

Politechnika Łódzka
Wydział Fizyki Technicznej, Informatyki
i Matematyki Stosowanej
Instytut Informatyki

Dariusz Puchała

AUTOREFERAT

Załącznik 2
do wniosku o przeprowadzenie
postępowania habilitacyjnego

Łódź, 2017

Łódź, dn. 28.12.2017 r.

dr inż. Dariusz Puchała
Politechnika Łódzka
Wydział Fizyki Technicznej,
Informatyki i Matematyki Stosowanej
Instytut Informatyki
ul. Wólczańska 215
90-924 Łódź

AUTOREFERAT

1. IMIĘ I NAZWISKO: Dariusz Puchała.

2. POSIADANE DYPLOMY, STOPNIE NAUKOWE – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytuł rozprawy doktorskiej:

- 2008 r.: stopień doktora nauk technicznych w dyscyplinie informatyka nadany uchwałą Rady Wydziału Fizyki Technicznej, Informatyki i Matematyki Stosowanej z dn. 01.07.2008 r. Tytuł rozprawy doktorskiej: „Szybkie algorytmy adaptacyjne przekształceń trygonometrycznych”,
- 2001 r.: tytuł magistra inżyniera informatyki uzyskany na Wydziale Fizyki Technicznej, Informatyki i Matematyki Stosowanej, w Instytucie Informatyki w dniu 10.09.2001 r. Tytuł pracy magisterskiej: „Kompresja obrazów medycznych metodą modulowanych przekształceń”,

pozostałe:

- 2002 r.: dyplom ukończenia Studium Doskonalenia Pedagogicznego, Politechnika Łódzka.

3. INFORMACJE O DOTYCHCZASOWYCH ZATRUDNIENIACH W JEDNOSTKACH NAUKOWYCH:

- od 2009 r.: adiunkt w Instytucie Informatyki, Wydział Fizyki Technicznej, Informatyki i Matematyki Stosowanej, Politechnika Łódzka,

- 2001-2009: asystent w Instytucie Informatyki, Wydział Fizyki Technicznej, Informatyki i Matematyki Stosowanej, Politechnika Łódzka,
- maj-wrzesień 2001 r.: stypendysta w Instytucie Informatyki, Wydział Fizyki Technicznej, Informatyki i Matematyki Stosowanej, Politechnika Łódzka.

4. WSKAZANIE OSIĄGNIĘCIA NAUKOWEGO wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuk i (Dz. U. 2016 r. poz. 882 ze zm. w Dz. U. z 2016 r. poz. 1311.).

4.1. Tytuł osiągnięcia naukowego (habilitacyjnego):

Szybkie liniowe przekształcenia parametryzowane. Struktury obliczeniowe i techniki adaptacji.

4.2. Jednotematyczny cykl publikacji

Moim głównym osiągnięciem naukowym są wyniki uzyskane w dziedzinie szybkich adaptacyjnych algorytmów obliczania przekształceń liniowych oraz związanych z nimi zagadnień optymalizacyjnych. Zostały one opublikowane w jednotematycznym cyklu artykułów naukowych, który obejmuje 9 prac naukowych wydawanych w języku polskim i angielskim w latach 2010-2017. W skład cyklu wchodzi:

- 1 monografia naukowa,
- 6 publikacji w czasopismach z listy Ministerstwa Nauki i Szkolnictwa Wyższego (MNiSW), w tym 4 z listy Journal Citations Report (JCR),
- 1 referat konferencyjny opublikowany w serii Springer Series in Advanced Intelligent Systems and Computing,
- 1 referat konferencyjny.

4.2.1. Monografia naukowa

[M] Puchala D., *Szybkie liniowe przekształcenia parametryzowane. Struktury obliczeniowe i techniki adaptacji*, (2017), Akademicka Oficyna Wydawnicza EXIT, Warszawa, Recenzent: prof. dr. hab. inż. Sławomir Wiak.

4.2.2. Publikacje w czasopismach z listy MNiSW (uszeregowane względem punktacji)

[A.1] Puchala D., *Approximating the KLT by Maximizing the Sum of Fourth-Order Moments*, (2013), Signal Processing Letters IEEE, tom 20, nr 3, str. 193-196.

[A.2] Puchala D., Yatsymirskyy, *Joint Compression And Encryption of Visual Data Using Orthogonal Parametric Transforms*, (2016), Bulletin of the Polish Academy of Sciences - Technical Sciences, tom 64, nr 2, str. 373-382.

[A.3] Puchala D., Yatsymirskyy M., *Fast Parametrized Biorthogonal Transforms*, (2012), Przegląd Elektrotechniczny, tom R. 88, nr 4a, str. 123-125.

[A.4] Puchala D., Yatsymirskyy M., *Fast Parametrized Biorthogonal Transforms with Normalized Basis Vectors*, (2013), Przegląd Elektrotechniczny, tom R. 89, nr 3a, str. 277-279.

[A.5] Puchala D., *Comparison of Selected Fast Orthogonal Parametric Transforms In Data Encryption*, (2015), Journal of Applied Computer Science, tom 23, nr 2, str. 55-68.

[A.6] Puchala D., Yatsymirskyy M., *Fast Neural Networks Learning Techniques For Signal Compression*, (2010), Przegląd Elektrotechniczny, tom R. 86, nr 1, str. 189-191.

4.2.3. Publikacja w czasopiśmie spoza listy MNiSW

[S] Puchala D., *Involutory Parametric Orthogonal Transforms of Cosine-Walsh Type With Application to Data Encryption*, (2018), In: Shakhovska N., Stepashko V. (eds), Advances in Intelligent Systems and Computing II, CSIT 2017 Selected Papers, Advances in Intelligent Systems and Computing, tom 689, str. 404-420, Springer.

4.2.4. Referat konferencyjny

[R] Puchala D., *The class of involutory parametric transforms of cosine-Walsh type*, (2017), XII-th International Scientific and Technical Conference Computer Science and Information Technologies (CSIT 2017), Lviv.

4.3. OMÓWIENIE CELU NAUKOWEGO I OSIĄGNIĘTYCH WYNIKÓW

4.3.1. Wprowadzenie

Dyskretnie przekształcenia liniowe są powszechnie wykorzystywane w bardzo wielu zagadnieniach informatycznych w zakresie cyfrowego przetwarzania i analizy sygnałów, tj. przykładowo w filtracji, kompresji danych, rozpoznawaniu kształtów, szyfrowaniu danych, klasyfikacji danych, i wielu innych (patrz [1, 2]). Najpopularniejszymi przekształceniami liniowymi są z pewnością dyskretnie przekształcenia: Fouriera, Walsha-Hadamarda, Hartleya, a także przekształcenia kosinusowe i sinusowe różnych typów. Wśród najważniejszych zalet wspomnianych przekształceń należy wymienić ich wysoką skuteczność w zastosowaniach praktycznych, a także możliwość budowy szybkich algorytmów w myśl zasady „dziel-i-rządź”. Szybkie algorytmy cechuje wysoka efektywność obliczeniowa oraz łatwość realizacji w schemacie równoległym, masowo-równoległym, czy też potokowym. Wymienione zalety są zatem bardzo ważne z punktu widzenia zastosowań praktycznych. Istotnym ograniczeniem dyskretnych przekształceń liniowych, które wynika bezpośrednio ze stałości wektorów bazowych, jest brak możliwości dopasowania postaci przekształcenia zarówno do wybranych charakterystyk sygnałów wejściowych, jak również specyficznych wymagań realizowanego zadania. Dla przykładu dyskretnie przekształcenie kosinusowe drugiego typu (DCT-II) [2] znalazło zastosowanie w popularnym standardzie stratnej kompresji obrazów JPEG [3] dzięki dobrym własnościom kondensacji energii w niewielkiej liczbie współczynników widmowych. Własność ta jest jednak prawdziwa dla sygnałów modelowanych jako stacjonarne procesy Markowa przy współczynniku autokorelacji bliskim jedności. Z oczywistych względów sygnały naturalne spotykane w praktyce mogą spełniać podane założenie jedynie w pewnym przybliżeniu. Oznacza to w szczególności, iż można znaleźć przekształcenia lepiej dopasowane do charakterystyk statystycznych danych wejściowych. Wymaga to jednak odpowiednich narzędzi w postaci przekształceń, które mogą podlegać adaptacji, a także technik umożliwiających samą adaptację. Odpowiedzią na wspomniane potrzeby są szybkie liniowe przekształcenia parametryzowane w połączeniu z dedykowanymi technikami adaptacji. Biorąc zatem pod uwagę bardzo cenną z punktu widzenia zastosowań praktycznych możliwość adaptacji przekształcenia nie dziwi fakt, iż od momentu opublikowania wyników badań dotyczących wykorzystania szybkich adaptacyjnych przekształceń parametryzowanych typu kosinusowego-Haara w zadaniach kompresji danych (patrz [4]), obserwujemy rosnące zainteresowanie środowisk naukowych zagadnieniami syntezy przekształceń parametryzowanych o różnych własno-

ściach i strukturach obliczeniowych, oczywiście z zachowaniem wspomnianych zalet szybkich przekształceń liniowych. Jako przykłady można wskazać wybrane publikacje dotyczące: (i) opracowania nowych klas przekształceń parametryzowanych o różnych własnościach (patrz [5]-[9]), (ii) badań w kierunku opracowania technik doboru wartości parametrów dla przekształceń parametryzowanych (patrz [10, 11]), (iii) propozycji obszarów zastosowania i eksperymentalnej weryfikacji skuteczności przekształceń parametryzowanych w wybranych zastosowaniach praktycznych (patrz [12]-[16]).

Mając na względzie aktualność i istotność badań w danym kierunku moja działalność naukowa była skoncentrowana na zagadnieniach wyszczególnionych powyżej w punktach (i)-(iii).

4.3.2. Zakres badań naukowych

Przedmiotem moich badań naukowych było: (i) opracowanie nowych klas szybkich przekształceń parametryzowanych o zadanych własnościach, (ii) zaproponowanie algorytmów automatycznego doboru wartości parametrów dla szybkich przekształceń parametryzowanych względem praktycznych kryteriów optymalizacyjnych, (iii) wskazanie nowych obszarów praktycznego wykorzystania szybkich przekształceń parametryzowanych w wybranych zagadnieniach informatycznych, a także eksperymentalna weryfikacja ich efektywności.

(i). Przez klasę przekształceń parametryzowanych o zadanych własnościach rozumiemy przekształcenia budowane w oparciu o ten sam sparametryzowany schemat obliczeniowy, który gwarantuje uzyskanie przekształceń posiadających zadane własności w sposób stały, tj. niezależny od wartości parametrów. Dobór samych własności może być podyktowany względami praktycznymi, tzn. może wynikać wprost z potrzeb realizowanego zadania. Może być także konsekwencją czynników ekonomicznych, tj. dla przykładu pozwala na uproszczenie implementacji sprzętowych lub programowych. Część prowadzonych przeze mnie badań dotyczyła opracowania schematów syntezy szybkich przekształceń parametryzowanych o zadanych własnościach, tj. przekształceń biortogonalnych, przekształceń biortogonalnych o wektorach bazowych jednostkowej długości, czy też przekształceń inwolutorycznych budowanych w oparciu o szybkie algorytmy znanych dyskretnych przekształceń liniowych.

(ii). Struktury parametryzowane, chociaż podlegają adaptacji, nie mogą być w sposób łatwy wykorzystanie w praktyce. Drugim, niezwykle ważnym ele-

mentem są techniki automatycznego doboru wartości parametrów. W pracach naukowych innych badaczy bardzo często wykorzystywano w tym celu proste podejścia oparte o parametryzację realizowaną w oparciu o jeden wzorcowy wektor bazowy przekształcenia (patrz [12]), co pozwalało jedynie na adaptację niewielkiej liczby parametrów i wymagało znajomości a priori postaci wektora wzorcowego, czy też stosowane podejścia bazowały na wyczerpującym przeszukiwaniu przestrzeni parametrów (patrz [17]), co z kolei było możliwe do realizacji w zakresie adaptacji bardzo niewielkiej liczby parametrów, i to z dużym krokiem kwantyzacji ich wartości. Podejścia takie mają zatem znaczenie jedynie badawcze i mogą być stosowane w celu eksperymentalnej weryfikacji pewnych hipotez. Z tego powodu znaczna część badań była skoncentrowana na opracowaniu technik adaptacji, które cechowałyby się dużą elastycznością oraz łatwością użycia w praktycznych zadaniach optymalizacyjnych.

(iii). Efektywne narzędzia w postaci szybkich adaptowanych przekształceń parametryzowanych w połączeniu z technikami automatycznego doboru wartości parametrów pozwalają na wykorzystanie rozważanych przekształceń wszędzie tam, gdzie swoje zastosowania znajdują przekształcenia o stałych wektorach bazowych. Dodatkowa możliwość parametryzacji przekształceń pozwala jednak na wskazanie nowych obszarów ich praktycznego wykorzystania. Tym samym część prac badawczych koncentrowała się właśnie na wskazaniu nowych obszarów wykorzystania szybkich liniowych przekształceń parametryzowanych, a także na eksperymentalnej weryfikacji ich efektywności we wskazanych obszarach.

4.3.3. Wykaz najbardziej znaczących wyników badań

Najbardziej znaczące wyniki moich badań w ujęciu ogólnym to:

- dokonanie przeglądu i systematyzacji wiedzy związanej z szybkimi przekształceniami parametryzowanymi, ich strukturami obliczeniowymi oraz technikami adaptacji, i opublikowanie otrzymanego opracowania w formie jednej monografii naukowej (patrz [M]).

Takie opracowanie nie miało wcześniej miejsca zarówno w polskiej, jak i w anglojęzycznej literaturze o tematyce naukowej.

W zakresie (i), tj. w zakresie opracowania nowych klas przekształceń parametryzowanych o różnych własnościach:

- uogólnienie szybkich ortogonalnych przekształceń parametryzowanych na

przypadek przekształceń biortogonalnych (patrz [A.3]),

Wcześniej w literaturze naukowej z zakresu przekształceń liniowych o zwartym nośniku nie zaproponowano uogólnienia szybkich przekształceń parametryzowanych na przypadek przekształceń odwracalnych. Rozważane uprzednio klasy przekształceń były w szczególności związane warunkiem ortogonalności wektorów bazowych. Zaproponowane w pracy [A.3] uogólnienie pozwala na bezpośrednie wykorzystanie przekształceń parametryzowanych wszędzie tam, gdzie optymalnym rozwiązaniem nie będzie przekształcenie ortogonalne, tj. chociażby w uogólnionej filtracji Wienera.

- zaproponowanie efektywnych struktur obliczeniowych dla biortogonalnych przekształceń parametryzowanych (patrz [A.3]),

Zaproponowane struktury obliczeniowe o zwiększonej efektywności obliczeniowej pozwalają na **niemal dwukrotną redukcję liczby operacji mnożenia** w ramach szybkich parametryzowanych przekształceń biortogonalnych. Uzyskanie takiego wyniku w zakresie przyspieszania algorytmów należy zaliczyć do osiągnięć bardzo wartościowych.

- zaproponowanie schematu budowy szybkich biortogonalnych przekształceń parametryzowanych o znormalizowanych wektorach bazowych (patrz praca [A.4]),

W tym miejscu mamy na myśli parametryzowane przekształcenia biortogonalne o wektorach bazowych jednostkowej długości, przy czym jednostkowa długość wektorów jest uzyskiwana poprzez odpowiednią konstrukcję szybkiej struktury obliczeniowej, a nie poprzez ich późniejszą normalizację. Takie wyniki są unikatowe w skali światowej. Własność jednostkowej długości wektorów bazowych pozwala na bezpośrednie wykorzystanie zaproponowanych szybkich przekształceń parametryzowanych w roli szybkiego klasyfikatora adaptacyjnego w zadaniach klasyfikacji danych.

- opracowanie schematu syntezy szybkich przekształceń parametryzowanych typu kosinusowego-Walsha z dodatkową własnością inwolucji (patrz [S], [K]).

Inwolutoryczne przekształcenia ortogonalne, to inaczej przekształcenia samoodwracalne, w przypadku których macierz przekształcenia jest ma-

cierzą symetryczną. Z kolei symetria macierzy przekształcenia jest korzystna z punktu widzenia realizacji sprzętowych. W takim przypadku ten sam układ elektroniczny może realizować zarówno przekształcenie proste, jak i przekształcenie odwrotne.

W zakresie (ii), tj. w zakresie opracowania automatycznych technik doboru wartości parametrów dla przekształceń parametryzowanych:

- opracowanie techniki adaptacji szybkich parametryzowanych przekształceń ortogonalnych w zadaniu kompresji z kwantyzacją dokładną (patrz praca [A.6]),

Bezpośrednią korzyścią płynącą z użycia proponowanego rozwiązania jest **dwukrotna redukcja liczby obliczeń** w stosunku do znanego podejścia autokodera. Wynika to wprost z potrzeby adaptacji wyłącznie przekształcenia prostego.

- opracowanie techniki adaptacji szybkich ortogonalnych przekształceń parametryzowanych do postaci aproksymującej przekształcenie Karhunen-Loévego z dokładnością do permutacji wektorów wierszowych (patrz praca [A.1]),

W odniesieniu do struktur adaptacyjnych takie kryterium optymalizacji nie było wcześniej znane. Pozwala ono na aproksymację przekształcenia KLT w procesie optymalizacji realizowanym znów jedynie w oparciu o adaptację jednego przekształcenia, tj. przekształcenia prostego.

- opracowanie techniki adaptacji szybkich przekształceń biortogonalnych, a także przekształceń biortogonalnych o znormalizowanych wektorach bazowych (patrz prace [M], [A.3], [A.4]),

W pracach innych badaczy z zakresu szybkich parametryzowanych przekształceń liniowych stosowano techniki doboru wartości parametrów, które poprzez brak elastyczności i efektywności nie mogą być stosowane w zadaniach praktycznych. Zaproponowane przeze mnie techniki posiadają wspomniane cechy i tym samym mogą znaleźć zastosowanie w praktyce, co potwierdzają eksperymenty przeprowadzane w ramach prac badawczych. W szczególności przedstawione kolejno w pracach [A.6] i [A.1] kryteria optymalizacji (w połączeniu dowolnymi technikami optymalizacji) pozwalają uzyskać w strukturach szybkich ortogonalnych przekształceń parametryzowanych odpowiednio aproksymację podprzestrzeni roz-

piętej na M pierwszych wektorach przekształcenia Karhunen-Loévego (KLT) (patrz [A.6]), czy też aproksymację samego przekształcenia KLT z dokładnością do permutacji wektorów bazowych (patrz [A.1]). Zaproponowane techniki adaptacji mają charakter unikatowy, i to również w odniesieniu do znanych technik trenowania sztucznych sieci neuronowych projektowanych z myślą o aproksymacji przekształcenia KLT (patrz [18]).

- propozycja wykorzystania zapisu macierzowego i elementów algebry macierzy do wyprowadzenia i opisu zależności umożliwiających adaptację szybkich przekształceń parametryzowanych z wykorzystaniem technik gradientowych.

Takie nie było stosowane w rozważanej dziedzinie. Bezpośrednimi korzyściami płynącymi z użycia zapisu macierzowego są: zgodność z ogólnie przyjętymi zasadami opisu postaci szybkich przekształceń parametryzowanych, a także spójność samego zapisu oraz brak licznych operacji sumowania i skomplikowanej indeksacji.

W zakresie (iii), tj. w zakresie wskazania nowych obszarów praktycznego wykorzystania szybkich przekształceń parametryzowanych w wybranych zagadnieniach cyfrowej analizy i przetwarzania sygnałów:

- propozycja zastosowania szybkich parametryzowanych przekształceń ortogonalnych o wektorach bazowych jednostkowej długości w zadaniach klasyfikacji danych (patrz [A.4]),

W wyniku użycia proponowanych przekształceń do klasyfikacji danych otrzymujemy szybki klasyfikator. Przeprowadzone badania (patrz [A.4]) wykazały niewielki, bo wynoszący 3%, spadek efektywności klasyfikacji w porównaniu z powszechnie stosowanym podejściem w postaci sztucznej sieci neuronowej Kohonena, przy jednoczesnej **redukcji liczby operacji matematycznych o 25%**.

- propozycja wykorzystania szybkich parametryzowanych przekształceń ortogonalnych do szyfrowania danych (patrz [A.5]),
- propozycja schematu łącznej kompresji i szyfrowania obrazów w standardzie JPEG, które są realizowane w oparciu o szybkie ortogonalne przekształcenia parametryzowane (patrz [A.2]),

Chociaż wcześniej znane były techniki szyfrowania obrazów w standar-

dzie JPEG z wykorzystaniem przekształceń ortogonalnych (patrz [M]), to używano w tym kontekście jedynie pewnych klas przekształceń, tj. diagonalnych przekształceń z elementami $\{-1, 1\}$ na głównej przekątnej, czy też macierzy permutacji. Zaproponowany w pracy [A.2] schemat łącznego szyfrowania i kompresji danych pozwala wykorzystać dowolne przekształcenie ortogonalne w celu szyfrowania danych. Korzyści płynące z użycia proponowanego schematu to: istotne zwiększenie złożoności kryptograficznej metody, możliwość uzyskiwania wysokich współczynników kompresji pomimo użycia szerszej klasy przekształceń szyfrujących, a także uzyskanie odporności na znane ataki kryptograficzne dedykowane rozważanemu schematowi szyfrowania (patrz [M]).

4.3.4. Szczegółowe omówienie osiągniętych wyników

a. Szybkie przekształcenia parametryzowane o zadanych własnościach

Część przeprowadzonych badań była skoncentrowana na opracowaniu klas szybkich przekształceń parametryzowanych o zadanych własnościach. Chronologicznie pierwsze badania (patrz [A.3]) dotyczyły uogólnienia szybkich ortogonalnych przekształceń parametryzowanych na klasę przekształceń cechujących się jedynie własnością odwracalności. Osłabienie wymogu ortogonalności oznacza, iż wektory bazowe takich przekształceń nie muszą cechować się jednostkową długością, ani też nie muszą być względem siebie parami prostopadłe. Z oczywistych względów efektywne obliczeniowo struktury szybkich przekształceń ortogonalnych powinny pozostać zachowane. W rezultacie przeprowadzonych badań w pracy [A.3] zaproponowano schemat budowy szybkich parametryzowanych przekształceń biortogonalnych oparty o struktury kratowe szybkich przekształceń ortogonalnych i dwupunktowe biortogonalne operacje bazowe. W tej samej pracy wprowadzono do literatury naukowej nowe pojęcie **szybkich przekształceń biortogonalnych**. Założone cele zostały osiągnięte jedynie poprzez zamianę operacji bazowych, które w przypadku przekształceń ortogonalnych realizowały operacje rotacji planarnych, na dwupunktowe operacje odwracalne o postaci ogólnej. Wówczas pojedynczy operator bazowy będzie opisywany wartością nie jednego, lecz trzech niezwiązanych parametrów. Jednakże, jak wykazały dalsze badania (patrz [A.3]), taka struktura jest obliczeniowo nadmiarowa i każdy operator bazowy może zostać sprowadzony do jednego z czterech wariantów operatorów o uproszczonej postaci (patrz również [M]). Zabieg taki wymaga wyprowadzenia na zewnątrz każdej operacji bazowej dwóch współczynników skalujących w postaci dwupunktowej macierzy diagonalnej. Współczynniki te

są dalej propagowane wprzód, przechodząc przez kolejne etapy, aż do wyjścia struktury, gdzie tworzą dodatkowy etap złożony z mnożników skalujących. Uzyskane w taki sposób operacje bazowe można opisać w efektywny sposób, który wymaga jedynie dwóch dodawań i dwóch mnożeń (wyznacznik takiego operatora jest zawsze równy jedności). W rezultacie otrzymuje się strukturę szybką o wysokiej efektywności obliczeniowej. Złożoność obliczeniowa takiej struktury, mimo możliwości realizacji szerszej klasy przekształceń, jest niższa, niż analogicznej struktury realizującej przekształcenie ortogonalne (**liczba mnożeń jest niemal dwukrotnie mniejsza**). W przypadku szybkich przekształceń ortogonalnych o stałych wektorach bazowych podobny zabieg jest znany i w rezultacie prowadzi do uzyskania tzw. przekształceń z mnożnikami tangensowymi [19].

Praktyczna skuteczność zaproponowanych szybkich przekształceń biortogonalnych została zweryfikowana eksperymentalnie (patrz [A.3]) w zadaniu filtracji odsumiającej sygnałów elektroencefalograficznych realizowanej w schemacie uogólnionej filtracji Wienera. Jak wiadomo przekształceniem optymalnym w takim przypadku będzie przeskalowane przez macierz odwracalną (o postaci zależnej od rodzaju szumu) przekształcenie Karhunen-Loèvego, tzn. w ogólności przekształcenie biortogonalne. Uzyskane wyniki eksperymentalne potwierdziły praktyczną skuteczność szybkich przekształceń biortogonalnych, które pozwoliły na uzyskanie wyników zbliżonych do optymalnych, przy złożoności obliczeniowej typowej dla przekształceń szybkich. Przykładowo dla przekształceń o rozmiarze $N = 32$ i $N = 64$ punkty spadek efektywności filtracji był mniejszy od 0.5 dB. Natomiast uzyskana **redukcja liczby operacji arytmetycznych wyniosła około 60%**.

W kolejnej pracy [A.4] przedstawione zostały wyniki badań prowadzonych nad szybkimi przekształceniami biortogonalnymi o wektorach bazowych jednostkowej długości. Wymóg taki oznacza, iż wektory bazowe takiego przekształcenia mogą być ułożone względem siebie pod różnymi kątami (ograniczonymi szybką strukturą obliczeniową), natomiast ich długości są zawsze jednostkowe. Zatem wektory takie opisują położenie punktów na powierzchni hipersfery o promieniu równym jeden. Możliwe obszary zastosowań, to chociażby klasyfikacja danych w oparciu o miarę podobieństwa, jaką jest iloczyn skalarny wektorów. Szybkie przekształcenie adaptacyjne o takich własnościach można określić, posługując się nazewnictwem z zakresu sztucznej inteligencji, mianem szybkiej sieci neuronowej Kohonena. Należy podkreślić, iż jednostkowa długość wektorów bazowych powinna być stałą cechą samych struktur obliczeniowych, tzn. powinna być zapewniona strukturalnie bez względu na sposób parametryzacji, i to z wykluczeniem normaliza-

cji poprzez dodatkowe współczynniki skalujące na wyjściu struktury. Takie skalowanie byłoby bowiem czasochłonne obliczeniowo i powodowałoby znaczną komplikację samych technik adaptacji. Założone cele osiągnięto poprzez wprowadzenie dwuetapowych struktur hybrydowych. Struktury takie stanowią kaskadowe połączenie dwóch przekształceń parametryzowanych, tj. przekształcenia ortogonalnego i przekształcenia biortogonalnego zbudowanego z operacji bazowych nowego typu. Operacje bazowe nowego typu posiadają strukturę analogiczną do operacji obrotów planarnych, przy czym pierwszy i drugi wiersz macierzy takiego przekształcenia są parametryzowane innymi wartościami kątów. Tym samym operator nowego typu opisuje nie jeden, lecz dwa parametry.

Skuteczność proponowanych szybkich przekształceń parametryzowanych o wektorach bazowych jednostkowej długości została potwierdzona eksperymentalnie w zadaniu klasyfikacji danych realizowanej w oparciu o ogólnie dostępną bazę gatunków win. Proponowane przekształcenia pozwoliły uzyskać efektywność klasyfikacji zbliżoną do sztucznej sieci neuronowej Kohonena w **czasie krótszym o ponad 25%**, przy rozmiarze przekształcenia wynoszącym raptem 8 punktów. Naturalnie w przypadku przekształceń o większej liczbie punktów zysk obliczeniowy będzie odpowiednio większy. W zakresie przyspieszania algorytmów taki wynik można uznać za bardzo dobry.

Pozostałe badania (patrz [S], [R]) prowadzone nad opracowaniem szybkich przekształceń parametryzowanych o zadanych własnościach, dotyczyły nałożenia warunku inwolucji na szybkie parametryzowane przekształcenia typu kosinusowego-Walsha (patrz praca [M]). Skuteczność szybkich przekształceń parametryzowanych tego typu została wykazana w zadaniach kompresji sygnałów pochodzących z rezonansu magnetycznego [20]. Z kolei ortogonalne przekształcenia inwolutoryczne, to przekształcenia posiadające własność samoodwracalności. Własność taka oznacza, że przekształcenie proste jest jednocześnie przekształceniem odwrotnym. Korzyści płynące z użycia przekształceń o takich własnościach będą w szczególności widoczne w przypadku realizacji sprzętowych. Wówczas ten sam układ elektroniczny może być wykorzystany do wyznaczania przekształcenia prostego i odwrotnego. Nałożenie wspomnianego ograniczenia na strukturę szybkiego przekształcenia kosinusowego-Walsha wymagało wyprowadzenia odpowiednich związków łączących pary parametrów struktury. Przeprowadzone badania eksperymentalne wykazały wysoką skuteczność takich przekształceń w zadaniach szyfrowania danych.

b. Propozycje algorytmów automatycznego doboru wartości parametrów

Jak wspomniano przekształcenia parametryzowane o szybkich strukturach obliczeniowych mogą znaleźć praktyczne zastosowania tylko w połączeniu z wydajnymi technikami automatycznej adaptacji wartości parametrów. W pracach wielu autorów w celu eksperymentalnej weryfikacji skuteczności rozważanych przekształceń stosowano: parametryzację na bazie wzorcowego wektora bazowego, wyczerpujące przeszukiwanie przestrzeni parametrów, czy też podejścia lokalne oparte o strategię zachłanną (przegląd technik adaptacji zamieszczono w [M]). Wspomniane techniki pozwalają, albo na adaptację wyłącznie ograniczonej liczby parametrów (wektor wzorcowy i przeszukiwanie przestrzeni parametrów), nie wspominając tutaj o potrzebie znajomości postaci wektorów wzorcowych, czy też czasochłonności przeszukiwania wyczerpującego, albo też z założenia nie pozwalają na odnalezienie globalnie optymalnej parametryzacji (techniki lokalne). Stąd znaczna część moich badań była skoncentrowana na opracowaniu technik automatycznego doboru wartości parametrów, które są wydajne obliczeniowo i dają dobre rezultaty w sensie bliskości znajdowanych rozwiązań względem rozwiązań optymalnych. Oczywiście badania były prowadzone z uwzględnieniem różnych klas przekształceń parametryzowanych i ich specyficznych własności.

Na pierwszym miejscu (patrz praca [A.6]) rozważano przypadek szybkich parametryzowanych przekształceń ortogonalnych w zadaniach kompresji danych z użyciem kwantyzacji dokładnej, tj. kwantyzacji przez obcięcie. Zaproponowano metodę adaptacji bazującą wyłącznie na przekształceniu prostym i kryterium maksymalizacji sumarycznej energii sygnału w podprzestrzeni. Należy zauważyć, iż klasyczne podejście oparte o schemat autokodera [3] wymaga zaangażowania w procesie adaptacji zarówno przekształcenia prostego, jak i odwrotnego. Tym samym zaproponowane podejście dało **dwukrotne przyśpieszenie obliczeń**. Oczywiście taki sposób adaptacji jest możliwy dzięki własności ortogonalności przekształceń parametryzowanych. Z kolei użycie przekształceń ortogonalnych jest w pełni uzasadnione, ponieważ wiadomym jest fakt, iż w przypadku kwantyzacji dokładnej optymalnym rozwiązaniem będzie podprzestrzeń rozpięta na wektorach bazowych przekształcenia Karhunen-Loévego (KLT), które w rozważanym przypadku jest przekształceniem ortogonalnym. Skuteczność proponowanej metody adaptacji poddano weryfikacji eksperymentalnej w oparciu o sygnały modelowe. Należy wspomnieć, że w tej samej pracy przeprowadzono także analizę porównawczą trzech typów operacji bazowych, tzn.: (a) operacja biortogonalna, (b) operacja ortogonalna bez normalizacji wektorów, (c) operacja ortonormalna

- obrót planarny. W przypadku pierwszych dwóch typów operacji bazowych ortogonalność całej struktury była uzyskiwana jedynie w pewnym przybliżeniu poprzez wykorzystanie mechanizmu funkcji kary. Badania eksperymentalne wykazały, że najszybszą zbieżnością, jak również wynikami najbliższymi optymalnym, cechują się szybkie struktury budowane w oparciu o operacje bazowe natywnie ortonormalne, tj. operacje typu (c). Ponadto zaproponowane w pracy podejście działa w oparciu o wektory próbek sygnału, a nie na podstawie macierzy autokorelacji. Może być zatem stosowane bezpośrednio w odniesieniu do sygnału wejściowego.

Kontynuacji prac w tym samym kierunku podjęto się w pracy [A.1]. Zaproponowano tutaj technikę adaptacji przekształceń ortogonalnych do postaci stanowiącej aproksymację przekształcenia KLT z dokładnością do permutacji wektorów bazowych. Termin aproksymacja był podyktowany faktem wykorzystania przekształceń parametryzowanych o szybkich strukturach obliczeniowych, które poprzez rzadką siatkę połączeń stawiają ograniczenia, co do realizowalności wszystkich przekształceń ortogonalnych. Z kolei wybór szybkich przekształceń wynikał wprost ze względów praktycznych. Pomijając jednak ograniczenia wynikające z użycia przekształceń szybkich można dowieść, iż zaproponowane w pracy [A.1] kryterium adaptacji, które polega na maksymalizacji sumy czwartych momentów zmiennych losowych w dziedzinie przekształcenia ortogonalnego, pozwala przy praktycznym założeniu uzyskiwać przekształcenia KLT z dokładnością do permutacji wektorów bazowych. W tej samej pracy znajdziemy także właściwe twierdzenie wraz z dowodem. Natomiast wspomnianym wcześniej założeniem praktycznym jest rozkład normalny zmiennych losowych rozpatrywanych w dziedzinie przekształcenia. W praktyce można przyjąć na mocy centralnego twierdzenia granicznego, że założenie takie będzie spełnione. Dążność do uzyskania przekształcenia KLT, bądź jego aproksymacji, jest z kolei podyktowana optymalnością przekształcenia KLT w takich zastosowaniach, jak filtracja, czy kompresja sygnałów [2]. Dodatkowym elementem nowości zawartym w pracy [A.1] są wyprowadzenia wyrażeń pozwalających na adaptację parametrów przekształceń szybkich w oparciu o zaproponowane kryterium adaptacji z wykorzystaniem zapisu macierzowego. Taki sposób opisu technik optymalizacji gradientowej nie był dotychczas wykorzystywany w literaturze tematu. Pozwala on jednak na łatwe i pozbawione rozbudowanej indeksacji, czy też licznych operacji sumowań, przedstawienie i posługiwanie się niezbędnymi zależnościami. Skuteczność proponowanej techniki adaptacji zweryfikowano eksperymentalnie w oparciu o sygnały modelowe. Uzyskane wyniki potwierdziły jej skuteczność. Należy ponadto wspomnieć, iż zaproponowane podejście działa w oparciu o wektory próbek i tym samym może być stosowane

bezpośrednio w odniesieniu do sygnału wejściowego. Zatem również i w tym przypadku nie jest wymagana znajomość postaci macierzy autokowariancji sygnału.

c. Wskazanie nowych obszarów praktycznego wykorzystania szybkich przekształceń parametryzowanych

Szybkie przekształcenia parametryzowane mogą być z powodzeniem stosowane wszędzie tam, gdzie zastosowania praktyczne znajdują liniowe przekształcenia dyskretne o stałych wektorach bazowych. Do klasycznych zastosowań zaliczyć należy z pewnością: kompresję z kwantyzacją dokładną [A.6], uogólnioną filtrację Wienera [A.3], czy kompresję realizowaną w oparciu o kwantyzację zgrubną [A.1], [A.2]. Możliwość parametryzacji przekształceń pozwala jednak na wskazanie nowych obszarów zastosowań, chociażby takich jak: szyfrowanie danych (patrz [A.5], [S] i [R]), łączna kompresja i szyfrowanie obrazów (patrz [A.2]), czy też opisana wcześniej w sekcji 5.4.1 klasyfikacja danych, gdzie szybkie przekształcenie parametryzowane pełni rolę adaptownego klasyfikatora.

Szyfrowanie danych z zachowaniem ich dobrych własności względem dalszego kroku kompresji nie jest zadaniem oczywistym. Wiadomo, iż pożądane z punktu widzenia jakości szyfrowania danych są: równomierny rozkład zmiennych losowych, a także brak korelacji. Z kolei dane o takim rozkładzie statystycznym są mało atrakcyjne z punktu widzenia kompresji. Oznacza to, że metoda łącznego szyfrowania i kompresji danych musi stanowić pewien dobrze wyważony kompromis. W pracy [A.5] zaproponowano schemat szyfrowania i kompresji obrazów statycznych bazujący na znanym standardzie kompresji stratnej JPEG. Schemat ten stanowi bardzo istotne ulepszenie wcześniej proponowanych w literaturze metod. W szczególności pozwala na uzyskiwanie wysokich współczynników kompresji, będąc jednocześnie odpornym na znane w danej klasie algorytmów metody kryptoanalizy. Mówiąc o klasie algorytmów mamy na myśli liniowe techniki szyfrowania danych posiadające bardzo istotną cechę, która polega na możliwości ich wykorzystania w standardzie kompresji JPEG (a także M-JPEG, czy MPEG) bez konieczności zmiany samego strumienia danych. Techniki takie wpisują się w następujący praktyczny scenariusz wykorzystania, tzn.: mamy nadawcę danych, tutaj przesyłanych jako obrazy, które są transmitowane w sposób zaszyfrowany ogólnie dostępnymi kanałami, z wykorzystaniem znanego i popularnego standardu kompresji danych - JPEG; jedynie odbiorcy autoryzowani, którzy znają klucz prywatny mogą z powodzeniem deszyfrować dane; pozostali

użytkownicy powinni mieć możliwość poprawnego wyodrębnienia obrazów ze strumienia danych, jednakże bez znajomości klucza prywatnego zobaczą obraz zupełnie nieczytelny, np. w wyniku zniekształcenia będącego konsekwencją nieliniowego przesunięcia fazy współczynników widmowych [21], czy też odczytany obraz będzie przypominał realizację szumu o rozkładzie Gaussa (patrz [A.2]). Przykładem potencjalnego obszaru zastosowania dla takiego schematu mogą być systemy transmisji telewizji cyfrowej. Wówczas wprowadzenie techniki szyfrowania dzięki zachowaniu spójności strumienia danych, nie będzie wiązało się z kosztowną wymianą urządzeń końcowych posiadanych przez odbiorców. Z drugiej strony charakter przesyłanych danych i ich wartość nie sprzyjają kosztownym i ryzykownym próbom ataków ze strony potencjalnych adwersarzy. Wiadomo bowiem, iż liniowe techniki szyfrowania nie są odporne na ataki z tekstem jawnym.

W pracy [A.2] zaproponowano technikę łącznej kompresji i szyfrowania obrazów, która wpisuje się w powyższy schemat. Do szyfrowania danych wykorzystano szybkie ortogonalne przekształcenia parametryzowane, dla których wartości parametrów są wyznaczone na podstawie klucza prywatnego. Dalej dzięki autorskiemu schematowi **mieszania międzyblokowego** szyfrowanie danych, będących fragmentami obrazu o wymiarach 8 na 8 pikseli, odbywa się w sposób umożliwiający zachowanie wysokich poziomów kompresji, które są charakterystyczne dla standardu JPEG. W pracy [A.2] dowodzi się, iż zaproponowany schemat zachowuje postać macierzy autokowariancji sygnału, a co za tym idzie, nie zmienia efektywności schematów kompresji stratnej opartej o kwantyzację blokową z dodatkowym krokiem kodowania entropii pierwszego rzędu. W standardzie JPEG obok kodowania Huffmana zastosowano również kodowanie długości serii (RLE) w odniesieniu do współczynników o wartościach zerowych, które pojawiają się po kwantyzacji zgrubnej. Ponieważ jest to kodowanie entropii rzędów wyższych, to w praktyce proponowana metoda powoduje pewien spadek efektywności samej kompresji. W pracy [A.2] przedstawiono wyniki badań eksperymentalnych nad skutecznością proponowanego podejścia. Wykazano na drodze eksperymentu, że proponowany schemat łącznej kompresji i szyfrowania danych pozwala uzyskiwać wysokie współczynniki kompresji, tj. bliskie współczynników otrzymywanym bez kroku szyfrowania, będąc przy tym odpornym na znane dla tej klasy technik ataki kryptologiczne, w szczególności atak typu Non-Zero Counting (NZCA) (patrz praca [22]).

Mając na względzie możliwość praktycznego wykorzystania szybkich ortogonalnych przekształceń parametryzowanych w zadaniach łącznej kompresji i szyfrowania danych, w pracy [A.5] dokonano analizy porównawczej wy-

branych przekształceń o popularnych strukturach obliczeniowych, względem następujących wskaźników jakości szyfrowania danych, tj.: rozkładu prawdopodobieństwa wartości relatywnego błędu średniokwadratowego (MSE) (wyrażonego względem energii sygnału wejściowego) pomiędzy sygnałem wejściowym, a deszyfrowanym przy losowym doborze klucza prywatnego w kroku deszyfrującym (próba ataku wyczerpującego), a także oczekiwanej wartości relatywnego błędu MSE wyrażonej w funkcji odległości Hamminga pomiędzy kluczami prywatnymi na etapach szyfrowania i deszyfrowania. Uzyskane wyniki eksperymentalne wskazywały dobre własności rozważanych szybkich przekształceń parametryzowanych. Przykładowo wartość oczekiwana relatywnego błędu MSE była na poziomie 200% energii sygnału wejściowego, co możemy interpretować w taki sposób, iż sygnał deszyfrowany był w wartości oczekiwanej prostopadły do sygnału wejściowego.

4.3.5. Krótka charakterystyka publikacji wchodzących w skład jednotematycznego cyklu publikacji (w porządku chronologicznym)

Fast Neural Networks Learning Techniques For Signal Compression (2010): propozycja algorytmu adaptacji szybkich ortogonalnych przekształceń parametryzowanych realizowana wg kryterium maksymalizacji energii w podprzestrzeni; proponowany algorytm adaptacji bazuje na gradientowej metodzie najszybszego spadku; przeprowadzono analizę porównawczą trzech typów operacji bazowych: (a) operacja biortogonalna, (b) operacja ortogonalna bez normalizacji wektorów, (c) operacja ortonormalna - obrót planarny; celem było wyłonienie operacji bazowych cechujących się najlepszymi własnościami, tj. szybkością zbieżności procesu adaptacji i bliskością znalezionego rozwiązania względem rozwiązania optymalnego; w przypadku operacji bazowych typu (a) i (b) ortogonalność całej struktury była narzucona poprzez funkcje kary; przeprowadzono badania na sygnałach modelowych; badania wykazały, że najszybszą zbieżnością i najlepszymi wynikami (najbliższymi optymalnym) cechują się operacje bazowe typu (c).

Fast Parametrized Biorthogonal Transforms (2012):

zaproponowano schemat budowy szybkich parametryzowanych przekształceń biortogonalnych; przekształcenia te stanowią uogólnienie klasy parametryzowanych przekształceń ortogonalnych, na klasę przekształceń cechujących się własnością odwracalności; zaproponowano wariant szybkich parametryzowanych przekształceń biortogonalnych cechujących się wysoką efektywnością obliczeniową; przeprowadzono badania nad praktyczną skutecznością proponowanych przekształceń w zadaniach filtracji odszumiającej, realizowanej w

schemacie uogólnionej filtracji Wienera; badania przeprowadzono z wykorzystaniem sygnałów ECG; wyniki potwierdziły praktyczną skuteczność rozważanych przekształceń; przykładowo dla przekształceń o rozmiarze $N = 64$ punkty uzyskano wyniki gorsze od KLT średnio raptem o 0.3 dB, przy 60% redukcji liczby obliczeń.

Fast Parametrized Biorthogonal Transforms with Normalized Basis Vectors (2012):

przedstawiono schemat budowy szybkich przekształceń parametryzowanych o wektorach bazowych jednostkowej długości; wskazano praktyczny obszar wykorzystania przekształceń w zadaniach klasyfikacji danych; szybkie przekształcenie parametryzowane o takich własnościach stają się niejako szybką sztuczną siecią neuronową Kohonena; zweryfikowano efektywność rozważanych przekształceń w zadaniach klasyfikacji danych na drodze eksperymentu w oparciu o znaną bazę gatunków win; uzyskane wyniki wskazały na wysoką skuteczność proponowanych przekształceń, przy jednoczesnej wysokiej efektywności obliczeniowej; uzyskane wyniki w sensie trafności klasyfikacji były gorsze o 3% w porównaniu ze sztuczną siecią Kohonena, przy 25% redukcji liczby operacji arytmetycznych.

Approximating the KLT by Maximizing the Sum of Fourth-Order Moments (2013):

w pracy została zaproponowana technika adaptacji szybkich ortogonalnych przekształceń parametryzowanych, która pozwala na uzyskanie w szybkiej strukturze przekształcenia parametryzowanego aproksymacji przekształcenia Karhunen-Loèvego z dokładnością do permutacji wektorów bazowych; adaptacja jest realizowana w oparciu o techniki gradientowe, chociaż przyjęte kryterium optymalizacyjne ma charakter ogólny; zaproponowanym kryterium optymalizacyjnym jest maksymalizacja sumy czwartych momentów statystycznych w dziedzinie przekształcenia; zamieszczono właściwe twierdzenie wraz z dowodem; do zapisu i wyprowadzenia wyrażeń pozwalających na adaptację wartości poszczególnych parametrów przekształcenia wykorzystano aparat macierzowy.

Comparison of Fast Orthogonal Parametric Transforms In Data Encryption (2015):

w pracy przeprowadzono analizę porównawczą szybkich ortogonalnych przekształceń parametryzowanych o różnych strukturach obliczeniowych w kontekście szyfrowania danych; rozważane struktury obliczeniowe to: uogólniona sieć Beneša [23], struktura przekształcenia Walsh-Hadamarda, struktura kratowa dla dwukanałowego banku filtrów ortogonalnych [24]; wykorzystano

elementarny schemat szyfrowania polegający na przekształceniu wektora wejściowego (tekstu jawnego) do dziedziny przekształcenia o postaci określonej przez wartości parametrów, które otrzymano na podstawie klucza prywatnego; obraz wektora w dziedzinie przekształcenia stanowi szyfrogram; w pracy opisano także sposób mapowania bitów klucza prywatnego na wartości parametrów; dalej szyfrogram podlegał deszyfrowaniu z użyciem odwrotnego przekształcenia parametryzowanego; jako miary odległości pomiędzy wektorem wejściowym, a jego wariantem deszyfrowanym użyto metryki relatywnego błędu średniokwadratowego (MSE), wyrażonego względem energii sygnału; wykonano badania w zakresie: wyznaczenia rozkładu prawdopodobieństwa dla wartości relatywnego MSE podczas losowania klucza prywatnego w kroku deszyfrującym (próba ataku wyczerpującego), a także wyznaczenia wartości relatywnego MSE w funkcji odległości Hamminga liczonej pomiędzy kluczami prywatnymi używanymi na etapach szyfrowania i deszyfrowania; przeprowadzone badania eksperymentalne wskazały wysoką skuteczność wszystkich rozważanych struktur - błąd względny MSE rekonstrukcji sygnału przy próbie odgadnięcia klucza prywatnego na poziomie 200% energii sygnału wejściowego.

Joint Compression And Encryption of Visual Data Using Orthogonal Parametric Transforms (2016):

w artykule zaproponowany został schemat łącznej kompresji i szyfrowania danych w odniesieniu do obrazów statycznych; zaproponowany schemat został wbudowany w standard stratnej kompresji obrazów JPEG; do szyfrowania danych wykorzystano szybkie ortogonalne przekształcenia parametryzowane; zaproponowany autorski schemat szyfrowania obrazów z użyciem tzw. mieszania międzyblokowego nie wpływa na jakość kompresji opartej o schemat kwantyzacji blokowej z dodatkowym krokiem kodowania entropii pierwszego rzędu, co zostało udowodnione w sposób ścisły; wykonano szereg badań eksperymentalnych wykazujących wysoką skuteczność proponowanego podejścia; na drodze eksperymentu wykazano również, że proponowany sposób szyfrowania jest odporny na znane ataki kryptologiczne, w tym również atak NZCA (patrz [22]).

Involutory Parametric Orthogonal Transforms of Cosine-Walsh Type With Application to Data Encryption (2017):

wyprowadzono odpowiednie warunki nakładane na wartości parametrów szybkiego parametryzowanego przekształcenia kosinusowego-Walsha, które pozwalają uzyskiwać w jego strukturze obliczeniowej przekształcenia inwolutoryczne; przekształcenia inwolutoryczne, inaczej przekształcenia samoodwracalne, to takie, w przypadku których przekształcenie proste i odwrotne są

opisane tą samą macierzą; na drodze eksperymentu wykazano praktyczną skuteczność inwolutowicznych przekształceń kosinusowych-Walsha w zadaniach szyfrowania danych, posługując się przy tym procedurą badawczą opisaną w pracy [A.5].

Szybkie liniowe przekształcenia parametryzowane. Struktury obliczeniowe i techniki adaptacji (2017):

to monografia naukowa poświęcona szybkim parametryzowanym przekształceniom liniowym, ich strukturom obliczeniowym, technikom adaptacji wartości parametrów, a także możliwym obszarom zastosowań praktycznych; w rozdziale 2 książki znajdziemy przegląd typów szybkich przekształceń ortogonalnych znanych z literatury; w rozdziale 3 rozważania te zostają uogólnione na przypadek szybkich parametryzowanych przekształceń biortogonalnych; w kolejnym rozdziale 4 zamieszczono przegląd znanych technik doboru wartości parametrów opartych o wektory wzorcowe, wyczerpujące przeszukiwanie przestrzeni parametrów, lokalne techniki zachłanne, czy też optymalizację gradientową; w rozdziale 5 opisano inne przykłady znanych przekształceń parametryzowanych, chociażby schemat pozwalający na jednoczesne adaptacyjne konstruowanie struktury przekształcenia i dobór wartości parametrów według kryterium minimalizacji iloczynu wariancji zmiennych losowych w dziedzinie przekształcenia, co jest istotne z punktu widzenia stratnej kompresji opartej o kwantyzację zgrubną; rozdział 6 monografii został poświęcony praktycznym zastosowaniom szybkich przekształceń parametryzowanych; w rozdziale 7 znajdziemy powiązania pomiędzy rozważaną dziedziną, a sztucznymi sieciami neuronowymi; rozdział 8 stanowi podsumowanie książki.

5. OMÓWIENIE PRAC BADAWCZYCH POZA WSKAZANYM CYKLEM PUBLIKACYJNYM

5.1. Prace naukowo-badawcze przed doktoratem

Tematem moich badań naukowych przed doktoratem były algorytmy adaptacyjnego obliczania dyskretnych przekształceń trygonometrycznych według kryterium: *dokładność-czas realizacji obliczeń (rozmiar przekształcenia)* (patrz [25]). Podstawą matematyczną opracowanych algorytmów jest numeryczne obliczanie przekształceń całkowych. Rozważane w pracy dyskretnie przekształcenie Fouriera, a także kosinusowe i sinusowe przekształcenia wybranych typów, stanowią złożone kwadratury prostokątów dla całkowitego przekształcenia Fouriera. Tym samym możliwe jest przeniesienie na grunt dyskretnych przekształceń trygonometrycznych znanych technik adaptacyj-

nego całkowania numerycznego, włącznie z wyrażeniami oceny dokładności kwadratur numerycznych. Pozwoliło to na sformułowanie adaptacyjnych algorytmów obliczania wspomnianych dyskretnych przekształceń trygonometrycznych. Mając na względzie fakt, iż efektywność obliczeniowa algorytmów jest bardzo istotna z praktycznego punktu widzenia, to w trakcie badań zaproponowane zostały również szybkie warianty algorytmów adaptacyjnych. W tym celu schemat adaptacyjnego obliczania przekształceń dyskretnych wbudowano w struktury szybkich algorytmów z przerzedzeniem w czasie. Algorytmy z przerzedzeniem w czasie pozwalają na obliczenie przekształcenia N punktowego bezpośrednio na bazie dwóch przekształceń $N/2$ punktowych. Tym samym w kolejnych krokach adaptacji możliwe jest dwukrotne zwiększanie liczby próbek sygnału, bez konieczności powtarzania części obliczeń. Ponieważ dla przekształceń kosinusowych i sinusowych rozważanych typów algorytmy z przerzedzeniem w czasie nie były wcześniej znane, to ich wzory rozkładów zostały zaproponowane w trakcie badań. Ponadto zaproponowano wyrażenia oceny dokładności obliczania przekształceń dyskretnych w popularnych względnych i bezwzględnych metrykach błędu średniokwadratowego oraz szczytowego stosunku sygnału do szumu. W dalszej części badań zaproponowane algorytmy adaptacyjne rozszerzono na przypadek przekształceń dwuwymiarowych i kubatur całkowania numerycznego. Wiązało się to bezpośrednio z potrzebą wyprowadzenia wzorów rozkładu szybkich algorytmów z przerzedzeniem w czasie dla przekształcenia Fouriera, a także kosinusowych i sinusowych przekształceń trygonometrycznych. W ostatniej części badań wskazano praktyczne zastosowania dla proponowanych przekształceń adaptacyjnych na przykładzie przekształcenia Fouriera i zadań rozpoznawania kształtów. Zaproponowany mechanizm można określić krótko mianem adaptacyjnych deskryptorów fourierowskich [26, 27].

Pozostałe prace badawcze, w których brałem udział przed doktoratem, dotyczyły opracowania hybrydowego algorytmu falkowo-fourierowskiego do kompresji danych pomiarowych pochodzących z monitoringu działania transformatorów wysokich mocy [28, 29].

Mój dorobek publikacyjny przed doktoratem obejmuje:

- 7 publikacji w czasopismach naukowych,
- 8 referatów opublikowanych w materiałach konferencyjnych, z czego 5 wygłoszonych samodzielnie.

5.2. Inne prace naukowo-badawcze po doktoracie spoza cyklu publikacji

Poza tematyką związaną ze wskazanym głównym nurtem badań moje aktywność naukowo-badawcza dotyczyła możliwości wykorzystania współczesnych procesorów graficznych (GPU) do obliczania szybkiego przekształcenia Fouriera, a także przekształceń falkowych w oparciu o struktury kratowe (patrz prace [30]-[33]). Od roku 2007 istnieje możliwość wykorzystania potencjału drzemiącego w procesorach GPU do realizacji typowych obliczeń inżynierskich. Jednak właściwe wykorzystanie mocy obliczeniowej GPU narzuca specyficzny charakter samych obliczeń, które są nastawione na masową równoległość (mamy do dyspozycji nawet tysiące rdzeni obliczeniowych) i prostotę algorytmów (np. unikanie sekcji krytycznych, prosta synchronizacja obliczeń). Wiąże się to z koniecznością opracowania nowych algorytmów spełniających wspomniane wymagania. Badania w tej tematyce dotyczyły w szczególności: (a) doboru struktury obliczeniowej typu radix-2 dla obliczania dyskretnego przekształcenia Fouriera z uwzględnieniem sposobów reprezentacji danych w pamięci, permutacji elementów w wektorach, czy też obliczania współczynników fazowych, (b) eksperymentalnego sprawdzianu efektywności wybranych struktur kratowych w zadaniu obliczania dyskretnych przekształceń falowych jedno- i dwuwymiarowych. Rezultaty badań zostały opublikowane w 2 artykułach naukowych i przedstawione w ramach 2 konferencji o zasięgu międzynarodowym. Ponadto wyniki prac nad masowo-równoległym obliczaniem przekształceń falkowych zostały zaprezentowane w ramach Targów Międzynarodowych IENA 2015 (Norymberga) i SIIF 2015 (Seul), gdzie otrzymały srebrne medale, a także dyplom uznania przyznany przez Stowarzyszenie "Russian House for International Scientific and Technological Cooperation".

Inna tematyka badań dotyczyła numerycznej dokładności wyznaczania obrazów całkowych z uwzględnieniem praktycznych implikacji ewentualnych niedokładności (patrz praca [34]). Podczas badań rozważono różne schematy obliczania obrazów całkowych, tj.: obliczanie bezpośrednio z definicji, w oparciu o podejście Viola and Jones [35], czy też obliczenia realizowane w schemacie wierszowo-kolumnowym. Dodatkowo w przypadku podejścia wierszowo-kolumnowego rozważono trzy znane struktury obliczeniowe, których postaci sprzyjają obliczaniu obrazów całkowych na procesorach GPU. Otrzymane wyniki wraz z komentarzami, które stanowią swoisty przewodnik do praktycznego wyznaczania obrazów całkowych, zostały opublikowane w artykule z listy JCR.

Kolejne badania dotyczyły opracowania aproksymacji dyskretnego przekształcenia kosinusowego drugiego rodzaju (DCT-II), która cechuje się bardzo niską złożonością obliczeniową, mając na względzie zastosowania w zadaniach stratnej kompresji obrazów w ramach standardu JPEG (patrz praca [36]). Zaproponowano aproksymację 8-punktowej transformaty DCT-II, która cechuje się liczbą 11 dodawań i 2 przesunięć bitowych. Proponowana aproksymacja DCT-II daje lepsze wyniki (nawet o 4 dB) od znanych podejść charakteryzujących się taką samą złożonością obliczeniową przy założeniu, że działamy w schemacie, w którym obraz jest kompresowany z wykorzystaniem aproksymacji DCT-II, natomiast proces dekompresji odbywa się z użyciem przekształcenia kosinusowego. Taki scenariusz może znaleźć praktyczne odzwierciedlenie w systemach służących do akwizycji obrazów z wykorzystaniem urządzeń o zasilaniu bateryjnym, od których wymaga się bardzo niskiego zużycia energii.

W ramach działań o charakterze naukowym realizowanych poza głównym nurtem badań opublikowano również wyniki prac badawczych realizowanych przed doktoratem w formie jednej monografii naukowej.

Tutaj mój dorobek publikacyjny obejmuje:

- 1 monografia naukowa,
- 5 publikacji w czasopismach naukowych z listy MNiSW, w tym jedna z listy JCR,
- 2 referaty opublikowane w materiałach konferencyjnych, z czego jeden w serii indeksowanej w bazie Web of Science.

Dariusz Pichota

Bibliografia.

- [1] Ahmed N., Rao K. R., *Orthogonal Transforms for Digital Signal Processing*, Springer-Verlag, 1975.
- [2] Rao K., Yip P., *Discrete Cosine Transform. Algorithms, Advantages, Applications*, Academic Press, 1990.
- [3] Skarbek W., red., *Multimedia. Algorytmy i standardy kompresji*, Akademicka Oficyna Wydawnicza PLJ, 1998.
- [4] Morháč M., Matoušek V., *Data Compression Using New Fast Adaptive Cosine-Haar Transform*, Digital Signal Processing, no. 8, pp. 63-81, 1998.
- [5] Bouguezel S., *A Reciprocal-Orthogonal Parametric Transform and Its Fast Algorithm*, IEEE Signal Processing Letters, vol. 19, no. 11, pp. 769-772, 2012.
- [6] Bouguezel S., Ahmad O., Swamy M. N. S., *A New Class of Reciprocal-Orthogonal Parametric Transforms*, IEEE Transactions On Circuits And Systems-I: Regular Papers, vol. 56, no. 4, pp. 795-805, 2009.
- [7] Bouguezel S., Ahmad O., Swamy M. N. S., *Image Encryption Using the Reciprocal-Orthogonal Parametric Transforms*, IEEE Proc. Int. Symp. Circuits and Systems, pp. 2542-2545, 2010.
- [8] Bouguezel S., Ahmad O., Swamy M. N. S., *New Parametric Discrete Fourier and Hartley Transforms, and Algorithms for Fast Computation*, IEEE Trans. Circuits And Systems - I: Regular Papers, vol. 58, no. 3, 2011.
- [9] Minasyan S., Guevorkian D., Sarukhanyan H., *On Parametrized Fast Haar- and Hadamard-like Transforms of Arbitrary Order*, Proc. 3-rd Int. Conf. On Computer Science and Information Technologies, pp. 294-298, 2001.
- [10] Minasyan S., Astola J., Guevorkian D., *On Unified Architectures for Synthesizing and Implementation of Fast Parametric Transforms*, IEEE International Conference on Information, Communications and Signal Processing, pp. 710-714, 2005.
- [11] Stolarek J., *Synthesis of a Wavelet Transform Using Neural Network*, XI International PhD Workshop OWD, vol. 26, pp. 71-74, 2009.

- [12] Bouguezel S., Ahmad O., Swamy M. N. S., *A New Involutory Parametric Transform and Its Application to Image Encryption*, IEEE International Symposium on Circuits and Systems, pp. 2605-2608, 2013.
- [13] Lipiński P., *Odporne cyfrowe znaki wodne w obrazach. Adaptacyjny dobór dziedziny osadzenia*, Akademicka Oficyna Wydawnicza EXIT, 2013.
- [14] Malakooti M.V., Dobuneh M.R.N., *A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms*, Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), pp. 240-244, 2012.
- [15] Minasyan S., Astola J., Egiazarian K., Guevorkian D., *Parametric Haar-like Transforms in Image Denoising*, IEEE Int. Conf. Image Processing, pp. 2629-2632, 2006.
- [16] Minasyan S., Astola J., Guevorkian D., *An Image Compression Scheme Based on Parametric Haar-like Transforms*, IEEE Proc. Int. Symposium on Circuits and Systems, 2005.
- [17] Agaian S., Tourshan K., Noonan J. P., *Parametric Slant-Hadamard Transforms With Applications*, IEEE Signal Processing Letters, vol. 9, no 11, 2002.
- [18] Luo Fa-Long, Unbehauen R., *Applied Neural Networks for Signal Processing*, Cambridge University Press, 1998.
- [19] Jacymirski M., *Szybkie algorytmy jednolite kosinusowych transformat drugiego i trzeciego rodzaju o mnożnikach tangensowych*, Automatyka AGH, tom 7, zeszyt 3, str. 727-741, 2003.
- [20] Morháč M., Matoušek V., *New Adaptive Cosine-Walsh Transform and its Application to Nuclear Data Compression*, IEEE Trans. On Signal Processing, vol. 48, no. 9, pp. 2693-2696, 2000.
- [21] Bhargava B. , Shi Ch., Wang Sh. Y., *MPEG Video Encryption Algorithms*, Multimedia Tools and Applications, vol. 24, no 1, pp. 57-79, 2004.
- [22] Li W., Yuan Y., *A Leak and Its Remedy in JPEG Image Encryption*, International Journal of Computer Mathematics, vol. 84, no. 9, pp. 1367-1378, 2007.
- [23] Beneš E. V., *Mathematical Theory of Connecting Networks and Telephone Traffic*, Academic Press, 1965.

- [24] Yatsymirskyy M., *Lattice Structures for Synthesis and Implementation of Wavelet Transforms*, Journal of Applied Computer Science, vol. 17, no. 1, pp. 133-141, 2009.
- [25] Puchala D., *Szybkie algorytmy adaptacyjne przekształceń trygonometrycznych*, Wydawnictwo Politechniki Łódzkiej, Łódź, 2016.
- [26] Puchala D., Yatsymirskyy M. M., *Fast Adaptive Fourier Transform for Fourier Descriptor Based Contour Classification*, Advances In Soft Computing – Computer Recognition Systems 2, Proc. of CORES'07 Conference, pp. 378-385, Springer 2007.
- [27] Puchala D., Yatsymirskyy M. M., *Neural Network in Fast Adaptive Fourier Descriptor Based Leaves Classification*, ICAISC'08, Artificial Intelligence and Soft Computing – ICAISC 2008, vol. 5097/2008, pp. 135-145, 2008.
- [28] Lipinski P., Puchala D., Wosiak A., Byczkowska-Lipinska L., *Transformer Monitoring System Taking Advantage of Hybrid Wavelet Fourier Transform*, ISEF 2007 - XIII International Symposium on Electromagnetic Fields in Mechatronics, Electrical and Electronic Engineering Prague, pp. 126-129, Czech Republic, September, 2007.
- [29] Lipiński P., Puchala d., Yatsymirskyy M. M., *Adaptive Hybrid Fourier-Wavelet Transform With Application to Signal Compression*, PD FCCS'07 Conference, 2007.
- [30] Puchala D., Szczepaniak B., Yatsymirskyy M., *Lattice Structure for Parallel Calculation of Orthogonal Wavelet Transform on GPUs With CUDA Architecture*, Przegląd Elektrotechniczny, vol. R.91, no. 7, pp. 52-54, 2015.
- [31] Puchala D., Szczepaniak B., Yatsymirskyy M., *Effective Realizations of Biorthogonal Wavelet Transforms of Lengths $2K+1/2K-1$ With Lattice Structures on GPU and CPU*, IDEAL 2015 Conference, LNCS Series, no. 9375, pp. 130-137, 2015.
- [32] Puchala D., Stokfiszewski K., Szczepaniak B., Yatsymirskyy M., *Effectiveness of Fast Fourier Transform Implementations on GPU and CPU*, 16th International CPEE Conference Conference, IEEEExplore, pp. 162-165, 2015.

- [33] Puchala D., Stokfiszewski K., Szczepaniak B., Yatsymirskyy M., *Effectiveness of Fast Fourier Transform Implementations on GPU and CPU*, Przegląd Elektrotechniczny, vol. R.92, no. 7, pp. 69-71, 2016.
- [34] Puchala D., Stokfiszewski K., *Numerical Accuracy of Integral Images Computation Algorithms*, IET Image Processing, 2017.
- [35] Viola P., Jones M. J., *Robust Real-time Face Detection*, International Journal of Computer Vision, vol. 57, no 2, pp. 137-154, 2004.
- [36] Puchala D., Stokfiszewski K., *Low-complexity Approximation of 8-point DCT for Image Compression*, Journal of Applied Computer Science, vol. 20, no. 2, pp. 107-117, 2012.