

**BIOMETRICS,
COMPUTER SECURITY SYSTEMS
AND
ARTIFICIAL INTELLIGENCE
APPLICATIONS**

BIOMETRICS, COMPUTER SECURITY SYSTEMS AND ARTIFICIAL INTELLIGENCE APPLICATIONS

Edited by

Khalid Saeed

Bialystok Technical University, Poland

Jerzy Pejaś

Szczecin University of Technology, Poland

Romuald Mosdorf

Bialystok Higher School of Finance and Management, Poland

 **Springer**

Khalid Saeed
Białystok Technical University
Faculty of Computer Science
Wiejska 45A
15-351 Białystok
POLAND
Email: aida@ii.pb.bialystok.pl

Jerzy Pejaś
Szczecin University of Technology
Faculty of Computer Science
Zolnierska 49
71 210 Szczecin
POLAND
Email: jpejas@wi.ps.pl

Romuald Mosdorf
University of Finance and
Management in Białystok
Ciepła 40
15 472 Białystok
POLAND
Email: mosdorf@wsfiz.edu.pl

Library of Congress Control Number: 2006928847

Biometrics, Computer Security Systems and Artificial Intelligence Applications
Edited by Khalid Saeed, Jerzy Pejaś, and Romuald Mosdorf

ISBN-13: 978-0-387-36232-8
ISBN-10: 0-387-36232-0
e-ISBN-13: 978-0-387-36503-9
e-ISBN-10: 0-387-36503-6

Printed on acid-free paper.

© 2006 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1

springer.com

FOREWORD

The book to which I was asked by the editors to write a foreword is an interesting collection of contributions. It presents the extended versions of the authors' works already introduced at the International Multi-Conference on Advanced Computer Information and Security Systems ACS-CISIM 2005. These contributions had already been reviewed once before the conference for presentation at the conference while some of them passed another selection to be prepared in their current versions for this book.

I am convinced the book will be of help to the researchers in the field of Computer Methods in Biometrics, Security Systems and Artificial Intelligence. They would find the contributions of other researchers of real benefit to them.

I would encourage those who have the book in hands to read it.

Professor Andrzej Salwicki

*Faculty of Mathematics,
Informatics and Mechanics
Warsaw University, Poland*

ACKNOWLEDGEMENTS

The editors are thankful to all contributors whose works have proved to be of great interest to all participants of the International Conference ACS-CISIM, which was held in Elk, Poland in summer 2005.

We also are greatly indebted to the Invited Speakers for their really worth listening and reading keynote talks.

The book could not have appeared without the deep devotion and hard effort of the reviewers, to whom the editors and the contributors really feel grateful. Their reviews for both the Conference Proceedings and this Postconference Book were of great benefit especially to the young researchers whose work still needed others' professional expertise and comments despite the fact that their scientific research output was positively evaluated. Most of the reviewers did proofreading instead of refereeing. We really are proud of having the book contributions reviewed by them.

Therefore, our indebtedness is due to all the following Professors:

- | | |
|--------------------------------|---------------------------------|
| 1) <i>Abraham Ajith</i> | 14) <i>Ochin Evgeny</i> |
| 2) <i>Bagiński Czesław</i> | 15) <i>Petrovsky Alexander</i> |
| 3) <i>Bartkowiak Anna</i> | 16) <i>Piegat Andrzej</i> |
| 4) <i>Bielecki Włodzimierz</i> | 17) <i>Rakowski Waldemar</i> |
| 5) <i>Bobrowski Leon</i> | 18) <i>Rogoza Walery</i> |
| 6) <i>Choraś Ryszard S.</i> | 19) <i>Salwicki Andrzej</i> |
| 7) <i>Dańko Wiktor</i> | 20) <i>Skarbek Władysław</i> |
| 8) <i>Huntsinger Ralph</i> | 21) <i>Akira Imada</i> |
| 9) <i>Jarmolik Vyacheslav</i> | 22) <i>Stepaniuk Jarosław</i> |
| 10) <i>Kuriata Eugeniusz</i> | 23) <i>Stokłosa Janusz</i> |
| 11) <i>Kompanets Leonid</i> | 24) <i>Tadeusiewicz Ryszard</i> |
| 12) <i>Madani Kurosh</i> | 25) <i>Wierzchoń Sławomir</i> |
| 13) <i>Mirkowska Grażyna</i> | |

Editors: Khalid Saeed, Jerzy Pejaś, Romuald Mosdorf

INTRODUCTION

This book presents the most recent achievements in the field of a very fast developing Computer Science. It is a very fascinating science, which still encompasses a number of uncovered areas of study with urgent problems to be solved. Therefore, thousands of scientists are dealing with it elaborating on more and more practical and efficient methods. It is likely that their work will soon result in construction of a very effective, artificial computer-brain.

All scientific works presented in this book have been partitioned in three topical groups:

1. Image Analysis and Biometrics,
2. Computer Security Systems,
3. Artificial Intelligence and Applications.

All papers in the book are noteworthy, but especially we would like to draw the reader's attention to some particular papers beginning from part 1.

Image analysis and biometrics is the branch of Computer Science, which deals with a very difficult task of artificial, visual perception of objects and surroundings and problems connected with it. To the most remarkable papers in this part certainly

belongs the invited paper of Anna Bartkowiak et al. where the authors present an interesting mathematical model showing their experience in visualization multivariate data. In his invited paper, Ryszard Choraś introduces a survey on Content-Based Image Retrieval showing his and others' last achievements in this field. Three innovative papers on Face Recognition are also given in the same part. The remaining papers outline their authors' contribution to Speech Analysis, Signature Recognition using Dynamic Time Warping algorithm and hybrid fused approaches for Speech and Speaker Identification.

Computer Security and Safety is at present a very important and intensively investigated branch of Computer Science because of the menacing activity of hackers, of computer viruses etc. To the most

interesting papers in this chapter belongs the invited paper of Janusz Stokłosa et al. It contains an excellent overview of experiments in designing S-boxes based on nonlinear Boolean functions. The authors present also their new algorithm for random generation of perfect nonlinear function. Krzysztof Chmiel's paper concerns also S-boxes, but in contrast to the previous paper, the author discusses the problem of the differential and the linear approximations of two classes of S-box functions. Two other papers relate to PKI services, which can be used for sending sensitive information and for the public key certificate status validation.

The third part of the book **Artificial Intelligence** contains 15 absorbing papers, five of which are keynotes and invited papers. The keynotes and invited papers presented at or sent to the ACS-CISIM 2005 conference introduce the latest achievements of their authors W. Dańko, G. Facchinetti et al., A. Imada, K. Madani, G. Mirkowska with

A. Salwicki (their keynote paper is not included in this book on their request),

R. Tadeusiewicz et al. and S. Wierzchoń et al. The new approaches or notes they show in Computer Artificial Intelligence and its applications are really worth making use of. The remaining papers in this part demonstrate the latest scientific results in the works of their authors in different aspects and areas of Computer Science and its wide applications.

The works contained in the presented book will surely enable you, Dear Reader, to keep pace with significant developments in Computer Science.

We wish you a great satisfaction from reading it.

Professor Leon Bobrowski, Dean
Faculty of Computer Science
Białystok Technical University
Poland

Professor Andrzej Piegat, Dean
Faculty of Computer Science
Szczecin University of Technology,
Poland

TABLE OF CONTENTS

PART I - IMAGE ANALYSIS AND BIOMETRICS

<i>ANDRYSIAK Tomasz, CHORAŚ Michał</i> Image Filtration and Feature Extraction for Face Recognition	3
<i>BARTKOWIAK Anna, EVELPIDOU Niki</i> Visualization of Some Multi-Class Erosion Data Using GDA and Supervised SOM	13
<i>BOBULSKI Janusz</i> Wavelet Transform in Face Recognition	23
<i>CHORAŚ Ryszard S.</i> Content-Based Image Retrieval – A Survey	31
<i>KUBANEK Mariusz</i> Method of Speech Recognition and Speaker Identification Using Audio-Visual of Polish Speech and Hidden Markov Models	45
<i>LIVSHITZ Michael, PETROVSKY Alexander</i> Synthesis of Codebooks with Perceptually Monitored Structure for Multiband CELP-Coders	57
<i>MICIAK Mirosław</i> The Color Information as a Feature for Postage Stamps Recognition	69
<i>RYDZEK Szymon</i> Iris Shape Evaluation in Face Image with Simple Background	79
<i>SAEED Khalid, ADAMSKI Marcin</i> Experimental Algorithm for Characteristic Points Evaluation in Static Images of Signatures	89

PART II - COMPUTER SECURITY SYSTEMS

<i>BIELECKI Włodzimierz, BURAK Dariusz</i> Parallelization of Standard Modes of Operation for Symmetric Key Block Ciphers	101
---	-----

<i>CHMIEL Krzysztof</i> On Differential and Linear Approximation of S-box Functions	111
<i>GROCHOLEWSKA-CZURYŁO Anna, STOKŁOSA Janusz</i> Random Generation of S-Boxes for Block Ciphers	121
<i>KURIATA Eugeniusz</i> Problems of Sending Sensitive Information	137
<i>KURIATA Eugeniusz, MAĆKÓW Witold, SUKIENNIK Paweł</i> Hash Chaining for Authenticated Data Structures Freshness Checking	155
<i>PUCZKO Mirosław, YARMOLIK Vyatcheslav N.</i> Stream Cipher Keys Generation with Low Power Consumption Based on LFSR	165
<i>WITKOWSKA Joanna</i> The Quality of Obfuscation and Obfuscation Techniques	175

PART III - ARTIFICIAL INTELLIGENCE AND APPLICATIONS

<i>ADDABBO Tindara, FACCHINETTI Gisella, MASTROLEO Giovanni</i> Capability and Functionings: A Fuzzy Way to Measure Interaction between Father and Child	185
<i>DAŃKO Wiktor</i> Remarks on Computer Simulations	197
<i>IGNATOWSKA Bożena, MOSDORF Romuald</i> Analysis of E-learning System Dynamics	207
<i>IMADA Akira</i> Can a Negative Selection Detect an Extremely Few Non-self Among Enormous Amount of Self Cells?	217
<i>KARBOWSKA-CHILIŃSKA Joanna</i> An Average Length of Computations of Normalized Probabilistic Algorithms	227

<i>ŁEBKOWSKI Andrzej, DZIEDZICKI Krzysztof, TOBIASZ Marcin, ŚMIERZCHALSKI Roman, TOMERA Mirosław</i>	237
A Marine Environment Simulator for Testing Ship Control Systems in Dangerous Situations	
<i>MADANI Kurosh</i>	247
Image Enhancement and Image Half-toning Using Fluid Particles Physics Dynamics	
<i>ONISZCZUK Walenty</i>	259
Tandem Models with Blocking in the Computer Subnetworks Performance Analysis	
<i>PIECH Henryk, PTAK Aleksandra, MACHURA Marcin</i>	269
Interchangeable Strategies in Games Without Side Payments on the Base of Uncertain Information on Resources	
<i>PIEKARSKI Krzysztof, TADEJKO Paweł, RAKOWSKI Waldemar</i>	279
Properties of Morphological Operators Applied to Analysis of ECG Signals	
<i>REJER Izabela</i>	289
Input's Significance Evaluation in a Multi Input-Variable System	
<i>SZUSTALEWICZ Adam, VASSILOPOULOS Andreas</i>	299
Calculating the Fractal Dimension of River Basins, Comparison of Several Methods	
<i>TADEUSIEWICZ Ryszard, AUGUSTYNIAK Piotr</i>	311
Automatic Management of Tele-Interpretation Knowledge in a Wearable Diagnostic Device	
<i>WIERZCHOŃ Sławomir, KUŹELEWSKA Urszula</i>	323
Evaluation of Clusters Quality in Artificial Immune Clustering System - SARIS	
<i>ZIENIUK Eugeniusz, SZERSZEŃ Krzysztof, BOŁTUĆ Agnieszka</i>	333
Convergence Analysis of the Boundary Geometry Identification Obtained by Genetic Algorithms in the PIES	