Akademia Górniczo-Hutnicza
im. Stanisława Staszica
w Krakowie

Wydział Elektrotechniki, Automatyki, Informatyki
i Inżynierii Biomedycznej

AUTOREFERAT
ROZPRAWY DOKTORSKIEJ

Wykorzystanie technik biometrycznych do tworzenia cyfrowych znaków wodnych

Wioletta Wójtowicz

Promotor
prof. dr hab. Marek R Ogiela

Kraków 2015

1. Cele i teza pracy

Temtayką rozprawy doktorskiej i przedmiotem realizowanych badań było opracowanie nowych rozwiązań w dziedzinie biometrycznego znakowania wodnego obrazów cyfrowych, które polegało na zastosowaniu zindywidualizowanych (opartych na cechach biometrycznych) znaków wodnych. Uzasadnieniem celowości podjęcia takiej tematyki jest zarówno potrzeba zapewniania bezpieczeństwa danych cyfrowych, które ze względu na powszechny dostęp do komputerów mogą być łatwo kopiowane i rozpowszechniane bez wiedzy właściciela, jak i niedoskonałości tradycyjnych znaków wodnych. Podstawową wadą konwencjonalnych znaków wodnych, zwykle w postaci sekwencji binarnych, obrazów, logotypów lub tekstu, jest brak unikalności, co sprawia, że po detekcji znaku nawet nieuprawnione osoby mogą korzystać z obrazów niemalże na prawach właścicieli ([2]). W związku z tym obecnie dąży się do zindywidualizowania informacji zawartej w znakach wodnych, w czym bardzo pomocne okazują się techniki biometryczne ze względu ich zdolność do odróżniania uprawnionych użytkowników od osób, które się tylko za takie podają ([5]). Rozwijane metody tzw. biometrycznego znakowania wodnego charakteryzują się tym, że znaki wodne umieszczane w obrazach są konstruowane na podstawie cech biometrycznych właścicieli tych obrazów. Z tego powodu po ekstrakcji umożliwiają one zidentyfikowanie legalnych użytkowników i mogą być wykorzystane do uwierzytelniania obrazów. Metody te mają na celu wykorzystanie biometrycznych identyfikatorów w zastosowaniach klasycznych i odpornych algorytmów cyfrowego znakowania wodnego w takich obszarach jak ochrona praw autorskich i zapewnianie bezpiecznej transmisji obrazów cyfrowych. W związku z powyższym sformułowano następującą tezę rozprawy doktorskiej:
Możliwe jest opracowanie nowej klasy algorytmów 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.

Uzasadnieniem podejmowanej w pracy tematyki badań oraz sformułowania tezy pracy jest argumentacja przemawiająca za dużym potencjałem wykorzystania biometrii w systemach zapewniania bezpieczeństwa danych, ale także niedoskonałości zaproponowanych

dotychczas rozwiązań w dziedzinie biometrycznego znakowania wodnego. Dokładniej, analiza aktualnego stanu wiedzy w tym obszarze pozwoliła na rozpoznanie słabych stron istniejących algorytmów znakowania wodnego opartych na wykorzystaniu pojedynczych identyfikatorów biometrycznych. Możliwe było również zidentyfikowanie perspektywicznego kierunku rozwoju tego typu metod, który dotyczy koncepcji wielomodalnego znakowania wodnego.

Podstawową wadą opracowanych do tej pory i opisanych w literaturze algorytmów związanych z umieszczaniem pojedynczych identyfikatorów biometrycznych w neutralnych obrazach cyfrowych np. [11, 12, 13] jest fakt, że często pomija się w nich etap ewaluacji danych biometrycznych po ekstrakcji. W większości zaproponowanych algorytmów dokonuje się jedynie porównania danych wyekstrahowanych z ich oryginalnymi wersjami, używając często stosowanych w konwencjonalnym znakowaniu wodnym miar takich jak np. współczynnik korelacji. Jednak wyniki takiej analizy nie dostarczają informacji o użyteczności wyekstrahowanych znaków wodnych w uwierzytelnianiu osób, które wymaga porównania tych danych z całą bazą danych biometrycznych. Przeprowadzenie takich badań pozwalałoby także na kompleksowe porównywanie różnych metod biometrycznego znakowania wodnego, wykorzystujących alternatywne reprezentacje biometryk lub różne algorytmy znakowania wodnego.

Kolejnym istotnym zagadnieniem w biometrycznym znakowaniu wodnym i występującym także w tradycyjnych systemach biometrycznych jest fakt, że stosowanie tylko jednego identyfikatora może prowadzić do dużych błędów rozpoznania. W znakowaniu wodnym obrazów cyfrowych jest to szczególnie ważne, ponieważ algorytmy te bazują na operacjach przetwarzania obrazów, które mimo iż są odwracalne, to jednak powodują, że wydobyte dane rzadko są identyczne z ich oryginalnymi wersjami. Rozwiązaniem tego typu problemu może być stosowanie więcej niż jednego identyfikatora biometrycznego jako znaku wodnego [4, 7, 8]. Jednak to podejście pociąga za sobą stawianie wyższych wymagań algorytmom znakowania wodnego oraz rozważanie różnych scenariuszy biometrycznych (wybór odpowiedniej kombinacji cech, reprezentacji biometryk, sposobu łączenia informacji

dostarczanych przez biometryki). W konsekwencji wykazanie tezy doktoratu sprowadzono do realizacji dwóch celów pracy:

- *włączenie pojedynczych biometrycznych znaków wodnych do istniejących algorytmów znakowania wodnego, bazujących na wykorzystaniu jednego znaku wodnego, i porównanie tych algorytmów pod kątem skuteczności identyfikacji właściciela obrazu opartej na znakach wodnych po ekstrakcji;*
- *opracowanie nowego wielomodalnego algorytmu znakowania wodnego, który pozwoli na umieszczanie dwóch biometryk jednocześnie i przeprowadzenie weryfikacji biometrycznej właściciela obrazu, w oparciu o fuzję informacji dostarczanych przez te biometryki.*

2. Zawartość rozprawy i uzyskane wyniki

Rozprawa doktorska została podzielona na pięć rozdziałów, których zawartość przedstawia się następująco:

Rozdział 1 zawiera wprowadzenie do technologii znakowania wodnego oraz zastosowań technik biometrycznych w systemach bezpieczeństwa, ze szczególnym uwzględnieniem metod włączania biometrii do współczesnych algorytmów znakowania wodnego w celu podnoszenia bezpieczeństwa biometryk jak i dowolnych neutralnych obrazów.

Rozdział 2 zawiera przegląd zaproponowanych dotychczas rozwiązań w dziedzinie ukrywania danych biometrycznych w obrazach cyfrowych. Początki tej dziedziny badań związane są głównie z wykorzystaniem znakowania wodnego do zabezpieczania obrazów biometrycznych stosowanych w tradycyjnych systemach biometrycznych. Z czasem jednak zaczęły pojawiać się również propozycje rozwiązań, w których biometryczne znaki wodne wypierały te konwencjonalne w zastosowaniach związanych z ochroną praw autorskich dowolnych obrazów cyfrowych.

W **rozdziale 3** pracy zaprezentowano badania, które polegały na włączeniu biometrycznych znaków wodnych opartych na wykorzystaniu biometryki twarzy do kilku istniejących algorytmów znakowania wodnego, reprezentujących najbardziej popularne w literaturze naukowej podejścia. Badanie to miało na celu pokazanie jak można łączyć istniejące algorytmy znakowania wodnego z technikami biometrycznymi oraz dokonanie

porównania tych algorytmów biorąc pod uwagę użyteczność wydobytych z obrazów biometryk.

Do konstrukcji znaków wodnych wykorzystane zostały metody rozpoznawania twarzy oparte na uczeniu maszynowym ([1]), tj. *analiza składowych głównych* (*Principal Component Analysis*, PCA) oraz *metoda normowania i ekstrakcji cech własnych* (*Eigenfeature Regulaization and Extraction*, ERE, [6]), które umożliwiły wyznaczenie wektorowej reprezentacji obrazów twarzy o możliwie najmniejszym rozmiarze, nie tracąc przy tym istotnych z punktu widzenia klasyfikacji informacji zawartych w tych obrazach. Wykorzystanie metod uczenia maszynowego do znalezienia odpowiedniej reprezentacji obrazów twarzy wynikało z faktu, że identyfikacja osób na podstawie otrzymanych reprezentacji danych jest szybsza i skuteczniejsza niż gdyby analizowano obrazy lub wektory bez redukcji wymiarowości. Ponadto, wykorzystanie zredukowanej reprezentacji obrazów twarzy jako znaków wodnych wprowadza mniejsze zmiany w obrazie oryginalnym, a ukrywany znak wodny jest bardziej niewidoczny.

Następnie wektory twarzy były umieszczane w obrazach cyfrowych przy użyciu kilku algorytmów znakowania wodnego działających w dziedzinie przestrzennej i dziedzinie transformat, tj. DFT, DCT oraz DWT. Po ekstrakcji znaków wodnych dokonano porównania tych algorytmów w oparciu o wyniki identyfikacji biometrycznej przeprowadzonej za pomocą zbudowanej na potrzeby eksperymentu sieci neuronowej typu *feedforward*, która dla podanego na wejściu wektora (wyekstrahowanego znaku wodnego) zwracała identyfikator rozpoznanej osoby. Wykorzystanie stosunkowo krótkich wektorów reprezentujących poszczególne twarze sprawiło, że zarówno trenowanie jaki i testowanie sieci przebiegło szybko, a ponieważ zbiory treningowe i testowe były rozłączne, parametry sieci były każdorazowo wyznaczane niezależnie od danych, które stanowiły późniejsze zapytania.

Otrzymane wyniki symulacji pozwoliły odpowiedzieć na kilka pytań dotyczących najlepszej metody konstrukcji znaku wodnego (metoda ERE), najodporniejszego algorytmu spośród tych testowanych (algorytm oparty na wykorzystaniu transformaty DCT) oraz doboru parametrów sieci.

Zaprezentowane w tym rozdziale pracy podejście do wykorzystania biometrycznych metod

identyfikacji w algorytmach znakowania wodnego potwierdza, że pierwszy z celów szczegółowych pracy, którym była propozycja włączenia biometrycznych znaków wodnych do istniejących algorytmów znakowania wodnego i porównanie tych algorytmów pod kątem skuteczności identyfikacji właścicieli obrazów, został osiągnięty.

W **rozdziale 4** zaprezentowano opracowany przez autorkę pracy algorytm biometrycznego znakowania wodnego działający w *dziedzinie składowych niezależnych* obrazu (*Independent Component Analysis*, ICA, [3]). Algorytm ten umożliwia umieszczenie w obrazie dwóch niewidocznych i niezależnych znaków wodnych zawierających identyfikatory biometryczne, tj. obraz odcisku palca i kod tęczówki oka. Zaproponowana procedura polega na obliczeniu czterech niezależnych komponentów bazowych obrazu oryginalnego i wybraniu dwóch spośród nich do umieszczenia znaków wodnych. Komponent będący aproksymacją obrazu oryginalnego jest łączony z zakodowanym obrazem odcisku palca. Z kolei w jednym z komponentów zawierających szczegóły obrazu za pomocą metody kwantyzacji pikseli został umieszczony binarny znak wodny zawierający kod tęczówki i jej maskę. Wybór akurat tej dziedziny znakowania wodnego był podyktowany jej ciekawymi właściwościami, głównie niezależnością otrzymywanych komponentów bazowych, które stwarzały możliwość ukrycia w nich w sposób niewidoczny więcej niż jednego znaku wodnego. W związku z tym procedurę osadzania znaków wodnych dostosowano do własności otrzymanych komponentów bazowych, tj. do bardziej odpornego komponentu wstawiany jest cały obraz odcisku palca, podczas gdy w mniej odpornym komponencie, zawierającym tylko szczegóły obrazu, umieszczono mniejszy i prostszy znak wodny.
W części eksperymentalnej rozdziału omówione zostały poszczególne etapy działania algorytmu oraz dobór parametrów. Celem przeprowadzonych eksperymentów było zbadanie wpływu procedury znakowania wodnego na jakość i użyteczność wydobytych danych biometrycznych, w tym także w scenariuszach uwzględniających ataki kryptoanalityczne. Kluczowym zadaniem w prezentowaniu funkcjonalności algorytmu było wykazanie jak duży wpływ na minimalizację błędów weryfikacji użytkowników ma wykorzystanie informacji dostarczanych przez obydwie biometryki jednocześnie. W tym celu przeprowadzono procedurę weryfikacji biometrycznej opartą na wspólnej mierze dopasowania będącej sumą

ważoną miar dopasowania dla poszczególnych biometryk, a otrzymane wartości porównano z wynikami dla biometryk rozważanych osobno. Zgodnie z oczekiwaniami zaobserwowano, że podejmowanie decyzji dotyczącej rozpoznania na podstawie połączonych miar dopasowania znacznie zmniejsza wpływ ataków na wyniki weryfikacji.

Główną zaletą proponowanego algorytmu jest fakt, że ponieważ obydwa biometryczne znaki wodne mają różne reprezentacje i są wstawiane do niezależnych komponentów, procedura znakowania wodnego (z atakami lub bez) w różnym stopniu wpływała na te znaki. Ma to szczególne znaczenie z uwagi na fakt, że nawet jeżeli jakość jednego ze znaków wodnych ulegała znacznemu pogorszeniu, to dobre wyniki weryfikacji mogły być osiągane dla drugiego znaku wodnego. Ponadto, w proponowanym algorytmie do przeprowadzenia weryfikacji nie potrzebne są oryginalne znaki wodne tylko pobrane od użytkowników próbki obu biometryk, które o ile tylko będą wystarczająco podobne do wyekstrahowanych danych (w terminach biometrycznych progów tolerancji) mogą zapewnić skuteczną weryfikację.

Zaproponowany w tym rozdziale pracy algorytm bimodalnego znakowania wodnego stanowi nową i ciekawą propozycję rozwiązania, w którym wykorzystując zalety systemów wielomodalnych udało się nie tylko podnieść skuteczność weryfikacji użytkowników obrazów, ale także uodpornić system na ataki oraz poprawić jego bezpieczeństwo. Otrzymane wyniki eksperymentów pozwalają wnioskować, iż zaproponowana metoda nie tylko nie prowadzi do istotnego pogorszenia wyników weryfikacji, ale także czyni system bardziej odpornym na słabszą jakość niektórych wydobywanych biometryk. Zaprezentowany algorytm oraz wyniki związane z jego testowaniem potwierdzają, że drugi z celów szczegółowych pracy, którym było opracowanie algorytmu biometrycznego znakowania wodnego pozwalającego na wykorzystanie więcej niż jednej biometryki, został osiągnięty i zgodnie z oczekiwaniami fuzja biometryk wpłynęła korzystnie na osiągnięte wyniki związane ze skutecznością uwierzytelniania użytkowników obrazów.

Rozdział 5 zawiera podsumowanie najistotniejszych wyników zawartych w rozprawie. Poza wnioskami końcowymi dotyczącymi zrealizowanego celu pracy zawarto w nim również perspektywy dalszych badań.

3. Oryginalne wyniki rozprawy

Podejmowane w rozprawie problemy badawcze wynikały z dostrzeżenia pewnych niedoskonałości istniejących rozwiązań w obszarze biometrycznego znakowania wodnego, które w ocenie autorki pracy, albo wymagały ulepszeń, albo stanowiły nowy ciekawy kierunek rozwoju tego typu metod. Jeżeli chodzi o znakowanie wodne za pomocą pojedynczych identyfikatorów, to zwrócono uwagę na możliwość unowocześnienia istniejących algorytmów znakowania wodnego poprzez zastosowanie w nich biometrycznych znaków wodnych oraz zaproponowano metodę ewaluacji takich systemów. W związku z tym w rozdziale 3 rozprawy zaprezentowano badanie, w których przetestowano i porównano kilka algorytmów znakowania wodnego po włączeniu do nich technik biometrycznych związanych z rozpoznawaniem twarzy. Z kolei w dziedzinie wielomodalnego znakowania wodnego, w rozwój której wkład jest obecnie zdecydowanie zbyt mały, zaproponowano nowy algorytm bimodalnego znakowania wodnego, którego szczegóły i zalety zaprezentowano w rozdziale 4 pracy.

Podsumowując realizację nakreślonych we wstępie rozprawy celów i wykazanie tezy doktoratu do najistotniejszych oryginalnych osiągnięć pracy można zaliczyć:

- przeprowadzenie badań porównawczych kilku wybranych algorytmów znakowania wodnego pod kątem skuteczności identyfikacji właścicieli obrazów po włączeniu do nich biometrycznych znaków wodnych;
- wykorzystanie metody ERE do konstrukcji znaków wodnych opartych na biometryce twarzy jako alternatywy dla stosowanej dotychczas w biometrycznym znakowaniu wodnym metody PCA;
- opracowanie nowego algorytmu bimodalnego znakowania wodnego oraz metody jego ewaluacji;
- wykorzystanie w opracowanym algorytmie bimodalnego znakowania wodnego dziedziny składowych niezależnych obrazu, która nie była dotychczas stosowana w biometrycznym znakowaniu wodnym;
- przetestowanie znanych procedur biometrycznych na danych z nowej multimodalnej bazy danych biometrycznych SDUMLA-HMT.

4. Podsumowanie

Problematyka podjęta w rozprawie doktorskiej dotyczyła zagadnień związanych z metodami biometrycznego znakowania wodnego obrazów cyfrowych, które polegają na zastępowaniu konwencjonalnych znaków wodnych identyfikatorami biometrycznymi. Zawartości znaków wodnych poświęca się ostatnio coraz więcej uwagi, ponieważ od postaci i wiarygodności danych ukrywanych w znakach wodnych może zależeć skuteczność algorytmów znakowania wodnego. W szczególności dąży się do zindywidualizowania informacji zawartej w tych znakach tak, aby samo wydobycie znaku wodnego przez nieuprawnionego użytkownika nie umożliwiało mu jeszcze korzystania z obrazu na prawach właściciela. W związku z tym znaki wodne, które zawierają identyfikatory biometryczne wydają się być dobrą alternatywą dla rozwiązań konwencjonalnych, ponieważ pozwalają stwierdzać czy aktualny użytkownik jest właścicielem obrazu (posiada prawa autorskie) lub przynajmniej czy korzysta z niego legalnie. Z drugiej strony wykorzystywanie takich spersonalizowanych znaków wodnych pociąga za sobą konieczność ewaluacji algorytmów znakowania wodnego, pod kątem wykorzystania wydobytych danych do rozpoznawania właścicieli obrazów. Podczas ewaluacji algorytmów biometrycznego znakowania wodnego należy sprawdzić jak przetwarzanie obrazów związane ze znakowaniem wodnym wpływa na zmiany poziomu błędów rozpoznania wyznaczonych na podstawie surowych danych biometrycznych. W proponowanym podejściu nie bez znaczenia jest też fakt, że porównywanie danych wyekstrahowanych z całą bazą danych biometrycznych, pozwala bardziej tolerancyjnie spojrzeć na wymagania stawiane algorytmom znakowania wodnego. Wynika to z faktu, że nawet jeżeli jakość wydobytego z obrazu znaku wodnego ulegnie pogorszeniu to, o ile tylko będzie można wyekstrahować z niego istotne z punktu widzenia rozpoznania cechy, nadal będzie on wartościowym źródłem informacji.

Bibliografia

[1] Bishop, C.M., *Pattern recognition and machine learning*, Springer-Verlang, New York, 2006.

[2] Cox, I.J., Miller, M.L., Bloom, J., Fridrich, J., Kalker, J., *Digital watermarking and steganography*, Morgan Kaufmann Publishers, Burlington MA, USA, 2008.

[3] Hajisami, A., Hosseini, S.N., "Application of ICA in Watermarking," *Mithun Das Gupta (Ed.), Watermarking - Volume 1*, InTech, 2012.

[4] Inamdar, V., Rege, P., "Dual watermarking technique with multiple biometric watermarks," *Sadhana*, 39(1): 3–36, 2014.

[5] Jain, A.K., Flynn, P., Ross, A., *Handbook of Biometrics*, Springer, New York, 2008.

[6] Jiang, X., Mandal, B., Kot, A., "Eigenfeature Regularization and Extraction in Face Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence* , 30(3): 383–394, 2008.

[7] Paunwala, M., Patnaik, S., "Biometric template protection with DCT-based watermarking," *Machine Vision and Applications*, 25: 263–275, 2014.

[8] Qi, M., Lu, Y., Du, N., Zhang, Y., Wang, Ch., Kong, J., "A novel image hiding approach based on correlation analysis for secure multimodal biometrics," *Journal of Network and Computer Applications*, 33(3): 247–257, 2010.

[9] Wioletta Wójtowicz, Marek R. Ogiela, "Security issues on digital watermarking algorithms," *Annales Universitatis Mariae Curie-Skłodowska. Sectio AI, Informatica*, 12(4): 123–139, 2012.

[10] Wioletta Wójtowicz, "An introduction to watermarking of medical images," *Bio-Algorithms and Med-Systems*, 9(1): 9–16, 2013.

[11] Wioletta Wójtowicz, "Biometric watermarking for medical images - example of iris code," *Technical Transactions, Mechanics* 1-M(5): 409–416, 2013.

[12] Wioletta Wójtowicz, "Biometric watermarking for security enhancement in digital images," *Challenges of Modern Technology*, 4(4): 7-11, 2013.

[13] Wioletta Wójtowicz, "A Fingerprint-Based Digital Images Watermarking for Identity Authentication," *Annales UMCS Informatica AI IX*, 1: 85–96, 2014. DOI: 10.2478/umcsinfo-2014-0008.

[14] Wioletta Wójtowicz, Marek R. Ogiela, "Biometric watermarks based on face recognition methods for authentication of digital images," *Security Comm. Networks*, 2014. DOI: 10.1002/sec.1114.