Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems

Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems

Edited by

Jerzy Pejaś
Andrzej Piegat
Technical University of Szczecin, Poland

Springer

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Pejaś, J.
Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems/ edited by Jerzy Pejaś, Andrzej Piegat
p.cm.

ISBN 1-4020-7776-9 e-book 0-387-23484-5 Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11053675 (HC)

springeronline.com

Table of Contents

Chapter 2
Biometric Systems

Chapter 3
Methods of Artificial Intelligence and Intelligent Agents

Preface

The book contains mainly (but not only) works of European scientists investigating problems in the area of computer science.

The works give a picture of the present state and progress concering this field of science and show directions of contemporary research investigations. Authors present new scientific methods and show how these methods and other well known methods could be used to solve some particular practical problems.

All papers contained in the book were assembled into 3 chapters:

1. Methods of Artificial Intelligence and Intelligent Agents,
2. Information Technology Security,
3. Biometric Systems.

Chapter 1 contains 13 papers comprising various areas of artificial intelligence such as: fuzzy set theory, predicate logic, neural networks, fuzzy arithmetic, expert systems, evolutionary computations, clustering, data mining and others. The 7 of all 13 papers present applications of artificial intelligence in solution of such practical problems as: requalification of contaminated sites, training of aviation pilots, ship control, firm bankruptcy, stock market, soil erosion, and flight control.

All papers are interesting but especially I would like to draw the reader attention to some particular papers, beginning from **Chapter 1**.

A very interesting paper in this chapter is the paper "*A fuzzy expert approach for comparing alternative end uses for requalification of contaminated sites*" prepared by a group of Italian scientists: G. Facchinetti, I. Mannino, G. Mastroleo, and S. Soriani. To make the decision "how a contaminated site of a country should be used after their remediation" is very difficult, because many features of the site and many future possible destinations of it have to be taken into account. The features and destinations mostly can not be evaluated numerically (ie.: using the numeric values) but only with use of linguistic, fuzzy evaluations. The authors show how multi-dimensional fuzzy problem can be solved by its decomposition and application of fuzzy logic.

In the paper "Choosing representative data items: Kohonen, Neural Gas or Mixture Model?- A case of erosion data" by A. Bartkowiak and co-authors accomplish an interesting comparison of various neural models used as representatives of a big data sets. It is a very practical problem - how effective are various types of neural networks? This effectiveness can probably be evaluated only by specific experimental investigations - and the authors applied this method.

I would like also draw the reader attention to a very important but underestimated problem of the neural model extrapolation outside the region

covered by measurement data. The problem is presented in the paper "*Algorithm for automatic definition of validated and non-validated region in multi-dimensional space*" written by P. Klęsk. The extrapolation problem is generally not noticed by users of neural models and other types of models, what results in many errors, mistakes and false evaluation of neural networks. The author shows a method, which allows to detect in which region of the problem space calculations delivered by a model can be trusted and where can not.

The problems and their solutions presented in the **Chapter 2** "Information Technology Security" belong to three important areas of security engineering in information systems: analysis of software security, public key infrastructure, and development/design of new cryptographic algorithms and protocols.

Analysis of software security aims mainly at detection of software errors, construction of appropriate techniques of software creation (e.g. of an error-robust ones) and at evaluation of the software influence on security of the whole information system. From this point of view of the software user the software itself and generally the whole information system has to be secure and has to realize only such tasks, which are compatible with its specification. Thus a prerequisite of the information system is the trust of its users that the system is able to contribute to the achievements of the business objectives of users, to bring them some benefits. The problem of the IT-trust analysis and of increasing the trust was presented in the papers "*How to justify trust in software based systems?*" by J. Górski and "*Tool support for* detecting *defects in object-oriented models*" by J. Górski and co-authors.

The technology of the public key infrastructure has no more been treated as a technical novelty since a long time. There exist many proves that its practical application gives many benefits and considerable savings. One of such examples is given in the paper "*Integrated payment system for public key infrastructure services*" by I. E. Fray and J. Pejaś. The nEPSKIP-system proposed in the paper may be used not only to account the PKI-services but also to other doubled services as e.g. bank clearing. However, construction of that services must be supported by other PKI-components, such as by service of the certificate status verification and devices for secure signature signing. Proposals of a novelty solution of the two components enable an easier usage of the PKI-technology and increase its usefulness for creation of e-society.

Cryptographic algorithms have to guarantee a high resistance level against break and a high speed of coding/decoding operations. The high speed can be achieved not only by application of appropriate calculation and information processing methods but by parallelization of operations as well. In the paper by V. Beletskyy and D. Burak "*Parallelization of the data encryption standard (DES) algorithm*" the authors show that also classical algorithms as DES can be parallelized, though its structure is not based on operations of parallelization. A new cryptographic algorithm is also presented in the paper of T. Hebisz and E. Kuriata "*The capacity of ciphers fulfilling the accessibility of cryptograms*". The authors propose a new cipher algorithm based on the techniques of error correction coding, which enable detection of changes and manipulations on cryptograms. They present also the VAST-system, which ensures WWW-users' confidentiality in the network.

Chapter 3 "Biometric Systems" is devoted to problems of processing and analysis of human features for person recognition and identification. It contains description of chosen algorithms and their implementations for personal computers,

in form of introductory descriptions and ready software systems as well. The chapter comprises 11 papers dealing mainly with the face picture analysis (6 papers) and recognition systems (3 papers). Analysis of the presented papers shows that investigations connected with biometric systems are going towards a few directions. The first of them is the design of new models, the second one is the usage of known and sometimes even classical methods of biometric problems solution, and the third direction is an implementation of the methods in form of active computer systems.

A complex model of a human face was presented in the paper "Częstochowa's precise model of a face based on the facial asymmetry, ophthalmogeometry, and brain asymmetry phenomena: the idea and algorithm sketch" by L. Kompanets and co-authors. The model is based on temporary knowledge about asymmetry, ophtalmogeometry, brain hemispheres functioning asymmetry phenomena and delivers tools useful in techniques of identity verification and person identification. It is also useful in investigation of human-computer interactions and person evaluation with respect to his/her cognition-psyche type.

The works "*An experimental criterion for face classification*" by K. Saeed and P. Charkiewicz present novel approaches to classification and to recognition. The approaches use eigenvalues obtained from Toeplitz matrices and have high effectiveness in comparison with other methods.

Application of the picture processing and recognition was presented in few papers. The first of them "*An environment for recognition system modeling*" by G. Kukharev and A. Kuźmiński describes a simulation system, which allows for planning of investigations and practical verification of many different methods. It is a valuable tool for scientists investigating different systems of picture recognition (not only in biometric tasks).

The paper "*The PCA reconstruction based approach for extending facial image databases for face recognition*" by L. Chen and co-authors presents application of the known PCA-method to improve operational effectiveness of face recognition systems. This method can be especially used in face databases, which includes incomplete information (e.g. missing picture of the face front or missing the side picture). In such difficult cases the method is able to reconstruct the missing picture data.

Implementation of chosen biometric algorithms is also the subject of the work:*"Modified gradient method for face localization"* written by G. Kukharev and co-authors. They propose a method that enables face localization in very complex pictures. An elaborated computer program allows for work in real time and guarantees high efficiency of the face localization independently from the scale and from the neighborhood conditions.

Remaining works presented in Chapter 3 refer to subjects closely connected with biometrics and methods that can find biometrical application. Their characteristic feature is the approach originality and possibility of practical implementation.

The works contained in presented book surely make you, Dear Reader, enable to keep pace with the siginificant development of computer science. I wish you a great satisfaction from the reading.

Professor Andrzej Piegat
Editor