Program Maple do szyfrowania i deszyfrowania plików, zapisanych na dyskach i na nośnikach wymiennych

Maple implementation of an interactive application for cryptographic protection of files stored on hard disk and portable memory devices

Czesław Kościelny[1]

Treść: Opisano przykład interaktywnej aplikacji typu `workhsheet` uruchamianej w środowisku Maple 2015.1 i realizującej zadania „bezkluczowego" szyfrowania i deszyfrowania plików. Aplikacja jest prosta w obsłudze, ponieważ użytkownik nie wprowadza żadnych danych tylko używa myszy. Program posiada prosty graficzny interfejs użytkownika i przeznaczony jest głównie do kryptograficznej ochrony plików przechowywanych na dyskach i na nośnikach wymiennych. Aplikacja wyjątkowo skutecznie i niezawodnie chroni pliki przed nieupoważnionym dostępem.

Słowa kluczowe: funkcja biblioteczna Maple convert/base, szyfrowanie symetryczne plików.

Abstract: An example of an interactive implementation Maple worksheet application which performs the „keyless" file encryption or decryption by means of the symmetric cipher has been presented. The application has simple graphical user interface and may be used mainly for cryptographic protection of files stored in disks and in portable memory devices. The application very effectively protect files against unauthorized access.

Keywords: Maple convert/base built-in function, symmetric file encryption

Training sequence decomposition

Dekompozycja ciągu uczącego

Swietłana Lebiediewa[1]

Treść: Sformułowano problem dekompozycji ciągu uczącego (CU). Zdefiniowano dwa rodzaje dekompozycji CU dla scentralizowanej bazy danych (SBD). Udowodniono twierdzenia dotyczące zajętości pamięci przez CU po dekompozycji. Oszacowano złożoność obliczeniową algorytmów dekompozycji. Przedstawiono wyniki eksperymentu obliczeniowego ilustrującego zajętość pamięci w zależności od rodzaju dekompozycji, redundancji cech w drzewie i na ścieżce oraz wysokości drzewa.

Słowa kluczowe: baza danych, rozpoznawanie wieloetapowe, ciąg uczący, dekompozycja

Abstract: The problem of decomposition of a training sequence (TS) is formulated. Two types of TS decomposition for a centralized database are formulated. Theorems concerning memory occupancy by the TS after decomposition are proved. The calculation complexity of decomposition algorithms is estimated. The results of a calculation experiment are presented that illustrate memory occupancy depending on the decomposition type, the redundancy of features in the tree, the path, and the tree height.

Keywords: database, multistage recognition, training sequence, decomposition

Approximation algorithm supported on minimizing the Kullback-Leibler information divergence in some class of dynamical systems (October 2015)

Algorytm aproksymacyjny w oparciu o informację Kullbacka-Leiblera w pewnej klasie systemów dynamicznych

Jan Owedyk[1], Zdzisław Mathia[2], Hubert Zarzycki[2]

Treść: W pracy przedstawiono algorytm, który umożliwia skonstruowanie przybliżonych rozwiązań dla pewnej klasy systemów dynamiczych opisujących ewolucję w czasie gęstości prawdopodobieństwa. Przybliżone rozwiązania otrzymujemy minimalizując informację Kullbacka-Leiblera przy dodatkowych warunkach.
Wykazano, że pochodna informacji Kullbacka-Leiblera dla dokładnych i przybliżonych rozwiązań jest opisana przez tą samą formułę. W konsekwencji gdy w dynamicznym systemie maleje informacja Kullbacka-Leiblera dla dokładnych rozwiązań to także maleje dla przybliżonych rozwiązań.

Słowa kluczowe: Algorytm aproksymacyjny, Informacja Kullbacka-Leiblera, Metoda minimalizacji, Równania Fokkera-Plancka

Abstract: In this work an algorithm is presented for creating approximate solutions in some class of dynamical systems describing the time evolution probability densities. The approximate solutions are obtained by minimizing Kullback-Leibler divergence under some constrains.
It is shown that the derivatives of the Kullback-Leibler divergence for exact solutions and for approximate solutions are described by the same formula. In consequence if in a dynamical system the Kullback-Leibler divergence decreases in time for exact solutions, it also decreases for approximate solutions.

Keywords: Approximation algorithm, Kullback-Leibler divergence, Minimization methods, Fokker-Planck equation

Wielkoskalowe symulacje biologicznych sieci neuronowych charakteryzujących się wewnętrzną topologią wielowymiarowych torusów z wykorzystaniem PGENESIS

Large-scale simulations of biological neural networks characterized by internal topology of multi-dimensional torus using PGENESIS

Monika Kwiatkowska[1] i Łukasz Świerczewski[2]

Treść: Praca obejmuje implementacje oraz testy wydajności i skalowania biologicznych sieci neuronowych charakteryzujących się wewnętrzną topologią wielowymiarowych torusów. Do obliczeń wykorzystano równoległą wersję symulatora GENESIS - PGENESIS. Symulacje przeprowadzono w środowisku równoległym na superkomputerze (klaster wydajnościowy o architekturze x86_64) HP BladeSystem/Actina, Hydra dostępnym w Interdyscyplinarnym Centrum Modelowania Matematycznego i Komputerowego Uniwersytetu Warszawskiego. Testy objęły procesory AMD Opteron 2435, AMD Opteron 6174, AMD Opteron 6272 oraz Intel Xeon X5660. Uwzględniono także aspekt wykorzystania interfejsów sieciowych Infiniband QDR, Infiniband DDR oraz 10Gb Ethernet w komunikacji międzywęzłowej. Dodatkowo wykonano analizę uzyskanego zysku wydajności dzięki zastosowaniu wersji PGENESIS skompilowanej pod kątem wybranego procesora. W pracy skupiono się jedynie na części dotyczącej pomiarów wydajności – nie podjęto jakichkolwiek prób analiz aktywności modelowanych biologicznych sieci neuronowych.

Słowa kluczowe: PGENESIS, biologiczne sieci neuronowe, topologia torus

Abstract: This paper includes implementation and performance tests and also scaling of biological neural networks characterized by internal topology of multi-dimensional toruses. For calculations there was used a parallel version of the GENESIS - PGENESIS simulator. Simulations were performed in a supercomputer's parallel environment, (a performance cluster with x86_64 architecture) HP BladeSystem/Actina, Hydra available at the Interdisciplinary Centre for Mathematical and Computational Modeling, Warsaw University. Tests included AMD Opteron 2435, AMD Opteron 6174, AMD Opteron 6272 and Intel Xeon X5660 prosessors. There was also taken into account the aspect of the use of network interfaces such like Infiniband QDR, DDR Infiniband and 10Gb Ethernet in interstitial communication. In addition, there was performed an analysis on the resulting performance gained by using the PGENESIS version compiled for the selected processor. In this paper author focused only on the section of performance measurement - there weren't taken any attempts of activity analysis of the modeled biological neural networks.

Keywords: PGENESIS, biological neural networks, torus topology

Testowanie przypuszczenia Beal'a z wykorzystaniem klasycznych procesorów

Testing Beal conjecture using classical processors

Monika Kwiatkowska[1] i Łukasz Świerczewski[2]

Treść: Praca obejmuje testowanie przypuszczenia Beal'a z wykorzystaniem klasycznych procesorów. Dodatkowo w wybranych funkcjach oprogramowania wykorzystano standard OpenMP, co umożliwiło zrównoleglenie obliczeń. Do obliczeń wykorzystano jednostki obliczeniowe wchodzące w skład komputerów IBM Blue Gene/P, IBM Blue Gene/Q oraz IBM Power 775. Testy wykonano także na superkomputerze HP BladeSystem/Actina, Hydra dostępnym w ICM UW - użyto tam węzła obliczeniowego posiadającego dwa procesory Intel Xeon X5660. Porównano wydajność własnych rozwiązań napisanych w języku C z możliwościami oprogramowania napisanego w języku Python przez Peter'a Novig'a.

Słowa kluczowe: przypuszczenie Beal'a, Blue Gene/P, Blue Gene/Q, Power 775

Abstarct: This paper includes the testing of Beal's conjecture using classical processors. Additionally some features of OpenMP standard were used in software what allowed to parallel the calculation. Calculations were based on computational units included in the computers IBM Blue Gene/L, IBM Blue Gene/Q, and the IBM Power 775 tests have been performed on the supercomputer HP BladeSystem / Actina, Hydra available in the ICM UW - computing nodes with Intel Xeon processors X5660 were used there. The performance of own solutions written in C was compared with the capabilities of software written in Python by Peter Novig.

Keywords: Beal conjecture, Blue Gene/P, Blue Gene/Q, Power 775

Acknowledgment

Interdisciplinary Centre for Mathematical and Computational Modeling (ICM), Warsaw University, Poland is acknowledged for providing the computer facilities under the Grant No. G55-11.

Śledzenie obiektów z wykorzystaniem obrazowania spektralnego

Object tracking with spectral imagery

Krzysztof Tutak[1], Mateusz Pieszko[1]

Treść. Niniejsza praca poświęcona jest analizie skuteczności śledzenia obiektów przy pomocy obrazowania spektralnego wykonywanego za pomocą 16-kanałowej kamery spektralnej rejestrującej dane w trybie wideo w zakresie 400-1000 nm. Wykorzystano algorytm Lucas-Kanade, wyznaczający przepływ optyczny w charakterystycznych punktach obrazu, określonych metodą Shi-Tomasi. Śledzenie inicjowane jest ręcznie poprzez wskazanie prostokątnego okna zawierającego obiekt. Do przetwarzania wybierany jest monochromatyczny obraz odpowiadający długości fali, dla której liczba punktów leżących w tym oknie jest największa. Zastosowano reprezentację obrazu w formie piramidy, dzięki czemu zmniejszono zależności od zmian skali obserwowanego obiektu. Otrzymane w każdym kroku śledzenia nowe pozycje punktów charakterystycznych były analizowane w celu odrzucenia obserwacji odstających. Wykonano szereg eksperymentów polegających na próbie śledzenia makiety samochodu wojskowego w trudnych warunkach oświetlenia i przy niejednorodnym tle o kolorystyce zbliżonej do barw maskujących pojazdu. Otrzymane rezultaty potwierdziły zasadność stosowania obrazowania spektralnego do śledzenia obiektów.

Słowa kluczowe: obrazowanie spektralne, przetwarzanie obrazów, śledzenie obiektów, przepływ optyczny, spektralny system wizyjny

Abstract. This paper is devoted to the analysis of the effectiveness of object tracking with spectral imagery performed with a 16-channel spectral video camera operating in the 400-1000 nm range. We used the Lucas-Kanade algorithm which computes the optical flow at characteristic points of the image which were determined by the Shi-Tomasi method. The tracking is initialized manually by pointing to a rectangular window containing the object. Monochrome image corresponding to the wavelength for which the number of points lying in this window is the greatest is selected for processing. We used a representation of an image in the form of a pyramid, so that dependence on scale changes of the observed object was reduced. New positions of characteristic points received in each step of tracking were analyzed in order to reject outliers. We performed a series of experiments that tries to track military vehicle model under difficult lighting conditions and heterogeneous background of a color similar to the vehicle masking colors. Obtained results confirmed the advisability of applying spectral imagery for object tracking.

Keywords: hyperspectral imaging, image processing, object tracking, optical flow, spectral vision system