Universitatea “Alexandru Ioan Cuza” din Iaşi
Facultatea de Informatică

LUCRARE DE DISERTAŢIE

Awesome Name

propusă de

Student: Oriana-Maria Oniciuc
Coordonator ştiinţific: Conf. Dr. Liviu Ciortuz

Sesiunea: iulie
2018

Universitatea “Alexandru Ioan Cuza” din Iaşi
Facultatea de Informatică

Awesome Name

Student: Oriana-Maria Oniciuc
Coordonator ştiinţific: Conf. Dr. Liviu Ciortuz

Sesiunea: iulie
2018

DECLARAŢIE PRIVIND ORIGINALITATE ŞI RESPECTAREA DREPTURILOR DE AUTOR

Prin prezenta declar că Lucrarea de disertaţie cu titlul "Awesome Name" este scrisă de mine şi nu a mai fost prezentată niciodată la o altă facultate sau instituţie de învăţământ superior din ţară sau străinătate. De asemenea, declar că toate sursele utilizate, inclusiv cele preluate de pe Internet, sunt indicate în lucrare, cu respectarea regulilor de evitare a plagiatului:

- toate fragmentele de text reproduse exact, chiar şi în traducere proprie din altă limbă, sunt scrise între ghilimele şi deţin referinţa precisă a sursei;
- reformularea în cuvinte proprii a textelor scrise de către alţi autori deţine referinţa precisă;
- codul sursă, imaginile etc. preluate din proiecte open-source sau alte surse sunt utilizate cu respectarea drepturilor de autor şi deţin referinţe precise;
- rezumarea ideilor altor autori precizează referinţa precisă la textul original.

Iaşi,
XX iunie 2018

Absolvent,
Oniciuc Oriana-Maria

_____

(semnătura în original)

DECLARAŢIE DE CONSIMŢĂMÂNT

Prin prezenta declar că sunt de acord ca Lucrarea de disertaţie cu titlul "Awesome Name", codul sursă al programelor şi celelalte conţinuturi (grafice, multimedia, date de test etc.) care însoţesc această lucrare să fie utilizate în cadrul Facultăţii de Informatică.

De asemenea, sunt de acord ca Facultatea de Informatică de la Universitatea "Alexandru Ioan Cuza" din Iaşi să utilizeze, modifice, reproducă şi să distribuie în scopuri necomerciale programele-calculator, format executabil şi sursă, realizate de mine în cadrul prezentei lucrări de disertaţie.

Iaşi,
XX iunie 2018

Absolvent,
Oniciuc Oriana-Maria

_____

(semnătura în original)

Abstract

This paper aims is to produce a method that classifies phonocardiograms corresponding to different heart symptoms that are extremely subtle and challenging to separate. The problem is of particular interest to machine learning researchers as it involves classification of audio sample data, where distinguishing between classes of interest is non-trivial. Data is gathered in real-world situations and frequently contains background noise of every conceivable type. Despite its medical significance, to date this is a relatively unexplored application for machine learning.

Some attempts to segment phonocardiograms (PCG) into heartbeats can be found in the literature. The characteristics of the PCG signal and other features such as heart sounds S1 and S2 location can be measured more accurately by digital signal processing techniques. Basic frequency content of PCG signal can be easily provided using Fast Fourier Transform technique. However, time duration and transient variation cannot be resolved just through FFT, and in this case the Continuous Wavelet Transform is a more suitable technique to analyze such a signal. The coefficients of the CWT give a graphic representation that is very helpful in extracting quantitative analysis simultaneously in time and frequency.

For the classification task some of the representative work that was done, has been presented in Classifying Heart Sounds Workshop. The teams used the J48 and MLP algorithms (using Weka) to train and classify the computed features, or exploit domain knowledge and compares the features of heartbeat before and after dropping out extra peaks and the smallest interval, used partial least squares regression, neural networks and convolution neural networks. The classification task in this project aims to give an alternative architecture for the convolution neural network proposed in Classification of Heart Sound Recordings using Convolution Neural Network.

Contents

I. Introduction

According to the World Health Organization, cardiovascular diseases are the number one cause of death globally. These diseases have remained the leading causes of death in the last 15 years. Any work done in detecting signs of heart disease could therefore have a significant impact on world health.

Classifying Heart Sounds PASCAL provides us with a dataset that is gathered in real-world situations and frequently contains background noise of every con- ceivable type, being recorded both in a Hospital environment by a doctor (using a digital stethoscope) and at home by the patient (using a mobile device). Success in classifying this form of data requires multiples pre-processing of the audio record- ings. This part of the research presents an overview of approaches to analysis of heart sound signals. The main purpose of this study is developing an automatic methodology for identifying systole and diastole in the phonocardiograms and to classify the heartbeats in three classes.

II. Elemente de criptografie

II.1. Criptografie

Criptografia a apărut pe vremea egiptenilor, cu peste 4000 de ani în urmă. În principal, până la începutul secolului al XX-lea, criptografia s-a ocupat mai ales de şabloane lingvistice. De atunci, accentul s-a mutat pe folosirea extensivă a matematicii, inclusiv a aspectelor de teoria informaţiei, complexitatea algoritmilor, statistică, combinatorică, algebră abstractă şi teoria numerelor. Din punct de vedere lexicografic, cuvântul *criptografie* este format din rădăcinile *cryptos* şi *grafie*.

$$\text{Criptografie} = \textit{cryptos}(\text{ascuns}) + \textit{grafie}(\text{a scrie})$$

Criptografia este o componentă a domeniului securităţii informaţiei şi poate fi definită astfel:

Definition 1. *Criprografia* este studiul tehnicilor matematice care se ocupă de următoarele aspecte ale securităţii informaţiei: confidenţialitatea, autentificarea, non-repudierea mesajelor şi integritatea datelor.

Principalele obiective ale unui sistem criptografic sunt:

- *Confidenţialitatea*: proprietatea de a păstra secretul informaţiei, astfel încât aceasta să fie utilizată numai de către persoane autorizate.
- *Autentificarea*: proprietatea de a identifica o entitate conform anumitor standarde. Aceasta implică:
  1. Autentificarea unei entităţi;
  2. Autentificarea sursei informaţiei.
- *Non-repudierea*: proprietatea care previne negarea unor evenimente anterioare.
- *Integritatea datelor*: proprietatea de a evita orice modificare (inserare, ştergere, substituţie) neautorizată a informaţiei.

Bibliography

[1] Popa Raluca Ada. *Building Practical Systems That Compute on Encrypted Data*. PhD thesis, Massachusetts Institute of Technology, 2014.

[2] Atanasiu Adrian. Curs - criptografie, 2016.

[3] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, pages 563–574. ACM, 2004.

[4] Niv Ahituv, Yeheskel Lapid, and Seev Neumann. Processing encrypted data. *Commun. ACM*, 30(9):777–780, September 1987.

[5] Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam O'Neill. *Order-Preserving Symmetric Encryption*, pages 224–241. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[6] Alexandra Boldyreva, Nathan Chenette, and Adam O'Neill. *Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions*, pages 578–595. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[7] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Second Edition*. The MIT Press, Cambridge , Massachusetts London, England, 2001.

[8] Joan Feigenbaum, Mark Y. Liberman, and Rebecca N. Wright. Cryptographic protection of databases and software. In *In Distributed Computing and Cryptography*, pages 161–172. American Mathematical Society, 1991.

[9] Iacob Florin. Curs - matematică, 2005.

[10] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, August 1986.

[11] Voratas Kachitvichyanukul and Bruce W. Schmeiser. Algorithm 668: H2pec: Sampling from the hypergeometric distribution. *ACM Trans. Math. Softw.*, 14(4):397–398, December 1988.

[12] Tiplea Ferucio Laurentiu. Curs - calculabilitate, decidabilitate şi complexitate, 2015.

[13] Tiplea Ferucio Laurentiu. Curs - coduri şi criptografie, 2015.

[14] Ponemon Institute LLC. 2015 cost of data breach study: Global analysis, 2015.

[15] F. López-Blázquez and B. Salamanca-Miño. Exact and approximated relations between negative hypergeometric and negative binomial probabilities. *Communications in Statistics - Theory and Methods*, 30(5):957–967, 2001.

[16] Cameron McDonald. *Analysis of Modern Cryptographic Primitives*. PhD thesis, Macquarie University, 2010.

[17] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Cambridge , Massachusetts London, England, 1996.