgroźniejszą dla znaku wodnego modyfikacją okazało się uszkodzenie obrazu poprzez wycinanie (wycięcie lewej górnej ćwiartki obrazu). Tylko znak wodny zintegrowany z obrazem za pomocą algorytmu oznaczonego w pracy jako A3 okazał się wystarczająco odporny na tego typu uszkodzenie oznakowanego obrazu.

Rozdział 4. **Bimodalny system biometrycznego znakowania wodnego w dziedzinie składowych niezależnych obrazu, oparty na wykorzystaniu obrazów tęczówki oka i odcisku palca** przedstawia wartościowe, oryginalne osiągnięcie Doktorantki. Autorka zakłada, że znacznie większą odporność znaku wodnego powinna zapewnić procedura integrująca z obrazem dwa niezależne od obrazu znaki wodne - istnieje bowiem

prawdopodobieństwo, że w przypadku uszkodzenia oznakowanego obrazu przynajmniej jeden znak wodny pozostanie rozpoznawalny. Podstawą konstrukcji znaku wodnego są tęczówka oka i odcisk palca, a więc cechy biometryczne dobrze identyfikujące osobę. Obrazy danych biometrycznych pochodzą z bazy SDUMLA-HMT. Ze względu na różną naturę danych użytych do tworzenia znaku wodnego Doktorantka stosuje dwie różne procedury. W ich wyniku powstają kod tęczówki i jego maska oraz szkielet odcisku palca z wyróżnionymi punktami swoistymi. Do integracji znaków wodnych ze znakowanym obrazem Autorka stosuje algorytm MR-ICA, zmodyfikowany samodzielnie dla potrzeb pracy z dwoma znakami. Procedura integracji znaku i obrazu polega na stworzeniu 4 miniatur obrazu (256x256 punktów), które są przekształcane w tzw. niezależne komponenty bazowe znakowanego obrazu w taki sposób, że pierwszy jest aproksymacją obrazu oryginalnego a pozostałe reprezentują szczegóły obrazu. Dwa komponenty zostają zintegrowane znakiem wodnym, przy czym Autorka stosuje osobną procedurę dla odcisku palca i osobną dla tęczówki oka. W ostatniej fazie komponenty są scalane w jeden obraz o rozmiarze obrazu oryginalnego. Ekstrakcja znaku wodnego ze znakowanego obrazu jest procesem odwrotnym, na którego wyjściu uzyskujemy kod i maskę tęczówki oraz szkielet odcisku palca. Autorka bada eksperymentalnie odporność znaków wodnych zintegrowanych z obrazem. Procedura przebiega następująco. Najpierw opatrzone znakiem wodnym obrazy są poddawane przekształceniom takim jak: skalowanie, zaszumianie (szum 'salt & peper' oraz szum Gaussa), zamiana górnej ćwiartki na odpowiednią ćwiartkę obrazu oryginalnego, kompresja stratna, redukcja poziomów intensywności punktów (pikseli). Następnie z przekształconego obrazu ekstrahuje się znak wodny, tj. kod i maskę tęczówki oraz szkielet odcisku palca. Wyekstrahowane znaki wodne są porównywane za pomocą stosownych metryk z - przekształconymi do postaci umożliwiającej porównanie - oryginałami z bazy SDUMLA-HMT.

Wynik porównania, które określa odporność znaku wodnego nie jest tak jednoznaczny jak w przypadku eksperymentu z rozdziału 3. Pełne wyniki zamieszczone w dodatku pokazują, że biometryczny znak wodny integrowany z obrazem za pomocą metody MR-ICA jest najmniej odporny na zamianę sekcji obrazu znakowanego oraz na kompresję stratną. Trudno jednak określić jaki rzeczywisty udział w wyniku ma zawodność użytych w badaniu metod porównywania znaku wodnego wyekstrahowanego z oryginałem (dopasowanie), a jaki przekształcenia, którym poddano oznakowany obraz. Zgodnie z założeniem, że wprowadzenie dwu znaków wodnych pozwoli w przypadku uszkodzenia jednego z nich na posłużenie się drugim Autorka wprowadza łączną dla obu znaków wodnych miarę odporności, jest nią ważona suma miar dopasowania obu znaków *Sif*. Można jednak zapytać, czy za proponowana w pracy ważona suma miar dopasowania dobrze określa odporność znaków wodnych. Bowiem jeśli, jak np. w tabeli 4.1. stopień błędu rozpoznania znaku wodnego przy wycięciu fragmentu wynosi dla *Sf* 11.16 i dla *Si* 7.47, to wartość ważonej sumy miar dopasowania *Sfi* równa 1.99 wydaje się zbyt optymistyczna. Jest to jednak pytanie czysto techniczne, które w żaden sposób nie umniejsza oryginalnego osiągnięcia Doktorantki.

Podsumowując mogę z całym przekonaniem stwierdzić, że praca mgr Wioletty Wójtowicz z naddatkiem spełnia wymagania ustawowo i zwyczajowo stawiane rozprawom doktorskim. Wnoszę więc o dopuszczenie mgr Wioletty Wójtowicz do dalszych etapów przewodu doktorskiego.