ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING 195

Valentina Emilia Balas
János Fodor
Annamária R. Várkonyi-Kóczy
József Dombi
Lakhmi C. Jain (Eds.)

Soft Computing Applications

Springer

Advances in Intelligent Systems and Computing 195

Editor-in-Chief

Prof. Janusz Kacprzyk
Systems Research Institute
Polish Academy of Sciences
ul. Newelska 6
01-447 Warsaw
Poland
E-mail: kacprzyk@ibspan.waw.pl

For further volumes:
http://www.springer.com/series/11156

Valentina Emilia Balas, János Fodor,
Annamária R. Várkonyi-Kóczy, József Dombi,
and Lakhmi C. Jain (Eds.)

Soft Computing Applications

Proceedings of the 5th International Workshop Soft Computing Applications (SOFA)

Springer

Editors
Prof. Valentina Emilia Balas
Associate Professor
Aurel Vlaicu University from Arad
Arad
Romania

Prof. János Fodor
Professor
Institute of Applied Mathematics
Óbuda University
Budapest
Hungary

Prof. Annamária R. Várkonyi-Kóczy
Professor
Institute of Mechatronics and Vehicle
Engineering
Obuda University
Budapest
Hungary

Prof. József Dombi
Department of Informatics
University of Szeged
Szeged
Hungary

Prof. Lakhmi C. Jain
School of Electrical and Information
Engineering
University of South Australia
Adelaide
South Australia SA
Australia

ISSN 2194-5357
e-ISSN 2194-5365
ISBN 978-3-642-33940-0
e-ISBN 978-3-642-33941-7
DOI 10.1007/978-3-642-33941-7
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2012949235

© Springer-Verlag Berlin Heidelberg 2013
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the Proceedings of the 5$^{\mathrm{th}}$ International Workshop on Soft Computing Applications (SOFA 2012). The main goal of the Workshop is to communicate and publish new theoretical and applicative research results, in the areas of Fuzzy Logic, Neural Networks, Evolutionary Computing, and other methods belonging or connected to Soft Computing (SC). A second and just as important goal is to encourage new reflections on SC issues and new links between interested researchers, R&D engineers, managers and so on.

The concept of Soft Computing - which was introduced by Lotfi Zadeh in 1991 - serves to highlight the emergence of computing methodologies in which the accent is on exploiting the tolerance for imprecision and uncertainty to achieve tractability, robustness and low solution cost. The principal constituents of soft computing are fuzzy logic, neurocomputing, evolutionary computing and probabilistic computing, with the later subsuming belief networks, chaotic systems and parts of learning theory. Soft computing facilitates the use of fuzzy logic, neurocomputing, evolutionary computing and probabilistic computing in combination, leading to the concept of hybrid intelligent systems. Such systems are rapidly growing in importance and visibility.

Nowadays in our complex world all problems cannot be dealt with conventional mathematical methods. With the help of soft computing techniques, that offer complementary methods allowing flexible computing tools, it is possible to find good solutions.

The book covers a broad spectrum of soft computing techniques, theoretical and practical applications employing knowledge and intelligence to find solutions for world industrial, economic and medical problems. The combination of such intelligent systems tools and a large number of applications introduce a need for a synergy of scientific and technological disciplines in order to show the great potential of Soft Computing in all domains.

The conference papers included in these proceedings, published post conference, were grouped into the following area of research:

- Soft Computing and Fusion Algorithms in Biometrics,
- Fuzzy Theory, Control andApplications,
- Modelling and Control Applications,
- Steps towards Intelligent Circuits,

- Knowledge-Based Technologies for Web Applications, Cloud Computing and Security Algorithms,
- Computational Intelligence for Biomedical Applications,
- Neural Networks and Applications,
- Intelligent Systems for Image Processing,
- Knowledge Management for Business Process and Enterprise Modelling.

In SOFA 2012 we had five eminent Keynote Speakers: Professor Lotfi A. Zadeh (USA), Professor Michio Sugeno (JAPAN), Professor Kay Chen Tan (Singapore), Professor Michal Baczynski (Poland) and Professor Laszlo B. Kish (USA). Their summaries or extended talks are included in this book.

The book is directed to all interested readers to evaluate to potential of Soft Computing: researchers in laboratories and universities interested to solve real problems, managers looking for tools and new views to improve their business.

We especially thank the honorary chair of SOFA 2012 Prof. Lotfi A. Zadeh who encouraged and motivated us. He participated actively in our workshop of this edition by sending us an interesting video tape lecture.

Special thanks to Professor Michio Sugeno who showed a constant support during all these years by participating to the last four SOFA editions.

We would like to thank the authors of the submitted papers for keeping the quality of the SOFA 2012 conference at high levels. The editors of this book would like to acknowledge all the authors for their contributions and also the reviewers.

For their help with organizational issues of all SOFA editions we express our thanks to TRIVENT Conference Office, Mónika Jetzin and Teodora Artimon for having customized the software Conference Manager, registration of conference participants and all local arrangements.

Special thanks go to Janusz Kacprzyk (Editor in Chief, Springer, Advances in Intelligent and Soft ComputingSeries) for the opportunity to organize this guest edited volume.

We are grateful to Springer, especially to Dr. Thomas Ditzinger (Senior Editor, Applied Sciences & Engineering Springer-Verlag) for the excellent collaboration and patience during the evolvement of this volume.

We hope that the readers will find this collection of papers inspiring, informative and useful. We also hope to see you at a future SOFA event.

Valentina Emilia Balas, Romania
János C. Fodor, Hungary
Annamaria R. Várkonyi-Kóczy, Hungary
József Dombi, Hungary
Lakhmi C. Jain, Australia

Contents

Keynote Invited Talks

Soft Computing and Fusion Algorithms in Biometrics

Fuzzy Theory, Control and Applications

Modelling and Control Applications

Steps towards Intelligent Circuits

Knowledge-Based Technologies for Web Applications, Cloud Computing and Security Algorithms

Computational Intelligence for Biomedical Applications

Neural Networks and Applications

Intelligent Systems for Image Processing

Knowledge Management for Business Process and Enterprise Modeling

List of Contributors

Lotfi A. Zadeh
Department of EECS, University of California, Berkeley, USA

Michio Sugeno
European Centre for Soft Computing Mieres-Asturias, Spain

Kay Chen Tan
Department of Electrical and Computer Engineering, National University of Singapore, Singapore

Michał Baczyński
University of Silesia, Institute of Mathematics, Katowice, Poland

R. Mingesz
Department of Technical Informatics, University of Szeged, Hungary

Laszlo B. Kish
Texas A&M University, Department of Electrical and Computer Engineering, USA

Z. Gingl
Department of Technical Informatics, University of Szeged, Hungary

C.G. Granqvist
Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, Uppsala, Sweden

H. Wen
Texas A&M University, Department of Electrical and Computer Engineering, USA and Hunan University, College of Electrical and Information Engineering, China

F. Peper
National Institute of Information and Communication Technology, Kobe, Japan

T. Eubanks
Sandia National Laboratories, Albuquerque, USA

G. Schmera
Space and Naval Warfare Systems Center, San Diego, CA 92152, USA

Bojan Jovanović
University of Niš, Faculty of Electronic Engineering, Dept. of Electronics, Niš, Serbia

Milun Jevtić
University of Niš, Faculty of Electronic Engineering, Dept. of Electronics, Niš, Serbia

Tsung-Chih Lin
Department of Electronic Engineering, Feng-Chia University, Taichung, Taiwan

Wei-Nan Liao
Department of Electronic Engineering, Feng-Chia University, Taichung, Taiwan

Valentina Emilia Balas
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

Mircea A. Ciugudean
Politechnica University of Timisoara

Marius M. Balas
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

Marius Socaci
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

Onisifor Olaru
"Constantin Brancusi" University of Targu Jiu, Romania

Elisa Valentina Moisi
Department of Computer Science and Information Technology, Faculty of Electrical Engineering and Information Technology, University of Oradea, Oradea, Romania

Vladimir Ioan Cretu
Department of Computer and Software Engineering, "Politehnica" University of Timisoara, Timisoara, Romania

Benedek Nagy
Department of Computer Science, Faculty of Informatics, University of Debrecen, Debrecen, Hungary

Silviu Ioan Bejinariu
Institute of Computer Science, Romanian Academy, Iasi Branch

Florin Rotaru
Institute of Computer Science, Romanian Academy, Iasi Branch

Cristina Diana Niţă
Institute of Computer Science, Romanian Academy, Iasi Branch

Adrian Ciobanu
Institute of Computer Science, Romanian Academy, Iasi Branch

Mihaela Costin
Institute of Computer Science, Romanian Academy, Iasi Branch

Tudor Barbu
Institute of Computer Science, Romanian Academy, Iasi Branch

Dorel Aiordachioaie
Electronics and Telecommunications Department, "Dunarea de Jos" University of Galati, Galati, Romania

Laurentiu Frangu
Electronics and Telecommunications Department, "Dunarea de Jos" University of Galati, Galati, Romania

N.A. Chira
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

S.A. Matisan
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

F.M. Suciu
Department of Automation and Applied Informatics, Aurel Vlaicu University of Arad, Arad, Romania

Dragan G. Radojević
University of Belgrade, Mihajlo Pupin Institute, Belgrade, Serbia

Pavle Milošević
Faculty of Organizational Sciences, University of Belgrade, Belgrade

Ivan Nešić
Faculty of Organizational Sciences, University of Belgrade, Belgrade

Ana Poledica
Faculty of Organizational Sciences, University of Belgrade, Belgrade

Bratislav Petrović
Faculty of Organizational Sciences, University of Belgrade, Belgrade

Aleksandar Rakicevic
Faculty of Organizational Sciences, University of Belgrade, Belgrade

Emanuel Ciprian Sasu
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Octavian Prostean
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Radu Boraci
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Cristian Vasar
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Maria Graça Ruano
CISUC, University of Coimbra and University of Algarve, Portugal

César A. Teixeira
CISUC, University of Coimbra, Portugal

Javid J. Rahmati
University of Algarve, Portugal

António E. Ruano
Centre for Intelligent Systems, IDMEC, IST and the University of Algarve, Portugal

S.H. Karamchandani
Indian Institute of Technology – Bombay, Mumbai, India

V.K. Madan
Kalasalingam University, Krishnankoil, Virudhunagar, India

P.M. Kelkar
Sneha Health Care Centre, Mumbai, India

S.N. Merchant
Indian Institute of Technology – Bombay, Mumbai, India

U.B. Desai
Indian Institute of Technology – Hyderabad, India

Daniel Dragu
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Valentin Gomoi
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Vasile Stoicu-Tivadar
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Doru Anastasiu Popescu
Faculty of Mathematics and Computer Science, University of Pitesti, Romania and National College "Radu Greceanu" Slatina, Romania

Dragos Nicolae
National College "Radu Greceanu" Slatina, Romania

Ioan Virag
Department of Computer Science, "Vasile Goldis" Western University of Arad, Romania

Antoanela Naaji
Department of Computer Science, "Vasile Goldis" Western University of Arad, Romania

Marius Popescu
Department of Computer Science, "Vasile Goldis" Western University of Arad, Romania

Alina Mădălina Lonea
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Daniela Elena Popescu
Computer Engineering Department, University of Oradea, Faculty of Electrical Engineering and Information Technology, Oradea, Romania

Octavian Prostean
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Huaglory Tianfield
School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, United Kingdom

Cosmin Koch-Ciobotaru
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Ildiko Tatai
"Politehnica" University, Timisoara, Romania

Marian Greconici
"Politehnica" University, Timisoara, Romania

Ovidiu Gana
"Politehnica" University, Timisoara, Romania

Marius Babescu
"Politehnica" University, Timisoara, Romania

Gabriel Gîrban
"Politehnica" University, Timisoara, Romania

Mircea Popa
"Politehnica" University, Timisoara, Romania

Gheorghe Sima
Aurel Vlaicu University of Arad, Arad, Romania

Iñigo Monedero
School of Computer Science and Engineering, Electronic Technology Department, Seville, Spain

Félix Biscarri
School of Computer Science and Engineering, Electronic Technology Department, Seville, Spain

Carlos León
School of Computer Science and Engineering, Electronic Technology Department, Seville, Spain

Juan Ignacio Guerrero
School of Computer Science and Engineering, Electronic Technology Department, Seville, Spain

Viorel Nicolau
Department of Electronics and Telecommunications, "Dunarea de Jos" University of Galati, Romania

Mihaela Andrei
Department of Electronics and Telecommunications, "Dunarea de Jos" University of Galati, Romania

Guilherme Madureira
Institute of Meteorology, Geophysical Center of S. Teotónio, Portugal

Cristiano L. Cabrita
University of Algarve, Portugal

Pedro M. Ferreira
Algarve STP – Algarve Science & Technology Park, Portugal

László T. Kóczy
Faculty of Engineering Sciences, Széchenyi István University, Gyõr, Hungary

Petru Radu
School of Engineering and Digital Arts, University of Kent, Canterbury, U.K.

Konstantinos Sirlantzis
School of Engineering and Digital Arts, University of Kent, Canterbury, U.K.

Gareth Howells
School of Engineering and Digital Arts, University of Kent, Canterbury, U.K.

Sanaul Hoque
School of Engineering and Digital Arts, University of Kent, Canterbury, U.K.

Farzin Deravi
School of Engineering and Digital Arts, University of Kent, Canterbury, U.K.

Cristina Madalina Noaica
Artificial Intelligence & Computational Logic Laboratory, Mathematics & Computer Science Dept., Spiru Haret University, Bucharest, Romania

Robert Badea
Artificial Intelligence & Computational Logic Laboratory, Mathematics & Computer Science Dept., Spiru Haret University, Bucharest, Romania

Iulia Maria Motoc
Artificial Intelligence & Computational Logic Laboratory, Mathematics & Computer Science Dept., Spiru Haret University, Bucharest, Romania

Claudiu Gheorghe Ghica
Artificial Intelligence & Computational Logic Lab., Mathematics & Computer Science Dept., Spiru Haret University, Bucharest, Romania, Programmer at Clintelica AB

Alin Cristian Rosoiu
Game Tester at *UbiSoft* Romania

Nicolaie Popescu-Bodorin
Artificial Intelligence & Computational Logic Laboratory, Mathematics & Computer Science Dept., Spiru Haret University, Bucharest, Romania

Crina Raţiu
Daramec SRL, Arad, România

Dominic Bucerzan
Department of Mathematics-Informatics, Faculty of Exact Sciences, “Aurel Vlaicu” University of Arad, România

Mihaela Crăciun
Department of Mathematics-Informatics, Faculty of Exact Sciences, “Aurel Vlaicu” University of Arad, România

Diana Betina Mirsu
Faculty of Management in Production and Transportation “Politehnica” University of Timisoara, Romania

Irina-Steliana Stan
Department of Economic Informatics, Faculty of Cybernetics, Statisics and Economic Informatics, Academy of Economic Studies, Bucharest, Romania

Ion-Sorin Stroe
Department of Economic Informatics, Faculty of Cybernetics, Statisics and Economic Informatics, Academy of Economic Studies, Bucharest, Romania

Serban Popa
Faculty of Management in Production and Transportation, “Politehnica” University of Timisoara, Romania

Cristian Olariu
“Politehnica” University of Timisoara, Romania

Alexandru Canda
“Politehnica” University of Timisoara, Romania

Anca Draghici
Faculty of Management in Production and Transportation, “Politehnica” University of Timisoara, Romania

Tomislav Rozman
BICERO, Business Informatics Center Rozman Ltd., Maribor, Slovenia

Ahmad Taher Azar
Misr University for Science & Technology (MUST), 6th of October City, Egypt

Shaimaa A. El-Said
Faculty of Engineering - Zagazig University, Zagazig, Sharkia, Egypt

Teodora Olariu
Vasile Goldis Western University of Arad, Romania

Behnam Yavari
School of Electrical and Computer Engineering Shiraz University, Shiraz, Iran

Seyed Hamidreza Abbasi
School of Electrical and Computer Engineering Shiraz University, Shiraz, Iran

Faridoon Shabaninia
School of Electrical and Computer Engineering Shiraz University, Shiraz, Iran

F. Khan
Department of Software Engineering University of Engineering and Technology Taxila, Pakistan

Amna Altaf
Department of Software Engineering University of Engineering and Technology Taxila, Pakistan

Amr F. Farag
Department of Systems and Biomedical Engineering, Cairo University, Giza, Egypt and Department of Biomedical Engineering, Shorouk Higher institute of Engineering, EL-Shorouk, Egypt

Shereen M. El-Metwally
Department of Systems and Biomedical Engineering, Cairo University, Giza, Egypt

Ahmed Abdel Aal Morsy
Department of Systems and Biomedical Engineering, Cairo University, Giza, Egypt

Rim Boughdiri
REGIM: REsearch Group on Intelligent Machines, University of Sfax, National Engineering School of Sfax (ENIS), Tunisia and LSIS, CNRS UMR 7296. Dom. Universitaire St Jérôme, Marseille, France

Hala Bezine
REGIM: REsearch Group on Intelligent Machines, University of Sfax, National Engineering School of Sfax (ENIS), Tunisia

Nacer K. M'Sirdi
LSIS, CNRS UMR 7296. Dom. Universitaire St Jérôme, Marseille, France

Aziz Naamane
LSIS, CNRS UMR 7296. Dom. Universitaire St Jérôme, Marseille, France

Adel M. Alimi
REGIM: REsearch Group on Intelligent Machines, University of Sfax, National Engineering School of Sfax (ENIS), Tunisia

Raghesh Krishnan K.
Department of Information Technology, Amrita Vishwa Vidyapeetham, Amrita Nagar, Coimbatore Tamilnadu, India

R. Sudhakar
Department of Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi Tamilnadu, India

Davood Mohammadi Souran
School of Electrical and Computer Engineering Shiraz University, Shiraz, Iran

Nasim Paykari
School of Electrical and Computer Engineering Shiraz University, Shiraz, Iran

Gabriela Prostean
Faculty of Management in Production and Transportation, "Politehnica" University of Timisoara, Romania

Adrian Adam
Faculty of Management in Production and Transportation, "Politehnica" University of Timisoara, Romania

Adela D. Berdie
Department of Electrical Engineering and Industrial Informatics, Faculty of Engineering Hunedoara, "Politehnica" University of Timisoara, Hunedoara, Romania

Mihaela Osaci
Department of Electrical Engineering and Industrial Informatics, Faculty of Engineering Hunedoara, "Politehnica" University of Timisoara, Hunedoara, Romania

Nicolae Budişan
Department of Automation and Applied Informatics, "Politehnica" University, Timisoara, Romania

Ana Daniela Hammes
Cellent AG Stuttgart, Germany

Manuela Panoiu
Department of Electrical Engineering and Industrial Informatics, Faculty of Engineering Hunedoara, “Politehnica” University of Timisoara, Hunedoara, Romania

Caius Panoiu
Department of Electrical Engineering and Industrial Informatics, Faculty of Engineering Hunedoara, “Politehnica” University of Timisoara, Hunedoara, Romania

Loredana Ghiormez
Faculty of Automation and Computers, “Politehnica University”, Timişoara, Romania

Matei Tămăşilă
“Politehnica” University, Timisoara, Romania

Ilie Mihai Tăucean
“Politehnica” University, Timisoara, Romania

Marius Bîzgă
Automation Department, Rovinari Power Plant, Romania

Soheil Davari
Department of Industrial Engineering, Amirkabir University of Technology, Tehran, Iran

Mohammad Hossein Fazel Zarandi
Department of Industrial Engineering, Amirkabir University of Technology, Tehran, Iran

Outline of a Restriction-Centered Theory of Reasoning and Computation in an Environment of Uncertainty, Imprecision and Partiality of Truth[*]

(Video Tape Lecture)

Lotfi A. Zadeh

Department of EECS,
University of California,
Berkeley, CA 94720-1776
zadeh@eecs.berkeley.edu

Abstract. The theory which is outlined in this lecture, call it RRC for short, is a departure from traditional approaches to reasoning and computation. A principal advance is an enhanced capability for reasoning and computation in an environment of uncertainty, imprecision and partiality of truth. The point of departure in RRC is a basic premise—in the real world such environment is the norm rather than exception.

A concept which has a position of centrality in RRC is that of a restriction. Informally, a restriction is an answer to the question: What is the value of a variable X? More concretely, a restriction, R(X), on a variable, X, is a limitation on the values which X can take—a limitation which is induced by what is known or perceived about X. A restriction is singular if the answer to the question is a singleton; otherwise it is nonsingular. Generally, nonsingularity implies uncertainty. A restriction is precisiated if the limitation is mathematically well defined; otherwise it is unprecisiated. Generally, restrictions which are described in a natural language are unprecisiated.

There are many kinds of restrictions ranging from very simple to very complex. Examples. $3 \leq X \leq 6$; X is normally distributed with mean m and variance σ^2; X is small; it is very likely that X is small; it is very unlikely that there will be a significant increase in the price of oil in the near future.

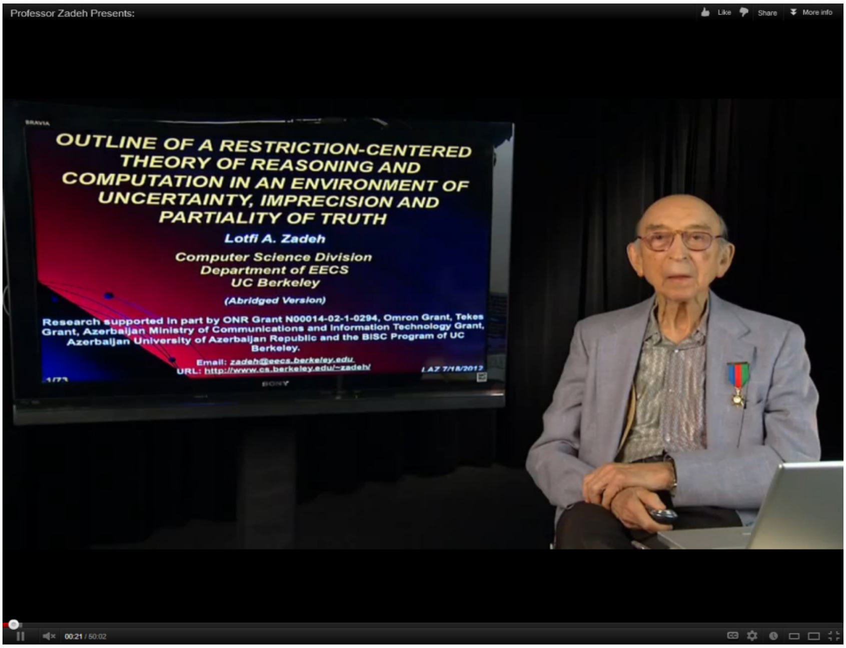
The canonical form of a restriction is an expression of the form X isr R, where X is the restricted variable, R is the restricting relation and r is an indexical variable which defines the way in which R restricts X.

In RRC there are two principal issues—representation and computation. Representation involves representing a semantic entity, e.g., a proposition, as a restriction. For

[*] Research supported in part by ONR N00014-02-1-0294, Omron Grant, Tekes Grant, Azerbaijan Ministry of Communications and Information Technology Grant, Azerbaijan University Grant and the BISC Program of UC Berkeley.

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 1–3.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

computation with restrictions what is employed is the extension principle. The extension principle is a collection of computational rules which address the following problem. Assume that Y=f(X). Given a restriction on X and/or a restriction on f, what is the restriction on Y, R(Y), which is induced by R(X) and R(f)? Basically, the extension principle involves propagation of restrictions. Representation and computation with restrictions is illustrated with examples.



OUTLINE OF A RESTRICTION-CENTERED THEORY OF REASONING AND COMPUTATION IN AN ENVIRONMENT OF UNCERTAINTY, IMPRECISION AND PARTIALITY OF TRUTH

Lotfi A. Zadeh

Computer Science Division
Department of EECS
UC Berkeley

(Abridged Version)

Research supported in part by ONR Grant N00014-02-1-0294, Omron Grant, Tekes Grant, Azerbaijan Ministry of Communications and Information Technology Grant, Azerbaijan University of Azerbaijan Republic and the BISC Program of UC Berkeley.

Email: zadeh@eecs.berkeley.edu
URL: http://www.cs.berkeley.edu/~zadeh/

1/73

LAZ 7/18/2012

Biographical Note

LOTFI A. ZADEH is Professor Emeritus, Computer Science Division, Department of EECS, University of California, Berkeley. In addition, he is serving as the Director of BISC (Berkeley Initiative in Soft Computing). Since the publication of his first paper on fuzzy sets in 1965, his research has been focused on fuzzy logic and its applications.

Lotfi Zadeh has received many awards, among them the IEEE Medal of Honor, IEEE Education Medal, IEEE Richard W. Hamming Medal, the ACM Allen Newell Award, the Honda Prize, the Okawa Prize, the Kaufmann Prize and Gold Medal, Grigore Moisil Prize, the Kampe de Feriet Award, Bolzano Medal, the Nicolaus Copernicus Medal, Norbert Wiener Award, the Benjamin Franklin Medal and the Friendship Order from the President of the Republic of Azerbaijan. He was inducted into the Silicon Valley Engineering Hall of Fame, the AI Hall of Fame and the Nixdorf Museum Wall of Fame. He is a recipient of twenty-five honorary doctorates, and is a member of the National Academy of Engineering. In addition, he is a foreign member of the Finnish Academy of Sciences, the Polish Academy of Sciences, the Korean Academy of Science & Technology, the Bulgarian Academy of Sciences, the Azerbaijan Academy of Sciences, Hungarian Academy of Engineering and Romanian Academy of Technical Sciences. His work is associated with 100,584 Google Scholar citations.

http://www.cs.berkeley.edu/~zadeh/

On Structure of Uncertainties

Michio Sugeno

European Centre for Soft Computing Mieres-Asturias, Spain
michio.sugeno@gmail.com

Abstract. As a conventional concept of uncertainty, we are familiar with the ‘probability’ of a phenomenon. Also we often discuss the ‘uncertainty’ of knowledge. Recently, Fuzzy Theory has brought a hidden uncertainty, ‘fuzziness’, to light. Reflections on these ideas lead to a fundamental question: What kinds of uncertainty are we aware of? Motivated by this question, this study aims to explore categories and modalities of uncertainty. For instance, we have found that:

(i) ‘form’ is a category of uncertainty;
(ii) ‘inconsistency’ is a modality of uncertainty;
(iii) the inconsistency of form is one of the major uncertainties.

Through the classification of adjectives implying various uncertainties, we elucidate seven uncertainties (or nine if subcategories are counted) and identify three essential ones among them, such as the fuzziness of wording. Finally the structure of uncertainty will be shown. The obtained structure is verified by psychological experiments, while the validity of three essential uncertainties is examined by linguistic analysis.

Michio Sugeno

Short biography

After graduating from the Department of Physics, The University of Tokyo, Michio Sugeno worked at Mitsubishi Atomic Power Industry. Then, he served the Tokyo Institute of Technology as Research Associate, Associate Professor and Professor

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 5–6.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

from 1965 to 2000. After retiring from the Tokyo Institute of Technology, he worked as Laboratory Head at the Brain Science Institute, RIKEN from 2000 to 2005, and then, as Distinguished Visiting Professor at Doshisha University from 2005 to 2010. He is currently Emeritus Professor at the Tokyo Institute of Technology, Japan, and Emeritus Researcher at the European Centre for Soft Computing, Spain.

He was President of the Japan Society for Fuzzy Theory and Systems from 1991 to 1993, and also President of the International Fuzzy Systems Association from 1997 to 1999. He is the first recipient of the IEEE Pioneer Award in Fuzzy Systems with Zadeh in 2000. He also received the 2010 IEEE Frank Rosenblatt Award.

Advances in Evolutionary Multi-objective Optimization

Kay Chen Tan

Department of Electrical and Computer Engineering
National University of Singapore
4 Engineering Drive 3, Singapore 117576
eletankc@nus.edu.sg

Abstract. Multi-objective evolutionary algorithms are a class of stochastic optimization Techniques that simulate biological evolution to solve problems with multiple (and often conflicting) objectives.

Advances made in the field of evolutionary multi-objective optimization (EMO) are the results of more than two decades of research, studying various topics that are unique to MO problems, such as fitness assignment, diversity preservation, balance between exploration and exploitation, elitism and archiving. However many of these studies assume that the problem is deterministic, while the EMO performance generally deteriorates in the presence of uncertainties. In certain situations, the solutions found may not even be implementable in practice. The lecture will first provide an overview of evolutionary computation and its application to multi-objective optimization. It will then discuss challenges faced in EMO research and present various EMO features and algorithms for good optimization performance. Specifically, the impact of noise uncertainties will be described and enhancements to basic EMO algorithmic design for robust optimization will be presented. The lecture will also discuss the applications of EMO techniques for solving engineering problems, such as control system design and scheduling, which often involve different competing specifications in a large and constrained search space.

Kay Chen TAN is currently an Associate Professor in the Department of Electrical and Computer Engineering, National University of Singapore. He is actively pursuing

Research in computational and artificial intelligence, with applications to multi---objective optimization, scheduling, automation, data mining, and games.

Dr Tan has Published over 100 journal papers, over 100 papers in conference proceedings, co--authored 5 books including Multiobjective Evolutionary Algorithms and Applications (Springer-Verlag, 2005), Modern Industrial Automation Software Design (John Wiley, 2006; Chinese Edition, 2008), Evolutionary Robotics: From Algorithms to Implementations (World Scientific, 2006; Review), Neural Networks: Computational Models and Applications (Springer-Verlag, 2007), and Evolutionary Multi-objective Optimization in Uncertain Environments: Issues and Algorithms (Springer-Verlag, 2009), co-edited 4 books including Recent Advances in

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 7–8.
springerlink.com Springer-Verlag Berlin Heidelberg 2013

Simulated Evolution and Learning (World Scientific, 2004), Evolutionary Scheduling (Springer-Verlag, 2007), Multiobjective Memetic Algorithms (Springer-Verlag, 2009), and Design and Control Of Intelligent Robotic Systems (Springer-Verlag, 2009).

Dr Tan is currently a Distinguished Lecturer of IEEE Computational Intelligence Society. He has been invited to be a keynote/invited speaker for over 25 international conferences. He served in the international program committee for over 100 conferences and involved in the organizing committee for over 30 international conferences, including the General Co-Chair for IEEE Congress on Evolutionary Computation 2007 in Singapore and the General Co-Chair for IEEE Symposium on Computational Intelligence in Scheduling in Tennessee, USA.

Dr Tan is currently the Editor-in-Chief of IEEE Computational Intelligence Magazine (5-Year IF: 4.094; IF: 2.833 –Rank 13 out of all 127 IEEE journals). He also serves as an Associate Editor / Editorial Board member of over 15 international journals, such as IEEE Transactions on Evolutionary Computation, IEEE Transactions on Computational Intelligence and AI in Games, Evolutionary Computation (MIT Press), European Journal of Operational Research, Journal of Scheduling, and International Journal of Systems Science.

Dr Tan is the awardee of the 2012 IEEE Computational Intelligence Society (CIS) Outstanding Early Career Award for his contributions to evolutionary computation in multi-objective optimization. He also received the Recognition Award (2008) from the International Network for Engineering Education & Research (iNEER) for his outstanding contributions to engineering education and research. He was also a winner of the NUS Outstanding Educator Awards (2004), the Engineering Educator Awards (2002, 2003, 2005), the Annual Teaching Excellence Awards (2002, 2003, 2004, 2005, 2006), and the Honour Roll Awards (2007). Dr Tan is currently a Fellow of the NUS Teaching Academic.

On the Applications of Fuzzy Implication Functions

Michał Baczyński

University of Silesia
Institute of Mathematics
Katowice, Poland
michal.baczynski@us.edu.pl

Abstract. Fuzzy implication functions are one of the main operations in fuzzy logic. They generalize the classical implication, which takes values in the set {0,1}, to fuzzy logic, where the truth values belong to the unit interval [0,1]. The study of this class of operations has been extensively developed in the literature in the last 30 years from both theoretical and applicational points of view.

In our talk we will concentrate on many different applications of this class of functions. Firstly we will discuss some aspects of mathematical fuzzy logic. Next we will show they role in finding solutions of different fuzzy relational equations. In the next part we present their relevance in approximate reasoning and fuzzy control. In this section we will discuss various inference schemas and we will also show some results connected with fuzzy implications, which are related with reducing the complexity of inference algorithms. In the final part of our talk we will show the importance of fuzzy implication functions in fuzzy mathematical morphology and image processing.

Michał Baczyński was born in Katowice, Poland. He received the M.Sc. and Ph.D. degrees in mathematics from the Department of Mathematics, Physics, and Chemistry, University of Silesia, Katowice, in 1995 and 2000, respectively. He received the "habilitation" degree in computer science from the Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland, in 2010.

He is currently with the Institute of Mathematics, University of Silesia. He has co-authored a research monograph on Fuzzy Implications and is the author or co-author

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 9–10.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

of more than 40 published papers in refereed international journals and conferences. He has been invited to be an invited speaker for 2 international conferences, in particular at last EUSFLAT - LFA 2011 Conference in Aix-Les-Bains, France. He is also a regular reviewer for many respected international journals and a member of various committees in international conferences. His current research interests include fuzzy aggregation operations, chiefly fuzzy implications, approximate reasoning, fuzzy systems, and functional equations. Dr. Baczyński is a member of the European Society for Fuzzy Logic and Technology (EUSFLAT) and the Polish Mathematical Society (PTM).

Information Theoretic Security by the Laws of Classical Physics

(Plenary Paper)

R. Mingesz[1], L.B. Kish[2], Z. Gingl[1], C.G. Granqvist[3], H. Wen[2,4],
F. Peper[5], T. Eubanks[6], and G. Schmera[7]

[1] Department of Technical Informatics, University of Szeged,
Árpád tér 2, Szeged, H-6701, Hungary
{mingesz,gingl}@inf.u-szeged.hu
[2] Texas A&M University, Department of Electrical and Computer Engineering,
College Station, TX 77843-3128, USA
Laszlo.Kish@ece.tamu.edu
[3] Department of Engineering Sciences, The Ångström Laboratory, Uppsala University,
P.O. Box 534, SE-75121 Uppsala, Sweden
Claes-Goran.Granqvist@Angstrom.uu.se
[4] Hunan University, College of Electrical and Information Engineering,
Changsha 410082, China
he_wen82@126.com
[5] National Institute of Information and Communication Technology,
Kobe, Hyogo 651-2492, Japan
peper@nict.go.jp
[6] Sandia National Laboratories, P.O. Box 5800,
Albuquerque, NM 87185-1033, USA
tweuban@sandia.gov
[7] Space and Naval Warfare Systems Center,
San Diego, CA 92152, USA
gabe.schmera@navy.mil

Abstract. It has been shown recently that the use of two pairs of resistors with enhanced Johnson-noise and a Kirchhoff-loop—*i.e.*, a Kirchhoff-Law-Johnson-Noise (KLJN) protocol—for secure key distribution leads to information theoretic security levels superior to those of a quantum key distribution, including a natural immunity against a man-in-the-middle attack. This issue is becoming particularly timely because of the recent full cracks of practical quantum communicators, as shown in numerous peer-reviewed publications. This presentation first briefly surveys the KLJN system and then discusses related, essential questions such as: what are perfect and imperfect security characteristics of key distribution, and how can these two types of securities be unconditional (or information theoretical)? Finally the presentation contains a live demonstration.

Keywords: information theoretic security, unconditional security, secure key exchange, secure key distribution, quantum encryption.

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 11–25.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

1 Introduction: Quantum Security Hacked

Practical quantum communicators—including several commercial ones—have been fully cracked, as shown in numerous recent papers [1-15], and Vadim Makarov, who is one of the leading quantum crypto crackers, says in *Nature News* that "Our hack gave 100% knowledge of the key, with zero disturbance to the system" [1]. This claim hits at the foundations of quantum encryption schemes because the basis of the security of quantum key distribution (QKD) protocols is the assumption that any eavesdropper (Eve) will disturb the system enough to be detected by the communicator parties (Alice and Bob). Furthermore this proves that we were right in 2007 when claiming in our *SPIE Newsroom* article [16] that quantum security is mainly theoretical because, at that time, no effort had been made to experimentally crack the communicators; instead research grants supported the development of new QKD schemes but not the "politically incorrect" challenge to crack them.

However, the last few years have seen a radically changed picture [1-15] on the security of practical quantum communicators, and even a full-field implementation of a perfect eavesdropper on a quantum cryptography system has been carried out [2], which is a most difficult task and is an attack on an already established "secure" QKD connection. These cracking schemes are referred to as "hacking" because they utilize physical non-idealities in the building elements of QKD devices. The number of these non-idealities is large, and so is the number of hacking types. The key lessons that has been learned here are that

(*i*) Quantum security at the moment is theoretical, and the applied theory is incorrect for practical devices; a new defense mechanism must be developed for each type of hacking attack, and the potential for yet unexplored non-idealities/ attacks is huge, and

(*ii*) Security analysis, taking into the account of the real physics of the devices, is essential when security matters.

An important aspects all these quantum attacks is the extraordinary (100%) success ratio (*i.e.*, information leak) of extracting the "secure" key bits by Eve, while Alice and Bob do not have a clue that efficient eavesdropping is going on. At this point we note that this information leak was only 0.19% for the *classical* secure communication scheme we are discussing in this paper in the case of a similar situation wherein the strongest vulnerability based on physical non-idealities was used; this is discussed further below.

Inspired by these interesting developments we discuss related issues in the key exchange system of the classical physical Kirchhoff-Law-Johnson-Noise (KLJN) protocol [16]. It should be noted here that there is a general misunderstanding of the KLJN scheme among people lacking the relevant expertise in statistical physics and noise-in-circuitry, as evidenced for example in the Wikipedia entry "Kish cypher" and its "talk page" where, most of the time, both the supporters and the opponents are wrong and the debate falls very short of an objective scientific discussion (amusingly, even the name "cypher" is incorrect). Therefore, after briefly surveying the KLJN system and its properties, we clarify the meaning of *perfect security* and *imperfect* *security* levels and also define the conditions of these measures: *information theoretic security* (or *unconditional security*) and its limited version *computationally unconditional security*. Furthermore we mention existing integer-number-based key exchange protocols that have (computationally) *conditional security*. It will be seen that theoretical/ideal QKD and KLJN protocols have perfect information theoretic (unconditional) security. However these schemes, when realized with practical/realistic (physical/non-ideal) building elements have imperfect security that is still information theoretic (unconditional), even though current QKD cracks [1-15] indicate that KLJN performs better.

2 The KLJN Secure Key Exchange Protocol

It is often believed that quantum physics represents modern science and that classical physics is old and outdated. Of course this is not true because the two fields rather pertain to different physical size regimes—the "small" versus the "large" where the appropriate rules of physics are different—not different periods of science history. The above claim regarding "modern" and "old" cannot be maintained even for the history of physics, though, when the point at issue concerns spontaneous random fluctuation phenomena, that are simply referred to as "noise", and it is true for even the most general and omnipresent type of classical physical noise, *viz.*, thermal noise (voltage or current fluctuations in thermal equilibrium) which is a younger field of physics than quantum mechanics. Indeed two Swedish scientists, John Johnson and Harry Nyquist both working at Bell Labs, discovered/explained the thermal noise voltage of resistors [17,18] several years after the completion of the foundations of quantum physics [19].

Similarly, quantum heat engines [20] with optional internal coherence effects [21] were proposed several years earlier than the application [22] of the thermal noise of resistors for a heat engine scheme with similar coherence effects.

Finally, the application of thermal noise for unconventional informatics, namely for noise-based logic and computing [23-30] and the KJLN secure key exchange [31-46], emerged decades later than the corresponding quantum informatics schemes such as quantum computing [47] and quantum encryption [48-50].

It is interesting to not that some "exotic" phenomena previously thought to belong to the class of "quantum-weirdness" occur and can be utilized also in the noise schemes, for example: teleportation/telecloning in KLJN networks [45] and entanglement in noise-based logic [23-30].

2.1 The Kirchhoff-Law-Johnson-Noise Key Distribution[1]

The KLJN secure key exchange scheme was introduced in 2005 [31-33] and was built and demonstrated in 2007 [34]; it is founded on the robustness of classical information as well as stochasticity and the laws of classical physics. It was named by

[1] This section is a modified version of related expositions elsewhere [36,46].

its creators the "Kirchhoff-loop-Johnson(-like)-Noise" scheme, while on the internet—in blogs and similar sites, including Wikipedia—it has widely been nicknamed "Kish cypher" or "Kish cipher" (where both designations are wrong). The concept has often been misinterpreted and misjudged.

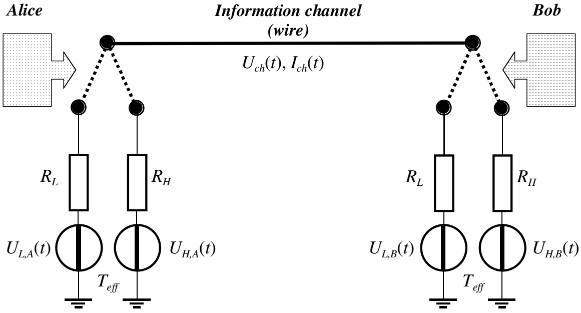


Fig. 1. Core of the KJLN secure key exchange system [31]. In the text below, the mathematical treatment is based on the power density spectra of the voltages and currents shown in the figure.

The KLJN scheme is a statistical-physical competitor to quantum communicators whose security is based on Kirchhoff's Loop Law and the Fluctuation-Dissipation Theorem. More generally, it is founded on the Second Law of Thermodynamics, which indicates that the security of the ideal scheme is as strong as the impossibility to build a perpetual motion machine of the second kind.

We first briefly survey the foundations of the KLJN system [31,33,36]. Figure 1 shows a model of the idealized KLJN scheme designed for secure key exchange [31]. The resistors R_L and R_H represent the low, L (0), and high, H (1), bits, respectively. At each clock period, Alice and Bob randomly choose one of the resistors and connect it to the wire line. The situation LH or HL represents secure bit exchange [31], because Eve cannot distinguish between them through measurements, while LL and HH are insecure. The Gaussian voltage noise generators (white noise with publicly agreed bandwidth) represent a corresponding thermal noise at a publicly agreed effective temperature T_{eff} (typically $T_{eff} > 10^9$ K [34]). According to the Fluctuation-Dissipation Theorem, the power density spectra $S_{u,L}(f)$ and $S_{u,H}(f)$ of the voltages $U_{L,A}(t)$ and $U_{L,B}(t)$ supplied by the voltage generators in R_L and R_H are given by

$$S_{u,L}(f) = 4kT_{eff}R_L \quad \text{and} \quad S_{u,H}(f) = 4kT_{eff}R_H , \tag{1}$$

respectively.

In the case of secure bit exchange (*i.e.*, the LH or HL situation), the power density spectrum of channel voltage $U_{ch}(t)$ and channel current $I_{ch}(t)$ are given as

$$S_{u,ch}(f) = 4kT_{eff}\frac{R_L R_H}{R_L + R_H} , \tag{2}$$

and

$$S_{i,ch}(t) = \frac{4kT_{eff}}{R_L + R_H}; \tag{3}$$

further details are given elsewhere [31,36]. It should be observed that during the *LH* or *HL* case, linear superposition turns Equation (2) into the sum of the spectra of two situations, *i.e.*, when only the generator in R_L is running one gets

$$S_{L,u,ch}(f) = 4kT_{eff}R_L\left(\frac{R_H}{R_L + R_H}\right)^2 , \tag{4}$$

and when the generator in R_H is running one has

$$S_{H,u,ch}(f) = 4kT_{eff}R_H\left(\frac{R_L}{R_L + R_H}\right)^2 . \tag{5}$$

The ultimate security of the system against passive attacks is provided by the fact that the power $P_{H\to L}$, by which the Johnson noise generator of resistor R_H is heating resistor R_L, is equal to the power $P_{L\to H}$ by which the Johnson noise generator of resistor R_L is heating resistor R_H [31,36]. A proof of this can also be derived from Equation (3) for a frequency bandwidth of Δf by

$$P_{L\to H} = \frac{S_{L,u,ch}(f)\Delta f}{R_H} = 4kT_{eff}\frac{R_L R_H}{(R_L + R_H)^2} , \tag{6a}$$

and

$$P_{H\to L} = \frac{S_{H,u,ch}(f)\Delta f}{R_L} = 4kT_{eff}\frac{R_L R_H}{(R_L + R_H)^2} . \tag{6b}$$

The equality $P_{H\to L}=P_{L\to H}$ (*cf.* Equations 6) is in accordance with the Second Law of Thermodynamics; violating this equality would mean not only going against basic laws of physics and the inability to build a perpetual motion machine (of the second kind) but also allow Eve to use the voltage-current cross-correlation $\left\langle U_{ch}(t)I_{ch}(t)\right\rangle$ to extract the bit [31]. However $\left\langle U_{ch}(t)I_{ch}(t)\right\rangle$ = 0, and hence Eve has an insufficient number of independent equations to determine the bit location during the *LH* or *HL* situation. The above security proof against passive (listening) attacks holds only for Gaussian noise, which has the well-known property that its power density spectrum or autocorrelation function provides the maximum information about the noise and no higher order distribution functions or other tools are able to contribute additional information.

It should be observed [31,33,34,36] that deviations from the shown circuitry—including parasitic elements, inaccuracies, non-Gaussianity of the noise, *etc.*—will cause a potential information leak toward Eve. One should note that the circuit symbol "line" in the circuitry represents an ideal wire with uniform instantaneous voltage and current along it. Thus if the wire is so long and the frequencies are so high that waves appear in it, this situation naturally means that the actual circuitry deviates from the ideal one because neither the voltage nor the current is uniform along the line [31].

To provide unconditional security against invasive attacks, including the man-in-the-middle attack, the fully armed KLJN system shown in Figure 2 monitors the instantaneous current and voltage values at both ends (*i.e.*, for Alice as well as Bob) [33,34,36], and these values are compared either via broadcasting them or via an authenticated public channel. An alarm goes off whenever the circuitry is changed or tampered with or energy is injected into the channel. It is important to note that these current and voltage data contain all of the information Eve can possess. This implies that Alice and Bob have full knowledge about the information Eve may have; this is a particularly important property of the KLJN system, which can be utilized in secure key exchange.

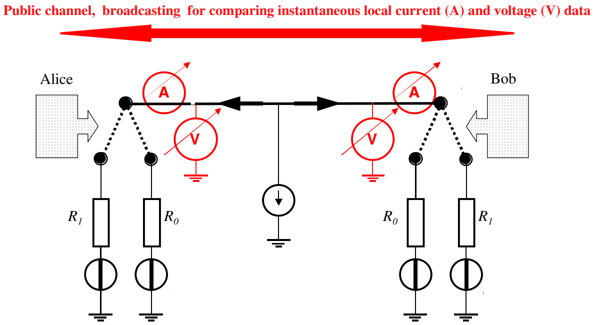

Public channel, broadcasting for comparing instantaneous local current (A) and voltage (V) data
Alice
Bob
A
A
V
V
R_1
R_0
R_0
R_1

Fig. 2. Sketch of the KLJN wire communication arrangement [33,36]. To detect the invasive eavesdropper (represented, for example, by the current generator at the middle), the instantaneous current and voltage data measured at the two ends are broadcasted and compared. The eavesdropping is detected immediately, within a small fraction of the time needed to transfer a single bit. Thus statistics of bit errors is not needed, so the exchange of even a single key bit is secure.

The situation discussed above implies the following important features of the KLJN system [31,33,34,36]:

(1) In a practical (non-idealized) KLJN system, Eve can utilize device non-idealities to extract some of the information by proper measurements. This is measurement information and does not depend on Eve's computational and algorithmic ability, *i.e.*, the level of security is computationally unconditional. The maximum leak toward Eve can be designed by Alice and Bob by supposing the physically allowed best/ultimate measurement system for Eve. This designed level of security is unconditional in every sense.

(2) Even when the communication is disturbed by invasive attacks or inherent non-idealities in the KLJN arrangement, the system remains secure because no information can be eavesdropped by Eve without the full knowledge of Alice and Bob

about this potential incidence, and without the knowledge of the full information that Eve might have extracted (a full analysis of this aspect is provided elsewhere [36]).

(3) In other words, the KLJN system is always secure, even when it is built with non-ideal elements or designed for a non-zero information leak, in the following sense: The current and voltage data inform Alice and Bob about the exact information leak and hence, for each compromised key bit, they can decide to discard it or even to use it to mislead/manipulate Eve [36].

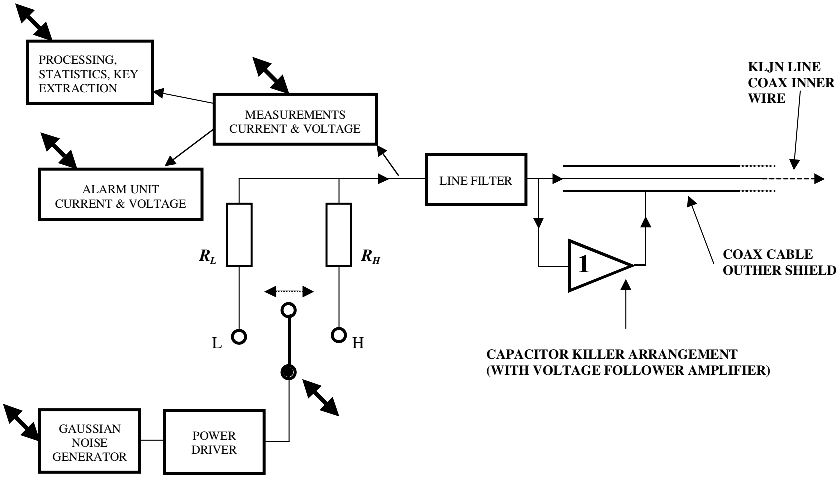

PROCESSING, STATISTICS, KEY EXTRACTION
MEASUREMENTS CURRENT & VOLTAGE
ALARM UNIT CURRENT & VOLTAGE
LINE FILTER
KLJN LINE COAX INNER WIRE
COAX CABLE OUTHER SHIELD
1
R_L
R_H
L
H
CAPACITOR KILLER ARRANGEMENT (WITH VOLTAGE FOLLOWER AMPLIFIER)
GAUSSIAN NOISE GENERATOR
POWER DRIVER

Fig. 3. A practical KLJN device set-up [34]. Double-ended arrows symbolize computer control.

(4) The KLJN arrangement is naturally and fully protected against the man-in-the-middle attack [33] even during the very first run of the operation when no hidden signatures can be applied. This feature is provided by the unique property of the KLJN system that zero bit information can only be extracted during a man-in-the-middle attack because the alarm goes off before the exchange of a single key bit has taken place [33].

(5) The security of the KLJN system is not based on the error statistics of key bits, and even the exchange of single key bits is secure.

Figure 3 outlines a prototype of the KLJN device [34]. The various non-idealities have been addressed by different tools with the aim that the information leak toward Eve due to non-idealities should stay below 1% of the exchanged raw key bits. For the KLJN device it was 0.19% for the most efficient attack [18]. Here we briefly address two aspects of non-idealities:

(*i*) The role of the line filter (and of the band limitation of the noise generator) is to provide the no-wave limit in the cable, *i.e.*, to preserve the core circuitry (*cf.* Figure 1) in the whole frequency band. This implies that the shortest wavelength component in the driving noise should be much longer than twice the cable length in order to guarantee that no active wave modes and related effects (*e.g.*, reflection, invasive attacks at high frequencies, *etc.*) take place in the cable.

(*ii*) Another tool to fight non-idealities is the cable capacitance compensation ("capacitor killer") arrangement (*cf.* Figure 3). With practical cable parameters and their limits, there is a more serious threat of the security: the cable capacitance shortcuts part of the noise current which results in a greater current at the side of the lower resistance end thus yields an information leak. This effect can be avoided by a cable-capacitor-killer [34] using the inner wire of a coax cable as KLJN line while the outer shield of the cable is driven by the same voltage as the inner wire. However, this is done via a follower voltage amplifier with zero output impedance. The outer shield will then provide all the capacitive currents toward the ground, and the inner wire will experience zero parasitic capacitance. Without "capacitor killer" arrangement and practical bare-wire line parameters, the recommended upper limit of cable length is much shorter and depends on the driving resistor values R_L and R_H .

2.2 Security Proofs and Attacks

The ideal system is absolutely secure, but real systems are rarely ideal and thus hacking attacks are possible by using non-idealities. Fortunately the KLJN system is very simple, implying that the number of such attacks is limited. Several hacking attack types based on the non-ideality of circuit elements causing deviations from the ideal circuitry have been published [36-42]. Each of these attacks triggered a relevant security proof that showed the efficiency of the defense mechanism (*cf.* Figure 2). Furthermore, all known attack types were experimentally tested [34], and the theoretical security proofs were experimentally confirmed.

For practical conditions, the most effective attack employed voltage-drop-related effects on non-zero wire resistance [32,37,38]. It should be noted that serious calculation errors were made by Scheuer and Yariv [37] resulting in a thousand times stronger predicted value of the effect than its real magnitude. The errors were pointed out and the calculations were corrected by Kish and Scheuer [38]. In an experimental demonstration [34], the strongest leak was indeed due to wire resistance, and 0.19% of the bits leaked out ($1.9 * 10^{-3}$ relative information leak) to Eve, while the fidelity of the key exchange was 99.98% (which means 0.02% bit error rate). This is a very good raw bit leak, and it can easily be made infinitesimally small by simple two-step privacy amplification, as further discussed in Section 2.3.

A general response to the mentioned and other types of small-non-ideality attacks was also presented [39], and the related information leak was shown to be miniscule due to the very poor statistics that Eve could obtain.

Other attack types of less practical significance were based on differences in noise temperatures by Hao [40], which were proven theoretically [41] and experimentally [34] insignificant. The very high accuracy of digital simulations and digital-analog converters (at least 12-bit resolution) allows setting the effective temperature so accurately (0.01% or less error) that this type of inaccuracy-based information leak is not observable. In the case of 12-bit resolution, the theoretical value of the relative information leak is $6 * 10^{-11}$, *i.e.*, to leak out one effective bit would require a

600 Megabit long key. Therefore this effect was not visible in the experiments even though extraordinarily long (74497) key bits were generated/exchanged in each run [34].

The practical inaccuracy of commercial low-cost resistors (1%) at the two ends [34,41] is a much more serious issue; the theoretical value is $<10^{-4}$ relative information leak (about 7 bits leak from the 74497 bit long key) for a resistance inaccuracy of 1% [34]. However, its impact was still not measurable because of the statistical inaccuracies, $\sqrt{74497} \approx 270$ bits, at this key length. These inaccuracies were about forty times greater than the theoretical information leak of 7 [34].

Wire capacitance would be the most serious source of information leak without the cable-capacitance-killer arrangement, but cable inductance effects are negligible [36].

Another attack [42] focusing on delay effects obtained 70% information leak with a wire simulation software by using physically invalid parameters, such as cable diameters being 28,000 greater than the diameter of the known universe at two km cable length (the error in this attack [42] was pointed out in a subsequent paper [36]). Although this attack was flawed, it is remarkable that even this non-existent, high information leak can be removed by a three-step privacy amplification as discussed in Section 2.3.

It is important to note that the level of allowed information leak is the choice of Alice and Bob, and its actual value is determined only by the invested resources and also typically depends on how much speed is given up. For example, the information leak due to the wire resistance scales inversely with the 4th power of wire diameter, which means that employing a ten times thicker cable would reduce the relative information leak of 0.19% to $1.9 * 10^{-7}$.

For Eve the best attack strategy is to observe the public data exchange about the instantaneous current and voltage amplitudes between Alice and Bob. Those data contain the highest amount of eavesdropping information because they are measured in the most ideal way, and Alice and Bob also base their decision about the bit values on those. Enhancing Eve's infrastructure beyond that ability does not improve her situation, and thus the security is information theoretic/ unconditional.

2.3 Privacy Amplification in Non-ideal Systems

Privacy amplification is a classical software-based technique, which was originally developed for QKD to ensure the security of an encryption scheme with partially exposed key bits. Horvath *et al.* [43] realized simple privacy amplification by executing XOR logic operation on the subsequent pairs of the key bits, thereby halving the key length while progressively reducing the information leak. If the reduction of the information leak is not enough, the same procedure can be repeated on the new key. The resulting key length scales with 0.5^N, where N is the number of these privacy amplification steps. It was found that, in contrast to quantum key distribution schemes, the high fidelity of the raw key generated in the KLJN system allows the users to always extract a secure shorter key. The necessary conditions are sufficiently high fidelity (small bit error rate), which the KLJN provides, and an upper limit less than one on the eavesdropper probability to correctly guess the exchanged key bits, which means the key exchange is not fully cracked (less than 100% relative information leak is present). The number of privacy amplification steps needed to achieve an information leak of less than 10^{-8} in the case of the 0.19% raw bit information leak is two, thus resulting in a corresponding slowdown by a factor of four [43]. In the case of the 70% information leak obtained by the flawed simulations in earlier work [42], the necessary number of privacy amplification steps is three thus resulting in a slowdown of a factor of eight [43].

3 Security Measures and Their Conditions

In this section we discuss security measures [52,53] and apply them to compare QKD, KLJN and software security schemes.

A *perfect security* level means that the information channel capacity of the eavesdropping-channel from Alice/Bob toward Eve is zero. *Imperfect security* level means that the information channel capacity of the eavesdropping-channel from Alice/Bob toward Eve is non-zero. We call the encryption "cracked" if Eve can extract all of the information communicated between Alice and Bob. Thus an imperfect security level does not necessarily mean that the encryption is cracked. If the bit-error-rate (BER) is negligible then, by using privacy amplification, the effective level of imperfect security can be enhanced so that it can arbitrarily approach the perfect security level.

To characterize the situations of perfect and imperfect security levels, we must address the conditions where these levels hold. Conditions that both QKD and the KLJN protocols represent are called *information theoretic security*, or *unconditional security*. We note, in passing, that these terms are often completely misunderstood by people who write into Wikipedia and to blog sites about the KLJN system, and these mistakes lead to incorrect conclusions and self-contradicting arguments.

The most rigorous security condition is *information theoretic security*, which means that the information content of the data Eve can extract is limited by information theory even if Eve is using the hypothetical most powerful processing of the extracted data. *Unconditional security* is a similar term indicating security when Eve has unlimited resources. It often means a computationally unconditional security measure, which limits the infrastructure to computers and algorithms, so it has limited validity compared to information theoretic security. Computationally unconditional security simply means that the information content of the data that Eve is able to extract is limited even if she has infinite computing power.

For example, today's generally used software algorithms utilizing prime numbers for key generation and distribution have neither information-theoretic nor computationally unconditional security. All of the information about the key exists in the data observed in the line by Eve, in a decodable form, thus it cannot be information theoretically secure. This information can be fully decoded with a sufficiently fast computer or integer-factoring algorithm, or with a normal computer running for long-enough but finite time. The security is (computationally) conditional:

it is based on the assumption that Eve does not have an efficient algorithm or a fast-enough computer to decode the key within the practically relevant time frame.

It is important to note that even imperfect security can be information theoretical or (computationally) unconditional [53]. Such a situation occurs with a physically secure key distribution only, such as QKD or KLJN, because the information leak will be determined by measurement information and not by computation or algorithmic decoding.

The way in which ideal/theoretical QKD makes the key exchange secure is based on the no-cloning theorem of quantum physics: photon states cannot be cloned without introducing errors. Because information bits are carried by (theoretically) single photons, Eve must clone the photon if she wants to measure one; otherwise the information is destroyed before reaching the receiving party. Thus Eve must clone the photon, which introduces extra errors into the line. When Alice and Bob recognize the increased bit-error-rate, they conclude that eavesdropping has happened and they discard the bit-package exhibiting the increased error rate.

The ideal QKD protects the system against eavesdropping, but this is strictly true only for an infinitely long key because Alice and Bob must prepare error statistics, and exact statistics requires infinite time. Otherwise, due to statistical fluctuations in the BER, Alice and Bob can never be absolutely sure that the key was not eavesdropped. To illustrate this problem, we can go to the simplest type of attacks: the intercept-resend attack for the BB84 QKD protocol (see, for example, [51]). The probability $P(N)$ that the eavesdropping will be discovered while Eve extracts N key bits is not 1 but

$$P_h = 1 - \left(\frac{3}{4}\right)^N . \tag{7}$$

Equation (7) shows that, even though a reasonably long key will be very secure and that security can further be enhanced by privacy amplification (see above), the security is not perfect although it can arbitrarily approach the perfect security level. However, if we want to extract only a single key bit, the security is extremely poor because Eve has 25% chance to succeed.

The way by which the ideal/theoretical KLJN scheme makes the key exchange secure depends on the type of the attack: whether it is passive (listening) or invasive (introducing energy in the channel and/or modifying the channel circuitry). In the case of passive listening, information theoretic security due to zero information in the extracted data is guaranteed by the Second Law of Thermodynamics, and this is true even for single-bit attacks where QKD fails. In the case of invasive attacks, the defense mechanics is similar to that of QKD; Alice and Bob will observe deviations between instantaneous signals and they detect the presence of eavesdropping virtually immediately so that, again, even a single bit attack has no chance. Table 1 shows the summary/conclusion about the security level of various key exchange protocols.

In conclusion, the ideal KLJN protocol protects a system against invasive eavesdropping and provides zero information to passive eavesdroppers.

Table 1. Comparison of relevant security levels for existing key exchange systems. Practical physically secure key distributions can never have perfect security, they can only approach it.

	Perfect	**Imperfect**	**Information theoretic or unconditional**	**Conditional**
QKD theoretical	**Yes** for the whole key **No** for a single bit	**No** for the whole key **Yes** for a single bit	**Yes**	**No**
KLJN theoretical	**Yes** for both the whole key and a single bit	**No**	**Yes**	**No**
QKD practical	**No**	**Yes**	**Yes**	**No**
KLJN practical	**No**	**Yes**	**Yes**	**No**
Software and prime number based	**Yes**	**No**	**No**	**Yes**

Acknowledgement. LBK is grateful to Vincent Poor for a discussion about unconditional (information theoretic) security of practical secure physical systems with imperfect security. This work was partially supported by grant TAMOP-4.2.1/B-09/1/KONV-2010-0005. HW's work was partially supported by the National Natural Science Foundation of China under grant 61002035.

References

[1] Merali, Z.: Hackers blind quantum cryptographers. Nature News (August 29, 2009), doi:10.1038/news.2010.436

[2] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Makarov, V.: Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications 2 (article number 349) (2011), doi:10.1038/ncomms1348.

[3] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics 4, 686–689 (2010), doi:10.1038/NPHOTON.2010.214

[4] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Scarani, V., Makarov, V., Kurtsiefer, C.: Experimentally faking the violation of Bell's inequalities. Phys. Rev. Lett. 107, 170404 (2011), doi:10.1103/PhysRevLett.107.170404

[5] Makarov, V., Skaar, J.: Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. Quantum Information and Computation 8, 622–635 (2008)

[6] Wiechers, C., Lydersen, L., Wittmann, C., Elser, D., Skaar, J., Marquardt, C., Makarov, V., Leuchs, G.: After-gate attack on a quantum cryptosystem. New J. Phys. 13, 013043 (2011), doi:10.1088/1367-2630/13/1/013043

[7] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Thermal blinding of gated detectors in quantum cryptography. Optics Express 18, 27938–27954 (2010), doi:10.1364/OE.18.027938

[8] Jain, N., Wittmann, C., Lydersen, L., Wiechers, C., Elser, D., Marquardt, C., Makarov, V., Leuchs, G.: Device calibration impacts security of quantum key distribution. Phys. Rev. Lett. 107, 110501 (2011), doi:10.1103/PhysRevLett.107.110501

[9] Lydersen, L., Skaar, J., Makarov, V.: Tailored bright illumination attack on distributed-phase-reference protocols. J. Mod. Opt. 58, 680–685 (2011), doi:10.1080/09500340.2011.565889

[10] Lydersen, L., Akhlaghi, M.K., Majedi, A.H., Skaar, J., Makarov, V.: Controlling a superconducting nanowire single-photon detector using tailored bright illumination. New J. Phys. 13, 113042 (2011), doi:10.1088/1367-2630/13/11/113042

[11] Lydersen, L., Makarov, V., Skaar, J.: Comment on Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. Appl. Phys. Lett. 99, 196101 (2011), doi:10.1063/1.3658806

[12] Sauge, S., Lydersen, L., Anisimov, A., Skaar, J., Makarov, V.: Controlling an actively-quenched single photon detector with bright light. Opt. Express 19, 23590–23600 (2011)

[13] Lydersen, L., Jain, N., Wittmann, C., Maroy, O., Skaar, J., Marquardt, C., Makarov, V., Leuchs, G.: Superlinear threshold detectors in quantum cryptography. Phys. Rev. Lett. 84, 032320 (2011), doi:10.1103/PhysRevA.84.032320

[14] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Avoiding the blinding attack in QKD; REPLY (COMMENT). Nature Photonics 4, 801 (2010), doi:10.1038/nphoton.2010.278

[15] Makarov, V.: Controlling passively quenched single photon detectors by bright light. New J. Phys. 11, 065003 (2009), doi:10.1088/1367-2630/11/6/065003

[16] Kish, L.B., Mingesz, R., Gingl, Z.: Unconditionally secure communication via wire. SPIE Newsroom (2007), doi:10.1117/2.1200709.0863

[17] Johnson, J.B.: Thermal agitation of electricity in conductors. Nature 119, 50–51 (1927)

[18] Nyquist, H.: Thermal agitation of electric charge in conductors. Phys. Rev. 32, 110–113 (1928)

[19] Born, M., Heisenberg, W., Jordan, P.: Quantum mechanics II. Z. Phys. 35, 557–615 (1926)

[20] Allahverdyan, A.E., Nieuwenhuizen, T.M.: Extraction of work from a single thermal bath in the quantum regime. Phys. Rev. Lett. 85, 1799–1802 (2000)

[21] Scully, M.O., Zubairy, M.S., Agarwal, G.S., Walther, H.: Extracting work from a single heat bath via vanishing quantum coherence. Science 299, 862–864 (2003)

[22] Kish, L.B.: Thermal noise engines. Chaos Solit. Fract. 44, 114–121 (2011), `http://arxiv.org/abs/1009.5942`

[23] Kish, L.B.: Noise-based logic: Binary, multi-valued, or fuzzy, with optional superposition of logic states. Phys. Lett. A 373, 911–918 (2009)

[24] Kish, L.B., Khatri, S., Sethuraman, S.: Noise-based logic hyperspace with the superposition of 2^N states in a single wire. Phys. Lett. A 373, 1928–1934 (2009)

[25] Bezrukov, S.M., Kish, L.B.: Deterministic multivalued logic scheme for information processing and routing in the brain. Phys. Lett. A 373, 2338–2342 (2009)

[26] Gingl, Z., Khatri, S., Kish, L.B.: Towards brain-inspired computing. Fluct. Noise Lett. 9, 403–412 (2010)

[27] Kish, L.B., Khatri, S., Horvath, T.: Computation using noise-based logic: Efficient string verification over a slow communication channel. Eur. J. Phys. B 79, 85–90 (2011), http://arxiv.org/abs/1005.1560

[28] Peper, F., Kish, L.B.: Instantaneous, non-squeezed, noise-based logic. Fluct. Noise Lett. 10, 231–237 (2011), http://www.worldscinet.com/fnl/10/1002/open-access/S0219477511000521.pdf

[29] Wen, H., Kish, L.B., Klappenecker, A., Peper, F.: New noise-based logic representations to avoid some problems with time complexity. Fluct. Noise Lett. (June, in press, 2012 issue), http://arxiv.org/abs/1111.3859

[30] Mullins, J.: Breaking the noise barrier. New Scientist (2780) (September 29, 2010), http://www.newscientist.com/article/mg20827801.500-breaking-the-noise-barrier.html?full=true

[31] Kish, L.B.: Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. Phys. Lett. A 352, 178–182 (2006)

[32] Cho, A.: Simple noise stymie spies without quantum weirdness. Science 309, 2148 (2005), http://www.ece.tamu.edu/~noise/news_files/science_secure.pdf

[33] Kish, L.B.: Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson(-like)-noise cipher and expansion by voltage-based security. Fluct. Noise Lett. 6, L57–L63 (2006), http://arxiv.org/abs/physics/0512177

[34] Mingesz, R., Gingl, Z., Kish, L.B.: Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. Phys. Lett. A 372, 978–984 (2008)

[35] Palmer, D.J.: Noise encryption keeps spooks out of the loop. New Scientist (2605), 32 (2007), http://www.newscientist.com/article/mg19426055.300-noise-keeps-spooks-out-of-the-loop.html

[36] Kish, L.B., Horvath, T.: Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. Phys. Lett. A 373, 901–904 (2009)

[37] Scheuer, J., Yariv, A.: A classical key-distribution system based on Johnson (like) noise – How secure? Phys. Lett. A 359, 737–740 (2006)

[38] Kish, L.B., Scheuer, J.: Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator. Phys. Lett. A 374, 2140–2142 (2010)

[39] Kish, L.B.: Response to Scheuer-Yariv: A classical key-distribution system based on Johnson (like) noise – How secure? Phys. Lett. A 359, 741–744 (2006)

[40] Hao, F.: Kish's key exchange scheme is insecure. IEE Proc. Inform. Sec. 153, 141–142 (2006)

[41] Kish, L.B.: Response to Feng Hao's paper Kish's key exchange scheme is insecure. Fluct. Noise Lett. 6, C37–C41 (2006)

[42] Liu, P.L.: A new look at the classical key exchange system based on amplified Johnson noise. Phys. Lett. A 373, 901–904 (2009)

[43] Horvath, T., Kish, L.B., Scheuer, J.: Effective privacy amplification for secure classical communications. Europhys. Lett. 94, 28002 (2011), http://arxiv.org/abs/1101.4264

[44] Kish, L.B., Saidi, O.: Unconditionally secure computers, algorithms and hardware. Fluct. Noise Lett. 8, L95–L98 (2008)

[45] Kish, L.B., Mingesz, R.: Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise. Fluct. Noise Lett. 21, C9-C21 (2006)

[46] Kish, L.B., Peper, F.: Information networks secured by the laws of physics. IEICE Trans. Commun. E95-B, 1501–1507 (2012)

[47] http://en.wikipedia.org/wiki/Quantumcomputer

[48] Wiesner, S.: Conjugate coding. SIGACT News 15, 78–88 (1983)

[49] Bennett, C.H., Brassard, G.: Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing. In: Proc. IEEE Internat. Symp. Inform. Theor., St-Jovite, Canada, p. 91 (1983)

[50] Brassard, G.: Brief history of quantum cryptography: A personal perspective. In: Proc. IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan, pp. 19–23 (2005), http://arxiv.org/abs/quant-ph/0604072

[51] Xu, F., Qi, B., Lo, H.K.: Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J. Phys. 12, 113026 (2010), http://arxiv.org/abs/1005.2376

[52] Liang, Y., Poor, H.V., Shamai, S.: Information Theoretic Security. Foundations and Trends in Communications and Information Theory 5, 355–580 (2008), doi:10.1561/0100000036

[53] Vincent Poor, private communications

The Biometric Menagerie – A Fuzzy and Inconsistent Concept

Nicolaie Popescu-Bodorin[1], Valentina Emilia Balas[2], and Iulia Maria Motoc[1]

[1] Artificial Intelligence & Computational Logic Lab.,
Mathematics & Computer Science Department,
Spiru Haret University, Bucharest Romania
{bodorin,motoc}@irisbiometrics.org
[2] Automatics and Applied Software Department,
Faculty of Engineering, Aurel Vlaicu University,
Arad, Romania
balas@drbalas.ro

Abstract. This paper proves that in iris recognition, the concepts of *sheep*, *goats*, *lambs* and *wolves* - as proposed by Doddington and Yager in the so-called Biometric Menagerie, are at most fuzzy and at least not quite well defined. They depend not only on the users or on their biometric templates, but also on the parameters that calibrate the iris recognition system. This paper shows that, in the case of iris recognition, the extensions of these concepts have very unsharp and unstable (non-stationary) boundaries. The membership of a user to these categories is more often expressed as a degree (as a fuzzy value) rather than as a crisp value. Moreover, they are defined by fuzzy Sugeno rules instead of classical (crisp) definitions. For these reasons, we said that the Biometric Menagerie proposed by Doddington and Yager could be at most a fuzzy concept of biometry, but even this status is conditioned by improving its definition. All of these facts are confirmed experimentally in a series of 12 exhaustive iris recognition tests undertaken for University of Bath Iris Image Database while using three different iris code dimensions (256x16, 128x8 and 64x4), two different iris texture encoders (Log-Gabor and Haar-Hilbert) and two different types of safety models.

Keywords: iris recognition, fuzzy, inconsistent, biometric menagerie.

1 Introduction

While working around speech recognition, Doddington et al. introduced in [2] four concepts reflecting four types of users: *sheep*, *goats*, *lambs* and *wolves* – which together form the so-called Biometric Menagerie. The second section of this paper presents an objective critique of this concept.

As far as we know, in 2010, N. Yager et al. [12] generalized Doddington's classification (also known as Doddington's zoo) for all fields of biometrics. Since then, just two papers investigating the presence of sheep, goats, lambs and wolves in certain benchmark databases have been published.

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 27–43.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

After [7] and [4], this is the third paper that analyses the partitioning of the iris code space extracted for a certain database (University of Bath Iris Image Database, UBIID, [10] – in our case) as a Fuzzy Biometric Menagerie showing that the extensions of the concepts *wolf*, *lambs*, *sheep* and *goats* have very unsharp and unstable (non stationary) boundaries. Moreover, the membership of a user to these categories can be more often expressed as a degree (as a fuzzy value) rather than as a crisp value. The fact that the Biometric Menagerie could be a fuzzy concept is confirmed experimentally here in a series of 12 exhaustive iris recognition tests undertaken for UBIID [10] by using three different iris code dimensions (256x16, 128x8 and 64x4), two different iris texture encoders (Log-Gabor and Haar-Hilbert [6]) and two different types of safety models [8]. All of these tests illustrate that the partitioning of template-space accordingly to the fuzzy concepts *wolves*, *lambs*, *sheep*, and *goats* depends not only on the users or on their biometric templates, but also on the parameters that calibrate the iris recognition system – fact which is also confirmed in [3] for a different iris image database (Iris Challenge Evaluation, [3]).

2 'Biometric Menagerie' in Iris Recognition. Open Problems and Contradictory Issues

Doddington et al. [2] and Yager et al. [12] defined the concepts of *sheep-user*, *goat-user*, *lamb-user* and *wolf-user* as follows:

Definition 1 (Yager, [12]):

- The *sheep* are those users for which the similarity score is high for genuine comparisons and low for imposter comparisons;
- The *goats* are those users which, most of the time, obtain low similarity scores for genuine comparisons;
- The *lambs* are those users easy to imitate (by *wolves*) and for which the similarity score for imposter comparison can be relatively high.
- The *wolves* are those users particularly good at impersonating other users (or in other words, as Yager said, the *wolves* "prey upon *lambs*" [12]) obtaining relatively high similarity scores for imposter comparison between them and the lambs.

2.1 Classifying Users vs Classifying Templates

Firstly, anyone should remark (we certainly did it) that classifying users in the first place is not necessarily a very good idea, simply because, any claimed relation that possibly hold two users or more is caused by something that happens with certain binary biometric templates stored in the system on their name. What happens with the templates determines what happens with the users, not vice versa. Hence, in any biometric system (including those based on iris recognition), the natural approach to classifying users goes through classifying biometric templates (through classifying iris codes - in our particular case). Therefore, a correct foundation for a hypothetically objective model called Biometric Menagerie should start with defining the *'animals'* [12] by analyzing their hypostases, i.e. in terms of biometric templates:

Definition 2:

- The *sheep-templates* are those for which the similarity scores associated to their genuine comparisons are *high enough* and the similarity scores associated to their imposter comparisons are *low enough* such that a safety threshold or a safety interval to separate the two distributions of genuine and imposter scores computed for them;
- The *goat-templates* are those that, *most of the time* or *too often*, obtain low similarity scores for their genuine comparisons;
- The *lamb-templates* are those *easy to imitate* (by wolves) and for which the similarity scores associated to their imposter comparisons can be relatively high;
- The *wolf-templates* are those particularly good at matching lamb-templates, obtaining *relatively high* similarity scores for imposter comparison between them and their pray (lamb-templates);
- *Biometric Menagerie* is a partitioning of biometric template space into the four classes defined above.

2.2 Fuzzy Biometric Menagerie vs System Calibration

Secondly, even admitting the fact that Biometric Menagerie is a well-defined concept, all conditions expressed in the above two definitions are rather fuzzy if-then Sugeno rules [11] than regular conditions of a classical definition – i.e. conditions on *genus and differentia* that do not contain fuzzy elements. More precisely, both definitions are intensional, the genus being the space of biometric templates, whereas a fuzzy rule declares the differentia. Therefore, there is no doubt that Biometric Menagerie is a fuzzy partitioning of the biometric templates space in sub-classes defined as extensions of the fuzzy concepts (pre-images of the fuzzy labels) sheep, goats, lambs and wolves, regardless the fact that it could refer to users or to biometric templates. As an example, let us formalize one condition of the second definition as a fuzzy if-then Sugeno rule:

IF: T is a biometric template
associated to
high genuine scores
and
low imposter scores
THEN: T is a sheep-template

whose structure is similar to that of a linguistic control rule [11] describing a multi-input & single-output system:

IF: X is *f-label-1* and Y is *f-label-2* THEN: Z is *f-label-3.*

As seen above, the concept of sheep-template is fuzzy and so it is the entire Biometric Menagerie. Despite the fact that the genus of sheep-template is a crisp set, is the fuzzy rule from above that declares the differentia using the fuzzy linguistic labels *'high'* and *'low'* whose possible quantitative semantics correspond to a choice of some underlying fuzzy sets associated with some membership functions. Someone must choose a numerical interpretation of what it means to be *high* as a genuine score and *low* as an imposter score, operation usually referred to as a part of calibrating the biometric system. Therefore, our first hunch (now partially validated through experimental work) was that the Biometric Menagerie is rather depending on the calibration of biometric system than being an objective concept, well defined and applicable in general for the users that pass through different single-biometric systems that use the same biometric trait (iris, face, fingerprint, palm-vein, etc.).

2.3 From Partitioning Templates to Partitioning Users

Let us assume that in an iris recognition system we need to define a partitioning of the users according to what happens with their biometric templates. For example, we could consider the case in which a user U_1 posses a template T_1 that candidates for the role of being a wolf-template by obtaining six imposter similarity scores high enough to generate six false accepts with six different users. In the same system, a user U_2 posses the templates T_2^1, T_2^2, T_2^3, each of them obtaining two imposter similarity scores high enough such that together they generate the same number of six false accepts with six different users. As seen in our example, detecting a wolf-user could be a problem of finding a group of template-wolves that together satisfy some conditions. The question is which one of those two users is a wolf-user. The answer hardly depends on a convention that the system use for qualifying users as wolves based on what happens with their templates (taken individually or as a group). At least because it relies on the detection of some wolf-templates - detection done by following a fuzzy rule (as described above), such a convention is a fuzzy if-then rule also:

IF:	for the user U there is a group G of its templates satisfying a *well chosen* f-convention *FC*	THEN:	U is a *wolf-user*

Hence, in the rule described above, besides the fact that the detection of the individual wolf-templates is fuzzy, there are two additional degrees of freedom for interpreting the fuzzy labels *"well chosen"* and *"FC"*. This fact makes the process of identifying the wolf-users even fuzzier and more subjective than the process of finding wolf-templates. Consequently, the concept of Biometric Menagerie as introduced by Doddington et al. in [2] and Yager et al. in [12] and even the concept of Biometric Menagerie discussed here in definition 2 are all fuzzy and subjective concepts, regardless if they consist in partitioning users or templates.

The fact itself that the process of partitioning the users or the templates in a Biometric Menagerie is a fuzzy one cannot be negatively connotated by default, excepting, of course, the cases in which there is not enough cointension between this artificial partitioning and the natural tendency of grouping that users actually have in reality. Unfortunately, this is exactly the case here, as shown below.

Biometric recognition is a diachronic process and therefore the basic vocabulary of any recognition theory should refer user instances, i.e. pairs (U, t) where U is a user and t is a time.

A recognition theory is logically consistent if and only if, regardless the time values t_1 and t_2, the similarity $(U_1, t_1) \equiv (U_2, t_2)$ certainly take place only for the same user $U_1 = U_2$. In other words, all users enrolled in the system diachronically generate a set of genuine comparisons that posses the pattern (U, t_1)-to-(U, t_2) and a set of imposter comparisons that also share a common pattern (U_1, t)-to-(U_2, τ) with $U_1 \neq U_2$ (the relation between t and τ having no importance in this case). Hence, the natural tendency of grouping that user instances actually have points out to only two classes, not to four classes – as the Biometric Menagerie has.

The situation described above is an important example illustrating that *fuzzy* could sometimes mean *logically inconsistent*, such is the case of artificial partitioning of the users in a Biometric Menagerie with four fuzzy classes, while the natural tendency of grouping that the users actually have in a consistent theory of recognition point out to a binary classification.

2.4 FBM vs. Iris Codes Space Homogeneity

According to the above definitions, the wolves are those users (proved or suspected – depending on how accurate the wolf definition actually is) responsible for much of the False Accept Rate (FAR), whereas the goats are the users responsible for much of the False Reject Rate (FRR). This is why the current paper gives a special attention to these two categories of users.

However, right from this moment it is very clear that accepting the above definitions would mean to accept that some users would be somehow special (more special than others) and therefore, some elements of the iris code space would be somehow more special than others, hence, the question if the iris code space is homogeneous or heterogeneous would certainly appear.

A thing to know for sure is if the iris code space actually is homogeneous or not. We believe it is. The situation described above is a classical kind of example illustrating that when adding something that initially appears inoffensive to a model (like a classification of users – in the current case) actually blows up the foundations of the model by introducing the contradiction in its logic. Let us assume that the iris code space is heterogeneous (i.e. it supports the definition 2) and that the partitioning of iris codes space is cointensive with a corresponding partitioning of user space, which consequently is heterogeneous on its turn. Can anybody tell us what makes the user space heterogeneous in the first place?

In a lottery, many players can win the minor prizes by partially matching the official extracted variant. Hence, we could say that the extracted variant is a wolf hunting on lambs (the winners of the minor prizes). We could say, but we do not say that. Nothing aggregates the group of these winners together, except the pure chance. In the same manner, the odds produce the matching between one specific iris code and many others purely by chance, meaning that the iris code space is locally too agglomerated and this agglomeration could become homogeneously present in the iris code space. The solution is not to invent wolves and lambs, but to recalibrate the system by increasing the power of discrimination between the future biometric templates.

2.5 FBM vs. Similarity Score Symmetry

The fact that Biometric Menagerie is fuzzy (regardless it refers to users or templates) is not the worst thing in the world. The real problem is that it is not objective. In order to prove that, let us comment the wolf-lamb relation.

According to Yager et al. [12], wolf-lambs relation is one-to-many, one wolf taking many lambs. However, in a biometric system in which the relation between users (between templates) is symmetric (why should not be?), if the user U_1 (the template T_1) impersonates the user U_2 (the template T_2), it is equally true that the user U_2 (the template T_2) impersonates the user U_1 (the template T_1), also. Therefore, it is not clear at all who is the hunter and who is hunted. Someone has chosen to say that, most probably (according to some experiences), the wolves take many lambs. Our question is: what if, actually, *many wolves target the same lamb*.

The situation described above allows us to say that denoting some users (templates) as wolves and others as lambs is a pure subjective convention which really affects the objectivity of Biometric Menagerie as a concept.

3 Experimental Results

This section presents the results of 12 exhaustive iris recognition tests, undertaken on the database [10], using iris codes of dimensions 256x16, 128x8 and 64x4.

All tests use the second version of Circular Fuzzy Iris Segmentation procedure (CFIS2, proposed in [5], available for download in [7]), the iris segments being further normalized to the appropriate dimension and encoded as binary iris codes by using Haar-Hilbert [6] and Log-Gabor [6] texture encoders. Each comparison between iris codes results in a matching score computed as Hamming similarity (unitary complement of Hamming distance). For each test, all-to-all comparisons result in similarity scores further interpreted as being *low* or *high* enough to motivate a biometric decision accordingly to the following two fuzzy if-then Sugeno [11] rules:

IF:	MS(C) is *low*	THEN:	C is (an) *imposter comparison*
IF:	MS(C) is *high*	THEN:	C is (a) *genuine comparison*

where MS is the matching score and C is a comparison.

3.1 Two Paradigms of Test Scenarios

For each test, the precisiation of the security model assumes the deffuzification of the fuzzy labels *'low'* and *'high'* as intervals situated on the left and right sides relative to a threshold value identified as the abscise of the EER point:

$$t_{EER} = (FAR^{-1}(EER)= FRR^{-1}(EER)),$$

or either relative to a safety interval initialized and determined maximally by the minimum Genuine Score (mGS) and the Maximum Imposter Score (MIS), and further decreased iteratively until the extensions of the f-concepts *'wolf'* and *'lamb'* become populated with some examples of wolf- and lamb-templates, respectively. For a given calibration of the recognition system established in terms of segmentation, normalization and encoding procedures, the safety model corresponding to the second case described above (that using a safety interval) is described by the following fuzzy 3-valent disambiguated model:

IF:	MS(C) is *under* the safety band	THEN:	C is an *imposter comparison*
IF:	MS(C) is *within* the safety band	THEN:	C is *undecidable*
IF:	MS(C) is *above* the safety band	THEN:	C is a *genuine comparison*

3.2 The Dynamics of FBM. The First and the Last Wolves and Goats

If the safety band is maximal - i.e. the safety band is the interval [mGS, MIS], all the comparisons within MS^{-1}([mGS, MIS]) are undecidable and therefore there are no wolfs, no lambs and no goats in the system, all users and templates qualifying as sheep. When the safety band narrows from both sides toward the threshold corresponding to the experimentally determined EER point, the examples of wolf-, lamb- and goat-templates slightly came into view. For this reason, we called these kind of templates *marginal wolf-*, *lamb-* and *goat-templates*. They are the first wolves, lambs and goats that appear in the system when the level of security decreases from the maximal safety band toward the threshold t_{EER}. The idea of searching for wolves and goats while the safety band narrows toward t_{EER} allow us to analyze the dynamics of Biometric Menagerie along the process of decreasing the safety level in a balanced manner that negotiates between false accepts and false rejects. Besides, in order to compare the partitioning of the users/templates in two different iris recognition systems, it was necessary to identify functioning regimes in which the two systems are objectively comparable. We found two functioning regimes of this kind: one identified through the maximal safety band [mGS, MIS] and other identified through t_{EER}. These two functioning regimes are the extreme cases between which anyone can study the variability of Biometric Menagerie while the safety band converges to t_{EER} through hypostases that balance the FAR-FRR risks. Safety band hypostases together simulate a family of decreasing nested Cantor intervals allowing us to see the stabilization of the Biometric Menagerie as a process of convergence, along which different iris recognition system are comparable. The last interval of this family is the smallest (first) in the order of inclusion and the last in the order given by the balanced risks assumed in the system. For this reason, we called the members of Biometric Menagerie detected when the system runs at EER, as being the last ones (*last wolf-, lamb- and goat-templates*). They are the last detected of their kind when system security falls in a balanced manner to the EER. All of these things allow us to state the following definition:

Definition 3: Let us consider an iris recognition system in which the score distributions overlap each other. Then:

- the *first wolf-, lamb- and goat-templates* are those detected when the system is running at the security level given by the first fuzzy 3-valent disambiguated model [8] in which they appear when the maximal safety band [mGS, MIS] narrows to t_{EER} such that to keep FAR-FRR risks balanced.
- the *last wolf-, lamb- and goat-templates* are those detected when the system is running at EER (i.e. the system is running on that safety threshold which balances the FAR-FRR risks).

3.3 Two Series of Tests

The first series of six tests aims to identify the indices of the *first wolf* and *goat-templates* detected when running the system with different encoders (Haar-Hilbert and Log-Gabor), with different iris code dimensions (256x16, 128x8, 64x4), at a high security level given by that safety band who allows the wolves and the goats to appear in the system. Table 1 shows the values determining the safety bands detected for each of these tests.

Table 1. The safety bands and their width for the first series of six all-to-all iris recognition tests

	Iris code dimension	64x4	128x8	256x16
Log-Gabor encoder	Safety band	[0.6003, 0.9075]	[0.6277, 0.6555]	[0.5566, 0.5757]
	Width	0.3072	0.0278	0.0191
Haar-Hilbert encoder	Safety Band	[0.6091, 0.6722]	[0.5456, 0.6823]	[0.5224, 0.5467]
	Width	0.0631	0.1367	0.0243

The second series of six tests has the same purposes as the first one, but each time the system is running at a maximally acceptable balanced degradation of the security level given by functioning at EER threshold (t_{EER}). Table 2 shows the values determining the safety bands detected for each of these tests.

Table 2. The EER and t_{EER} for the second series of six all-to-all iris recognition tests

	Iris code dimension	64x4	128x8	256x16
Log-Gabor encoder	EER	4.08E-2	9.37E-4	6.03E-4
	t_{EER}	0.7529	0.6392	0.5686
Haar-Hilbert encoder	EER	8.60E-3	1.70E-3	2.30E-3
	t_{EER}	0.6471	0.5765	0.5490

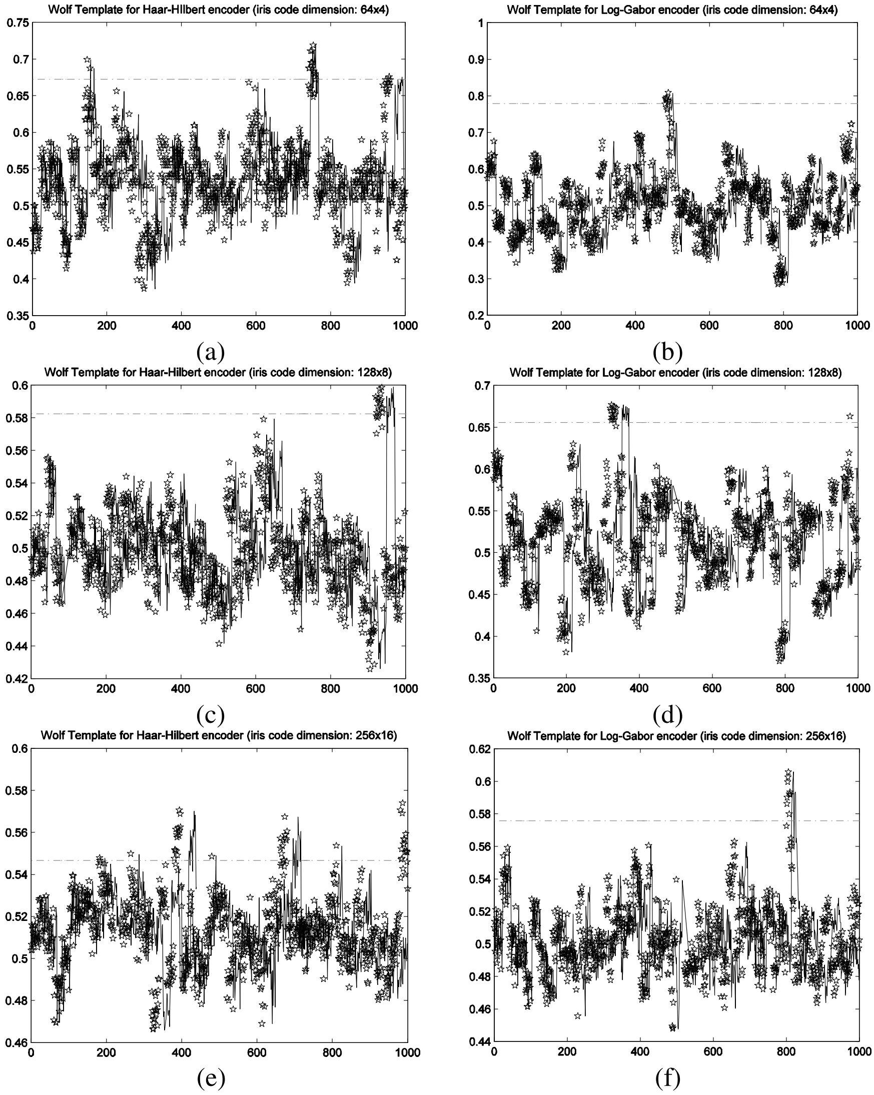
As seen in Table 2, accordingly to the EER criterion, the best calibration of the iris recognition system is that one using iris segments of dimension 256x16 and based on Log-Gabor encoder (EER = 6.0265E-4).

Also, the best calibration presented in Table 1 is that one having the smallest overlapping between the two score distributions, namely that one using iris segments of dimension 256x16 and based on Log-Gabor encoder (for which the amplitude of the overlapping is 0.0191).

3.4 Detecting the Marginal Wolf and Goat Templates

We recall that the safety bands used in the first series of six iris recognition tests are adaptively determined by narrowing the maximal safety band [mGS, MIS] toward t_{EER} while keeping the FAR-FRR risks balanced, until some examples of wolf and goat templates appear in the system (ensuring that the extensions of the corresponding concepts are not empty). Hence, each test results in a set containing the *first* (the *marginal*) *goat-* and *wolf-templates* corresponding to a given calibration of the biometric system in terms of encoder and iris code size.

Fig. 1 illustrates the fact that although the iris code dimension increases, the number of impersonations oscillates when using Log-Gabor encoder, and increases when using Haar-Hilbert encoder. As seen by comparing Fig. 1.a and Fig. 1.b (both of them obtained for the iris codes of dimension 64x4), the number of cases of impersonation was higher for the wolf-template obtained for Haar-Hilbert encoder than the one obtained for Log-Gabor encoder.



(a) (b)

(c) (d)

(e) (f)

Fig. 1. The *marginal wolf-templates* obtained for Haar-Hilbert (64x4 – a, 128x8 – c, 256x16 – e) and Log-Gabor (64x4 – b, 128x8 – d, 256x16 – f) encoders

Table 3. The *marginal wolf-/goat-templates* obtained by finding the corresponding safety band

	Iris code dimension	64x4	128x8	256x16
	Template type	Wolf | Goat	Wolf | Goat	Wolf | Goat
Log-Gabor encoder	Number of comparisons	7 | 4	17 | 3	9 | 3
	Template's index	**334 | 496**	**484 | 475**	**505 | 565**
Haar-Hilbert encoder	Number of comparisons	15 | 3	15 | 3	46 | 4
	Template's index	**549 | 565**	**88 | 565**	**236 | 565**

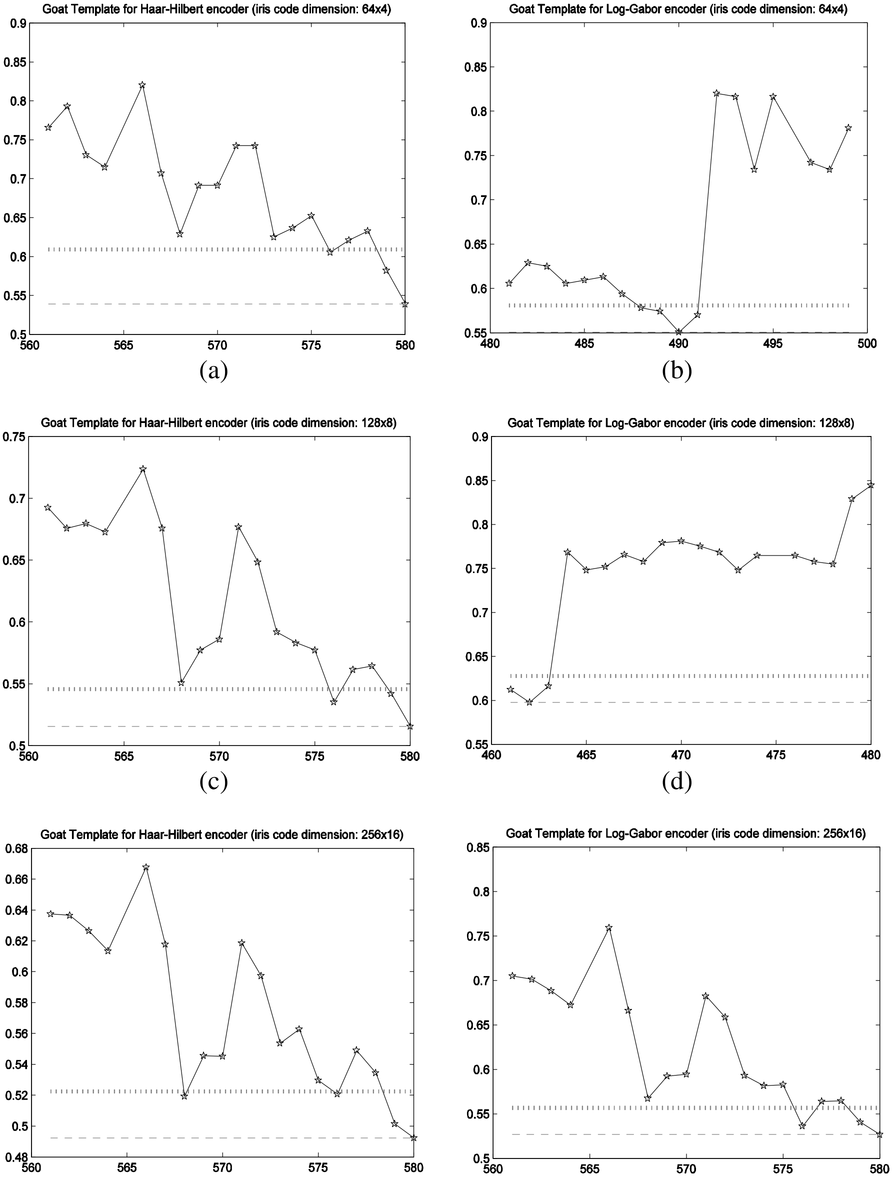
For iris codes of dimension 128x8 (Fig. 1.c and Fig. 1.d), the number of impersonations obtained when using Haar-Hilbert encoder is smaller that when using Log-Gabor encoder. For iris code of dimension 256x16, the Haar-Hilbert encoder obtained the greatest number of impersonations, as we can observe also by comparing the behavior of the wolf templates represented in Fig. 1.e and Fig. 1.f.

Table 3 presents the results obtained in these six tests performed to find the *marginal wolf-templates*. As seen in Table 3, each test points out to a different *marginal wolf-template* (which is an experimental result that agrees to those presented in [4] for the wolves detected in ICE database [3]).

The number of (qualifying) comparisons recorded in Table 3 must be interpreted differently according to the type of determination that it is linked to: for a wolf it represents the number of false accepts, whereas for a goat it represents the number of false rejects. For example: when using Log-Gabor encoder to generate iris codes of dimension 64x4, the detected *marginal wolf-template* is 334 and it generates 7 cases of impersonation, whereas in the same conditions the *marginal goat-template* is 496 and it generates 4 cases of false reject. What is spectacular in the Table 3 in the first place is that the *marginal goat-template* 496 (Log-Gabor, 64x4) and the *marginal wolf-template* 484 (Log-Gabor, 128x8) point out to the same eye, namely the 25th eye, i.e. the left eye of the 13th user from the database UBIID, [10]. Section 2.3 illustrated the fact that trying to qualify users as wolves or goats based on what happens with their template is not quite a simple and evident task. The situation described here reveals an additional degree of difficulty to the same problem, also. Based on the data reported in Table 3, is the left eye of 13th user a wolf, a goat or both? This aspect is also a facet of the inconsistency of Biometric Menagerie as a concept.

Fig. 2 illustrates that along with the increasing of the iris code dimension the number of rejections decreases for Log-Gabor encoder and increases for Haar-Hilbert encoder. In each graphic, we drawn the left limit of the safety band (dotted line) and the minimum genuine score (dashed line) obtained for the corresponding *marginal goat template*. Fig. 2.a and Fig. 2.b present the behavior of the *marginal goat-templates* obtained for iris codes of dimension 64x4. The template obtained for Log-Gabor encoder has a bigger number of rejections than the one resulted for Haar-Hilbert encoder. On the contrary, the numbers of rejections for the templates represented in Fig. 2.c and Fig. 2.d are the same for both encoders.

As seen in Fig. 2.e and Fig. 2.f, there are more cases of false reject for the *marginal goat-template* obtained with Haar-Hilbert encoder than for the one obtained with Log-Gabor encoder.



(a) (b)

(c) (d)

(e) (f)

Fig. 2. The *marginal goat-templates* obtained for Haar-Hilbert (64x4 – a, 128x8 – c, 256x16 – e) and Log-Gabor (64x4 – b, 128x8 – d, 256x16 – f) encoders

Let us comment another remarkable thing seen in the same Table 3: the *marginal goat-template* obtained for Haar-Hilbert encoder was the same in all three tests. Moreover, it is the *last goat-template* obtained for the same encoder (see Table 4, from below). This situation suggests that the concept of *'goat-template' could* be an objective concept (in certain conditions) unifying the concepts of *first* (*marginal*) and *last goat-templates* by actually depending much on the encoded iris segment and less on the size of the template. The third notable thing visible in Table 3 is that the *marginal wolf-templates* obtained for the six tests were not only different, but also came from different eyes (users). Different iris recognition systems can perceive differently the *marginal wolf-templates*, and consequently, the concept of *marginal wolf-template* is certainly far from being objective.

3.5 Detecting the Last Wolf and Goat Templates at t_{EER}

We recall that the safety levels corresponding to the second series of six exhaustive all-to-all iris recognition tests (further presented here) are those given by running the recognition system at EER threshold t_{EER}. Hence, according to the definition 2, each of these tests results in a set containing the *last goat-* and *wolf-templates* corresponding to a given calibration of the biometric system in terms of encoder and iris code size.

Fig. 3 presents the similarity scores obtained by the *last wolf-templates* mentioned in Table 4 and detected in this second series of tests.

Table 4. The *last wolf-/goat-templates* obtained by running the system at t_{EER}

	Iris code dimension	64x4	128x8	256x16
	Template type	Wolf I Goat	Wolf I Goat	Wolf I Goat
Log-Gabor encoder	Number of comparisons	63 I 11	22 I 4	14 I 5
	Template's index	**236 I 493**	**392 I 462**	**236 I 565**
Haar-Hilbert encoder	Number of comparisons	43 I 8	19 I 6	40 I 9
	Template's index	**549 I 565**	**88 I 565**	**236 I 565**

Table 5. The cumulative results of the two series of all-to-all exhaustive iris recognition tests (on UBIID, [10]) expressed in terms of *first* and *last goat- and wolf-templates*

Calibration	Goats		Wolves	
	First (Marginal)	Last	First	Last
LG, 64x4	496	493	334	236
LG, 128x8	475	462	484	392
LG, 256x16	565	565	505	236
HH, 64x4	565	565	549	549
HH, 128x8	565	565	88	88
HH, 256x16	565	565	236	236

Table 6. The cumulative results of the two series of all-to-all exhaustive iris recognition tests (on UBIID, [10]) expressed in terms of *possible first* and *last goat- and wolf-users*

Calibration	Goats		Wolves	
	First (Marginal)	Last	First	Last
LG, 64x4	25	25	17	12
LG, 128x8	24	24	25	20
LG, 256x16	28	28	26	12
HH, 64x4	29	29	23	23
HH, 128x8	29	29	5	5
HH, 256x16	29	29	12	12

As in the previously discussed case of *marginal wolf-templates*, it is visible in Table 4 that the *last wolf-templates* obtained for the six tests were not only different, but also came from different eyes (users). Different iris recognition systems can perceive differently the *last wolf-templates*, and consequently, the concept of *last wolf-template* is far from being objective.

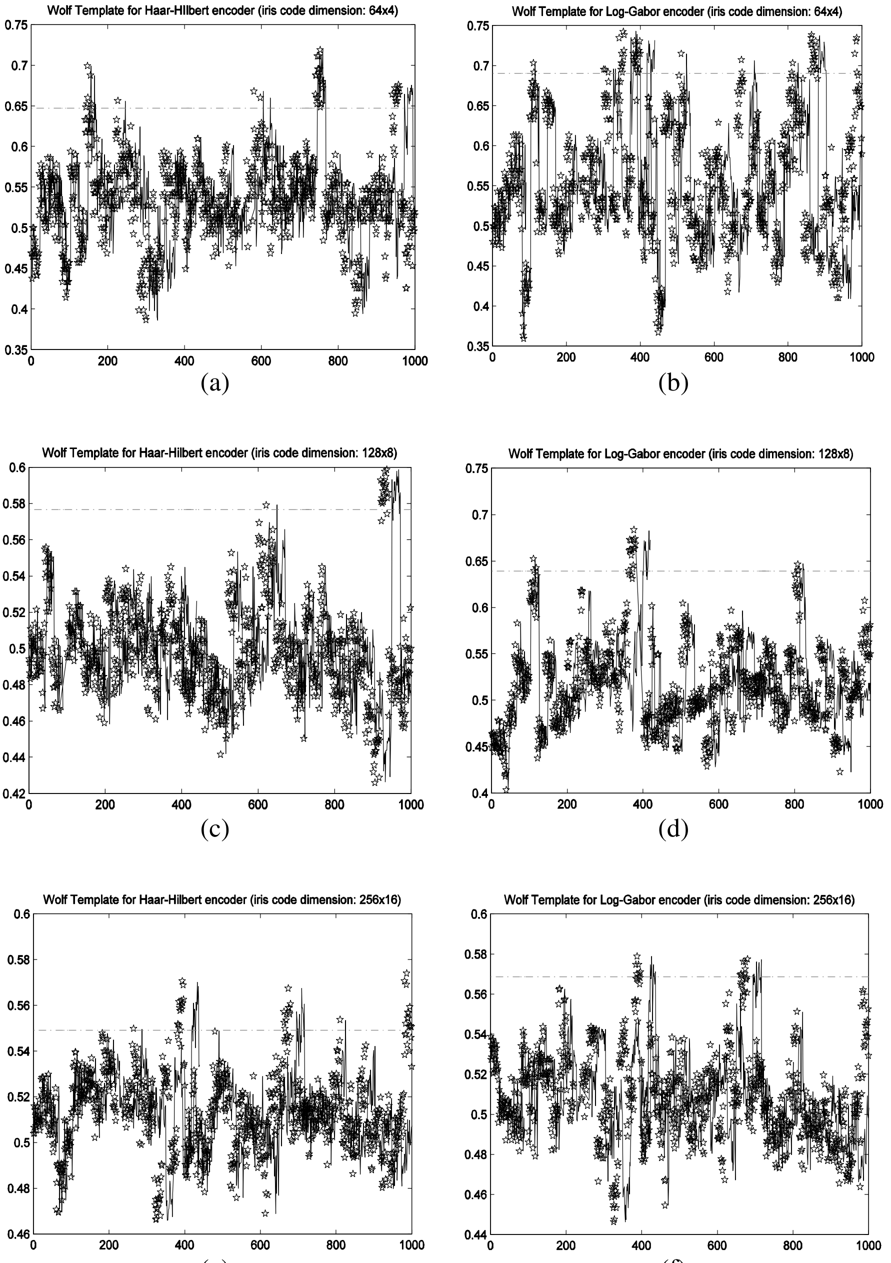
However, there are three different tests pointing out to the template no. 236 (see Table 4) as a *last wolf-template*. Still, this fact alone is not enough for qualifying the concept as being objective. Its extension is strongly dependent on system calibration variables such as the iris code dimension and the texture encoder.

Fig. 4 represents the similarity scores corresponding to the genuine comparisons generated by the *last goat-templates* obtained from the tests that use Haar-Hilbert and Log-Gabor encoders. It illustrates the fact that along with the increasing size of the iris code, the number of false rejects could decrease sometimes.

Table 5 and Table 6 illustrate the cumulative results of the two series of all-to-all exhaustive iris recognition tests (on UBIID, [10]) expressed in terms of *first* and *last goat-* and *wolf-templates* (Table 5), and in terms of *possible first* and *last goat-* and *wolf-users* (Table 6). We said “possible first and last goat- and wolf-users” because, as seen in Section 2.3, the process of identifying the wolf-users is even fuzzier and more subjective than the process of finding wolf-templates (there is not an unique rule that could qualify users as wolves based on what is happening with their templates). Specifically, the if-then fuzzy rule used here for this purpose is simple as follows:

IF: U *posses a wolf-/goat-template* THEN: U is a *wolf-/goat-user.*

The data within Table 5 generate the data within Table 6 by applying the above if-then fuzzy rule. The data within both tables allow us to conclude that the goat is the most objective concept of the Fuzzy Biometric Menagerie and Haar-Hilbert encoder is more objective than Log-Gabor encoder.

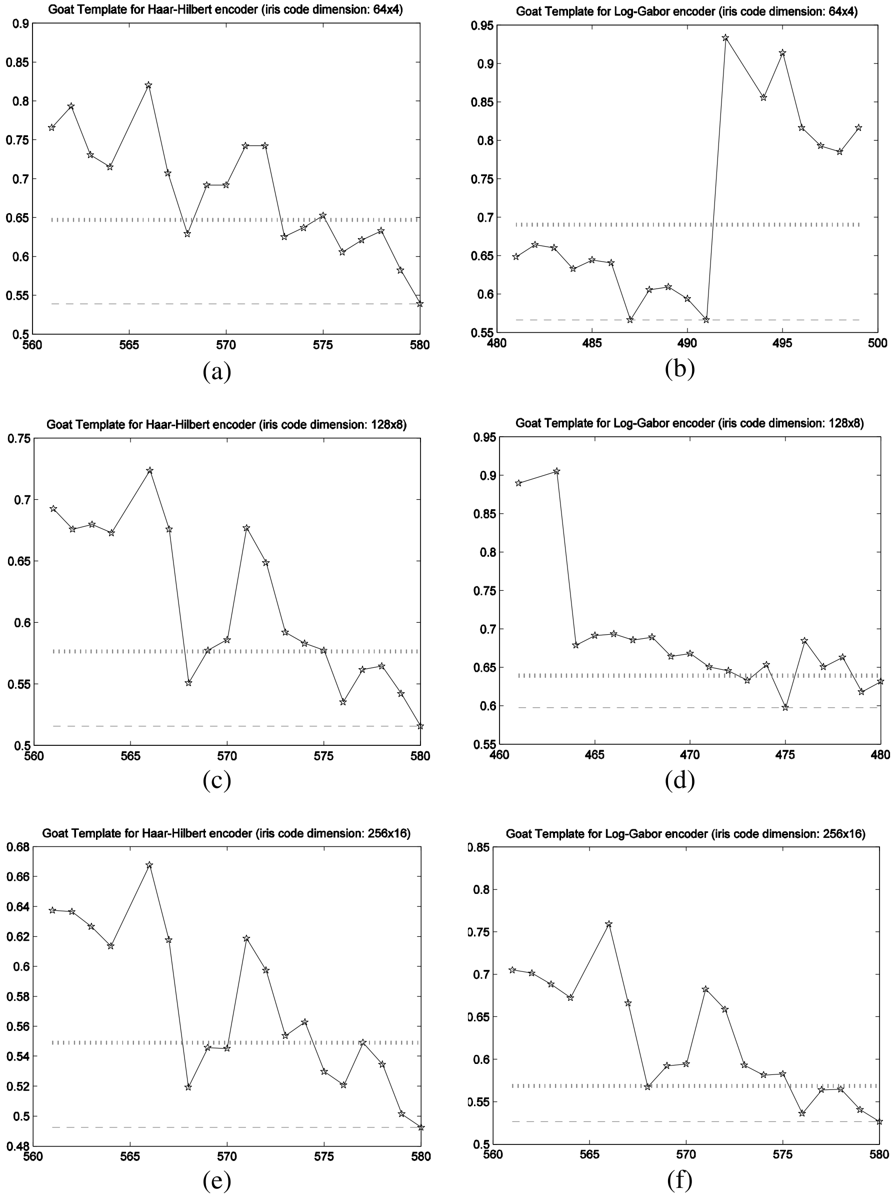


(a) (b)

(c) (d)

(e) (f)

Fig. 3. The similarity scores corresponding to the imposter comparisons generated by the *last wolf-templates* obtained for Haar-Hilbert (64x4 – a, 128x8 – c, 256x16 – e) and Log-Gabor (64x4 – b, 128x8 – d, 256x16 – f) encoders



Goat Template for Haar-Hilbert encoder (iris code dimension: 64x4)

(a)

Goat Template for Log-Gabor encoder (iris code dimension: 64x4)

(b)

Goat Template for Haar-Hilbert encoder (iris code dimension: 128x8)

(c)

Goat Template for Log-Gabor encoder (iris code dimension: 128x8)

(d)

Goat Template for Haar-Hilbert encoder (iris code dimension: 256x16)

(e)

Goat Template for Log-Gabor encoder (iris code dimension: 256x16)

(f)

Fig. 4. The similarity scores corresponding to the genuine comparisons generated by the *last goat-templates* obtained from the tests that use Haar-Hilbert (iris code dimension: 64x4 – a, 128x8 – c, 256x16 – e) and Log-Gabor (iris code dimension: 64x4 – b, 128x8 – d, 256x16 – e) encoders

4 Conclusions

This paper shown that, at least in iris recognition, the Biometric Menagerie is a fuzzy and inconsistent concept, regardless if it refers to the users or to their biometric templates. Twelve exhaustive all-to-all iris recognition tests proved this point by conterexample. They also suggest that the goat is the most objective concept of the Fuzzy Biometric Menagerie and that Haar-Hilbert encoder is more objective than Log-Gabor encoder is.

The experimental results presented in this paper shown that the fuzzy-linguistic labels defining the Biometric Menagerie in terms of *wolf-*, *sheep-*, *lamb-*, *goat-users* and those defining the Fuzzy Biometric Menagerie in terms of *first/last wolf-*, *sheep-*, *lamb-*, *goat-templates* or in terms of *possible wolf-*, *sheep-*, *lamb-*, *goat-users*, all of them depend on the calibration of the iris recognition system.

Paradoxically, this paper gave a new perspective on the fuzzy concepts sheep, goats, lambs and wolves, but a very critical one. By illustrating the fact that, different iris recognition systems actually perceive differently the wolf- and goat-templates, the current paper qualifies the concept of Biometric Menagerie as not heaving one of the most important and most needed attribute of a concept, namely the *universality* with respect to a *genus*.

We wonder if anybody could indicate us a sufficiently large class of iris recognition systems for which the partitioning of the users/templates as a Biometric Menagerie (fuzzy or not) is at least *almost* the same.

Until then, we will remember one of Newton's mottos: *hypotheses non fingo*.

Acknowledgments. The authors would like to thank Professor *Donald Monro* (Dept. of Electronic and Electrical Engineering, University of Bath, UK) for granting the access to the Bath University Iris Image Database.

References

[1] Balas, V.E., Motoc, I.M., Barbulescu, A.: Combined Haar-Hilbert and Log-Gabor Based Iris Encoders. In: Balas, V.E., Fodor, J., Varkonyi-Koczy, A. (eds.) New Concepts and Applications in Soft Computing. SCI, vol. 417, pp. 1–26. Springer, Heidelberg (2012)

[2] Doddington, G., Liggett, W., Martin, A., Przybocki, M., Reynolds, D.: Sheep, Goats, Lambs and Wolves. In: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation. In: Int'l Conf. Spoken Language Processing (ICSLP), Sydney, vol. 4, pp. 1351–1354 (1998)

[3] Iris Challenge Evaluation, N.I.S.T. retired Mars (2011), `http://iris.nist.gov/ice/`

[4] Paone, J., Flynn, P.: On the consistency of the biometric menagerie for irises and iris matchers. In: Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), pp. 1–6 (2011)

[5] Popescu-Bodorin, N.: Exploring New Directions in Iris Recognition. In: 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. Conference Publishing Services – IEEE Computer Society, pp. 384–391 (2009)

[6] Popescu-Bodorin, N., Balas, V.E.: Comparing Haar-Hilbert and Log-Gabor based iris encoders on Bath Iris Image Database. In: Proc. 4th Int. Work. on Soft Computing Apps., pp. 191–196. IEEE Press (2010)

[7] Popescu-Bodorin, N.: Processing Toolbox for the University of Bath Iris Image Database, PT-UBIID-v.02 (2010), `http://fmi.spiruharet.ro/bodorin/pt-ubiid/`

[8] Popescu-Bodorin, N., Balas, V.E., Motoc, I.M.: 8-Valent Fuzzy Logic for Iris Recognition and Biometry. In: Proc. 5th IEEE Int. Symp. on Computational Intelligence and Intelligent Informatics, Floriana, Malta, September 15-17, pp. 149–154. IEEE Press (2011)

[9] Popescu-Bodorin, N., Balas, V.E., Motoc, I.M.: Iris Codes Classification Using Discriminant and Witness Directions. In: Proc. 5th IEEE Int. Symp. on Computational Intelligence and Intelligent Informatics, Floriana, Malta, September 15-17, pp. 143–148. IEEE Press (2011)

[10] Bath University Iris Image Database, `http://www.smartsensors.co.uk/informations/bath-iris-image-database/`

[11] Sugeno, M., Yasukawa, T.: A Fuzzy-Logic-Based Approach to Qualitative Modeling. IEEE Trans. on Fuzzy Systems 1(1), 7–31 (1993)

[12] Yager, N., Dunstone, T.: The biometric menagerie. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(2), 220–230 (2010)

[13] Zadeh, L.A.: A New Direction in AI - Toward a Computational Theory of Perceptions. AI Magazine 22(1), 73–84 (2001)

[14] Zadeh, L.A.: Toward extended fuzzy logic A first step. Fuzzy Sets and Systems 160, 3175–3181 (2009)

A Multi-algorithmic Colour Iris Recognition System

Petru Radu, Konstantinos Sirlantzis, Gareth Howells,
Sanaul Hoque, and Farzin Deravi

School of Engineering and Digital Arts,
University of Kent, Canterbury, U.K
{pr95,k.sirlantzis,w.g.j.howells,s.hoque,f.deravi}@kent.ac.uk

Abstract. The reported accuracies of iris recognition systems are generally higher on near infrared images than on colour RGB images. To increase a colour iris recognition system's performance, a possible solution is a multi-algorithmic approach with an appropriate fusion mechanism. In the present work, this approach is investigated by fusing three algorithms at the score level to enhance the performance of a colour iris recognition system. The contribution of this paper consists of proposing 2 novel feature extraction methods for colour iris images, one based on a 3-bit encoder of the 8 neighborhood and the other one based on gray level co-occurrence matrix. The third algorithm employed uses the classical Gabor filters and phase encoding for feature extraction. A weighted average is used as a matching score fusion. The efficiency of the proposed iris recognition system is demonstrated on UBIRISv1 dataset.

1 Introduction

Iris recognition has become an emerging research topic due to its rich texture with a high number of degrees of freedom [1], which has allowed researchers to develop a large variety of iris authentication algorithms. Although the performance of the iris recognition algorithms is high [2, 3], they require a large amount of constraints on the user due to the fact that near infrared illumination is necessary for good quality images and a reliable operation.

The majority of iris recognition systems published in the literature have only been benchmarked on near infrared images, leaving a question mark on whether these algorithms can perform on colour iris images with a comparable accuracy. The pioneering iris recognition system proposed in [1], which uses phase based coding and binary features extracted from near infrared images is deployed in most of the commercial and military iris recognition devices currently available. This fact led to the formation of large iris databases which contain images acquired under near infrared illumination.

The United States National Institute of Standards and Technology (NIST) [4] conducted a series of iris recognition competitions [5], where the submitted algorithms were tested on large scale databases containing near infrared iris images. These competitions allowed the creation of an ISO standard for near infrared iris images [6], which will promote the interoperability between various iris recognition acquisition devices and authentication algorithms. Generally the near infrared iris image data

V.E. Balas et al. (Eds.): Soft Computing Applications, AISC 195, pp. 45–56.
springerlink.com © Springer-Verlag Berlin Heidelberg 2013

standard specifies the thresholds for different iris image quality measures, which from a practical point of view are translated into how large the constraints on the user have to be.

For iris images acquired in visible spectrum there hasn't been created a standard yet, but over the past several years advances have been made in colour iris recognition. However, the accuracies obtained in visible spectrum are not yet comparable to those obtained under near infrared illumination [7]. The practicability of a colour iris recognition system is considerably increased when compared to a near infrared iris recognition system because the constraints on the user are significantly relaxed. One of the pioneers of iris recognition in visible spectrum is Hugo Proenca, who organized a colour iris recognition competition called Noisy Iris Challenge Evaluation (NICE). It took place in 2 parts: part1 assessed only the segmentation of a subset of UBIRISv2 [8] dataset and in part 2 the classification algorithms were assessed on the same images. Proenca et al analyzed the results of the second part of NICE competition in [7], where they reported that by employing a multi-algorithmic approach between the top 5 ranked algorithms, the accuracy of the system increases significantly.

In this paper we employ a multi-algorithmic approach to enhance a colour iris recognition systems' accuracy, motivated by the results reported in [7]. We use three iris recognition algorithms, two proposed by us in the present paper and one is the classical method proposed in [1].

The main novelty of the present work consists of 2 iris feature extraction methods. The first one uses the gray levels of the 8 neighborhood of a pixel from the iris texture and the second one uses the gray level co-occurrence matrices (GLCM) of the iris texture, calculated for 8 directions. Also, we propose a transformation of the match scores of the iris recognition systems which enhances the separation between authentic and impostor score distributions. Further, we analyze how the system performs when only a small number of pixels around the pupil are unwrapped compared to the case when a large number of pixels around the pupil are used to form the unwrapped image.

The remainder of the paper is organized as follows: in Section 2, the component algorithms of the multi-algorithm iris recognition systems are detailed. In Section 3 the separation enhancement method between authentic and impostor score distributions is presented. The experimental results are reported in Section 4 and conclusions are given in Section 5.

2 Proposed Multi-algorithmic Iris Recognition System

In Fig. 1 the block diagram of the proposed multi-algorithmic iris recognition system is presented. As may be observed, the system only uses the red channel to extract the information from the iris texture. The red channel has the closest wavelength to the near infrared domain and yields the best accuracy from the RGB colour space, as reported in [9].

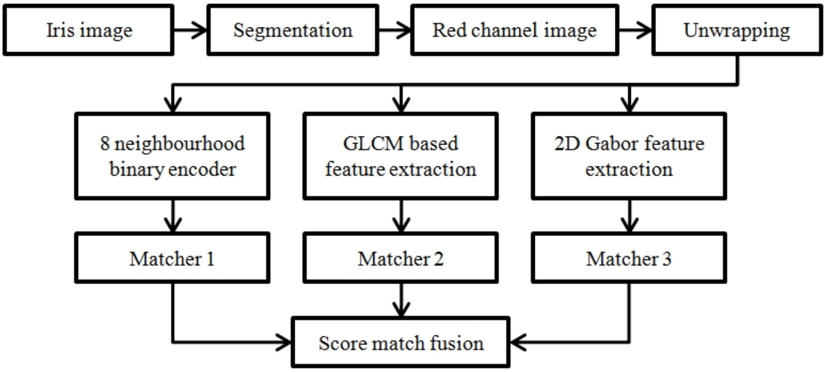


Fig. 1. Multi-algorithmic iris recognition system architecture

2.1 Preprocessing

An iris recognition system consists of five main stages: acquisition, segmentation, normalization, feature extraction and matching. For segmentation, the algorithm proposed in [10] was employed. In this work, we benchmarked the multi-algorithmic system on images from UBIRISv1 [11], Session 1 dataset. The segmentation accuracy on these images was approximately 95%. The remaining 5% were manually segmented, as they contain strong occlusions or other noise factors which make the segmentation difficult.

The unwrapping was done using the rubber sheet model proposed in [1]. To avoid including the eyelashes in the unwrapped image, the circle sector defined between -45^o and +45^o of vertical axis was not considered. The unwrapped image dimension initially is 120 by 50 pixels for the 8 neighborhood binary encoder and the classical phase based feature extraction and 360 by pixels 50 for the GLCM based system. Then, 100 pixels are considered around the pupil and the resulting unwrapped image dimension is 120 by 100 pixels and 360 by 100 pixels respectively.

As an efficient image enhancement was reported in [12] to be the second time consuming task from an iris recognition system after segmentation, our system does not employ any image enhancement techniques.

2.2 8-Neighborhood Binary Encoder

The pixel relationships are the basis of the least computationally demanding texture analysis techniques, as there is no filtering operation necessary. By using the 8 neighborhood of a pixel, we propose an iris feature extraction method which is computationally efficient and is therefore suitable to be implemented on mobile or embedded devices.

The working principle of the proposed feature extraction method is a simple, yet effective one: the 8 positions of the 8-neighborhood of a pixel may be encoded on 3 bits, as shown in Fig. 2. When the center pixel is immediately near its neighbors, we have an offset of 1, but the offset may be higher. Considering the values of the 8 neighbors of a pixel, the 3 bits corresponding to that pixel are the binary code corresponding to the position of the highest intensity value of the 8 neighbor pixels.

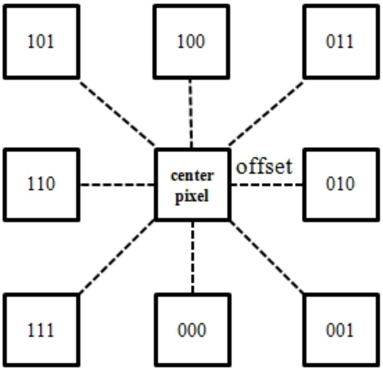


Fig. 2. Binary encoding of 8 neighborhood of a pixel

Additionally to encoding the position of the maximum pixel value of the 8-neighborhood, the value of the center pixel is compared to the mean of the 8-neighborhood. If the center pixel has a value smaller than the average, a logical 0 is concatenated to the 3 bits corresponding to the position of the maximum neighbor, otherwise a logical 1 is concatenated.

The 8-neighborhood does not have necessarily to be considered for every other pixel, it may be considered with a step for the horizontal scan and one for the vertical scan. In this way this feature extraction method becomes even more computationally efficient. We investigated how the performance varies with the step size via a direct search. As a matching algorithm, the Hamming distance is used [1].

The three parameters of this feature extraction method are the offset, the horizontal scanning step and the vertical scanning step. We found these parameters empirically, by taking the first 40 classes from UBIRISv1 [11] Session 1 dataset and computing the decidability index [1], which is a measure of the separation between the authentic and impostor score distributions. We found that the maximum decidability index was obtained for an offset of 7 pixels, a horizontal step of 1 pixel and a vertical step of 5 pixels. The resulting feature size is 3392 bits for the 120 by 50 pixels unwrapped image and 7632 bits for the 120 by 100 pixels image.

2.3 Co-occurrence Matrix Based Features

The co-occurrence matrix C for a 8-bit gray level image *I* is a 256 by 256 matrix which contains on row i and column j the counts of the number of pixels pairs with the intensity values i and j, which are separated by an offset and are at a relative inclination [13]:

$$C_{i,j=}\sum_{x=1}^{256}\sum_{y=1}^{256}\left(I_{x,y}=i\right)\wedge\left(I_{x',y'}=j\right) \tag{1}$$

where *x'* and *y'* are the offsets given by the distance *d* and inclination *θ*:

$$\begin{cases} x'=x+d\cos\theta \\ y'=y+d\sin\theta \end{cases} \tag{2}$$

The GLCM is symmetrical and if it has higher values around the main diagonal, it means that the image contrast is low. In the proposed feature extraction method, 8 co-occurrence non-symmetrical matrices were computed for an unwrapped iris image, corresponding to the directions given by the 8-neighborhood. A fused GLCM was obtained by averaging the 8 initial GLCM.

As the iris texture generally does not have high contrast, the higher values of the fused GLCM were concentrated around the main diagonal. The presence of noises such as eyelashes or reflections in the unwrapped iris image will be observed in high values in corner regions of the GLCM. From the original fused GLCM we only keep the part of the matrix with rows and columns indexes between 75 and 135. Therefore, the feature size will be $(135\text{-}75\text{+}1)^2$ = 3721 integer positive values. The indexes 75 and 135 were determined empirically with the criterion of maximizing the decidability index for 40 classes from UBIRISv1 dataset, Session 1, while keeping a manageable feature size of 3621 bytes. The larger the amount of data from the original GLCM is used, the higher the accuracy of the system will be, but the tradeoff is a higher computational demand and a larger template size.

From the selected 61 by 61 pixels matrix, we consider 20 vectors parallel and above the main diagonal and 20 vectors parallel and below the main diagonal. The main diagonal was not considered because it provides information about the pixels with the same intensity level. Let us denote the 20 vectors above the diagonal with v_1, ..., v_{20} and the 20 vectors below the main diagonal v_{-1}, ..., v_{-20}. In the matching phase, initially the Euclidian distances are computed between the corresponding vectors extracted from the probe and gallery images. As two initial scores, the means of the square roots of the Euclidean distances of the vectors above and below the main diagonal are computed using equations (3). The square root was used as a non-linear transformation to make the authentic and impostor score distributions narrower.

$$\begin{cases} \mathrm{M1}=\frac{1}{20}\sum_{i=1}^{20}\sqrt{\left\|v_i^{gallery},v_i^{probe}\right\|} \\ \mathrm{m2}=\frac{1}{20}\sum_{i=-20}^{-1}\sqrt{\left\|v_i^{gallery},v_i^{probe}\right\|} \end{cases} \tag{3}$$

The two means from equations (3) are used to compute the intermediate scores from equations (4). The hyperbolic tangent function is used to normalize the scores between 0 and 1. Hyperbolic tangent function takes values between 0 and 1 for positive arguments and maps all its arguments which are above 2.5 very close or equal to 1. The argument of hyperbolic tangent was used to bring the impostors scores above the value of 2.5 and the authentic scores as small as possible.

$$\begin{cases} \mathrm{dist1} = \tanh\left(\log\frac{20}{1+\mathrm{e}^{\mathrm{m1}}}\right)^6 \\ \mathrm{dist2} = \tanh\left(\log\frac{20}{1+\mathrm{e}^{\mathrm{m2}}}\right)^6 \end{cases} \tag{4}$$

The final co-occurrence matrix score (CMS) is obtained using equation (5) to fuse dist1 and dist2. dist1 and dist2 are below 1, and the product dist1*dist2 will be close to 0 for authentics and much larger for impostors. The absolute value of the base 2 logarithm of a number which is below 0.15 for example is above 2.5, while the absolute value of the base 2 logarithm of a number which is above 0.6 is below 0.6.

$$CMS = 1 - \tanh|\log_2(\mathrm{dist1} * \mathrm{dist2})| \tag{5}$$

2.4 Classical Phase-Based Feature Extraction

This method employs the classical 2D Gabor filters [1] to extract the information from the iris texture. The features are binary strings extracted using one set of parameters of the 2D Gabor filters. For each pixel of the unwrapped image, 2 bits of information are stored. We observed that if the 2 bits are extracted from every other pixel, the drop in performance is negligible.

The feature size is 3000 bits for the 120 by 50 pixels unwrapped iris image and 6000 bits for the 120 by 100 pixels image. For matching, the classical Hamming distance was used.

The issue of rotation is addressed by shifting one binary string 4 bits to the left and 4 bits to the right and the minimum Hamming distance out of the 9 computations is stored. The same method was applied to compensate for rotation of the features extracted using the 8-neighborhood binary encoder. The features extracted using GLCM are rotational invariant.

3 Enhancing the Authentic and Impostor Distributions

In any iris recognition system it is desirable to have a decidability index [1] between impostor and authentic score distributions as large as possible. A classical iris recognition system has most of the authentic scores concentrated in the range [0;0.2], while most of the impostor scores are above 0.4 [14-16].

In this paper we propose a transformation of the scores of an iris recognition system with the properties mentioned above by using equation (6). We will call the transformation (6) Kent Transform (KT). The reasoning of such a transform is the following: a non linear transformation that enhances the separation between 2 distributions which contain values between 0 and 1 is represented by $|\log_{10}(\mathrm{value}^2)|$. This expression will map values close to 0 above 1 and values above 0.32 below 1. When computing 1 – hyperbolic tangent of this expression, the values from the two original distributions will be more separated than they were initially.

$$\mathrm{KT}(\mathrm{score}) = 1 - \tanh\left|\log_{10}(\mathrm{score}^2)\right| \tag{6}$$

We will demonstrate the efficiency of the KT in the experimental results section, but let us first replace the scores of 0.2 and 0.4 in the above formula. Initially, the difference between the impostor score of 0.4 and authentic score of 0.2 is 0.2. After applying the KT we obtain KT(0.4) = 0.33 and KT(0.2) = 0.11 and the difference between the scores is now 0.22, larger by 10%.

When the impostor and authentic scores have values very close to the decision boundary, for example the impostor score is 0.35 and the authentic score is 0.3, then the difference of 0.05 between the 2 scores is increased by 18% to 0.059 when KT is applied. Therefore, the KT is a non-linear transformation which reduces the overlap between the authentic and impostor score distributions of an iris recognition system. KT may as well be applied to any type of biometric system which has the matching scores for authentics and impostors similar to those of a classical iris recognition system.

4 Experimental Results

The database used in our experiments was UBIRISv1 [11] Session 1. This session has 241 users enrolled with one eye. There are 5 colour RGB images for each user. The images were acquired in a semi-controlled environment, by reducing the noise factors, such as reflections, poor illumination or poor focus. The users were at a distance of 20 cm from the acquisition device. However, 10 images out of the total of 1205 are strongly or totally occluded and therefore no useful information can be extracted from them. We ran the experiments on all the images from the dataset, including the occluded ones.

The experimental setup consists of the classical one vs one score generation for all possible combinations between same class images and different class images. The fusion between the scores produced by the 3 algorithms was done by using weighted average. The weights for the 3 algorithms were determined using the first 40 classes via a direct search.

4.1 Using 50 Pixels around the Pupil

In Table 1, the decidability index is reported for all the images of UBIRISv1 Session 1 dataset and the 3 algorithms together with the means and standard deviations (in brackets) of the authentic and impostor distributions. There are 723000 impostor scores and 2410 authentic scores.

The KT is applied to the 8-neighborhood based algorithm and to the 2D Gabor filter based algorithm. The KT is not applied to the GLCM based algorithm because equation (5) which produces the matching scores of this algorithm is similar to KT.

Table 1. Decidability index and distribution means and standard deviations (in brackets) for the 3 algorithms

Algorithm	Authentic mean and std. deviation	Impostor mean and std. deviation	Decidability index
8-neighborhood	0.30 (0.038)	0.39 (0.017)	3.22
8-neighborhood with KT	0.22 (0.043)	0.33 (0.021)	3.31
GLCM	0.10 (0.227)	0.76 (0.336)	2.31
2D Gabor	0.20 (0.064)	0.40 (0.034)	3.92
2D Gabor with KT	0.12 (0.066)	0.34 (0.042)	4.03

In Table 2, the decidability index together with False Reject Rate (FRR) for 2 values of the False Acceptance Rate (FAR) and Equal Error Rate (EER) are reported for the last 201 classes left after the weights were determined using the first 40 classes. The weights obtained for the 2D Gabor with KT, 8-neighborhood with KT and GLCM algorithms are 0.61, 0.31 and 0.08 respectively.

Table 2. Performance measures for the 3 algorithms and fusion approach when 50 pixels around the pupil are used

Algorithm	Decidability index	FRR for FAR=0.01%	FRR for FAR=0.1%	EER
2D Gabor with KT	4.09	10.70 %	7.41 %	3.63 %
8-neighborhood with KT	3.33	22.34 %	11.74 %	3.51 %
GLCM	2.27	99.62 %	97.82 %	15.47 %
Fusion	4.38	11.39 %	7.91 %	3.33 %

From Table 2 may be observed that the GLCM based system performs poor compared to the other 2 algorithms, but when the scores of the 3 algorithms are fused, the decidability index of the best algorithm is increased by approximately 7% and the EER is decreased by approximately 8.2%. We have eliminated the GLCM based algorithm and implemented a weighted average between the other 2 systems, but the decidability index and the EER could only be improved by less than 1%.

4.2 Using 100 Pixels around the Pupil

In Table 3, the decidability index is reported for all the images of the 201 classes used for testing, together with the FRR for given thresholds of the FAR. In this case the optimum weights for 2D Gabor with KT, 8-neighborhood with KT and GLCM algorithms are 0.55, 0.34 and 0.11 respectively.

Table 3. Performance measures for the 3 algorithms and fusion approach when 100 pixels around the pupil are used

Algorithm	Decidability index	FRR for FAR=0.01%	FRR for FAR=0.1%	EER
2D Gabor with KT	4.93	4.42 %	3.38 %	2.45 %
8-neighborhood with KT	3.92	7.51 %	4.12 %	2.45 %
GLCM	3.19	99.58%	98.09 %	8.05 %
Fusion	5.17	10.7 %	4.67 %	2.25 %

The fusion of the 3 algorithms improves the decidability index by approximately 5% and the EER by approximately 8%. However, fusing of the 3 algorithms is not suitable if a low FAR is required for the operation of the iris recognition system.

In Fig. 3, the Receiving Operational Characteristic (ROC) curve is plotted for the 8-neighborhood and 2D Gabor algorithms, together with the ROC curve for the fusion of the 3 algorithms.

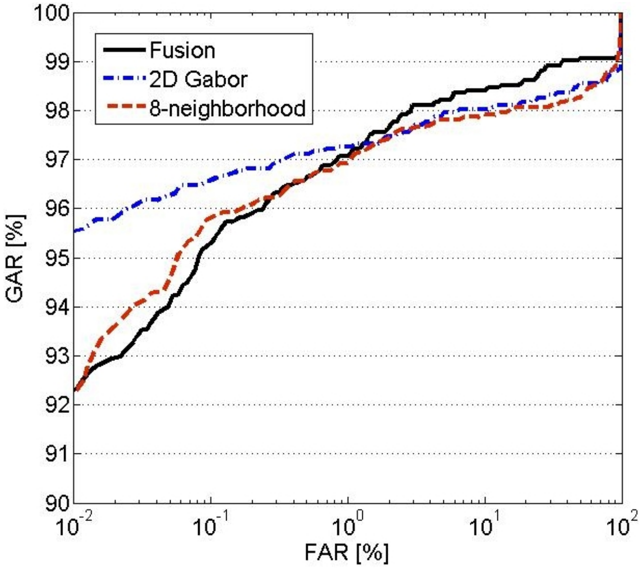


Fig. 3. ROC curve for 8-neighborhood, 2D Gabor and fusion of the 3 algorithms

To observe the improvement brought by using 100 pixels around the pupil over the case when only 50 pixels are used, we plotted in Fig. 4 the authentic and impostor distributions of the fused scores for the 3 algorithms produced on the 201 test classes. The EER when using 100 pixels around the pupil is improved by 32.42% compared to the case when only 50 pixels are used.