Advances in Intelligent Systems and Computing 297

Jeng-Shyang Pan · Vaclav Snasel
Emilio S. Corchado · Ajith Abraham
Shyue-Liang Wang *Editors*

Intelligent Data Analysis and Its Applications, Volume 1

Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13–15, 2014, Shenzhen, China

Springer

Advances in Intelligent Systems and Computing

Volume 297

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

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

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Advisory Board

Jeng-Shyang Pan · Vaclav Snasel
Emilio S. Corchado · Ajith Abraham
Shyue-Liang Wang
Editors

Intelligent Data Analysis and Its Applications, Volume 1

Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13–15, 2014, Shenzhen, China

Springer

Editors
Jeng-Shyang Pan
National Kaohsiung University of Applied Sciences
Kaohsiung
Taiwan

Vaclav Snasel
Faculty of Elec. Eng. & Comp. Sci.
Department of Computer Science
VSB-Technical University of Ostrava
Ostrava-Poruba
Czech Republic

Emilio S. Corchado
Facultad de Biología
Departamento de Informáca y Automática
University of Salamanca
Salamanca
Spain

Ajith Abraham
Scientific Network for Innovation and Research Excellence
Machine Intelligence Research Labs (MIR Labs)
Auburn Washington
USA

Shyue-Liang Wang
Department of Information Management
National University of Kaohsiung
Kaohsiung
Taiwan

ISSN 2194-5357 ISSN 2194-5365 (electronic)
ISBN 978-3-319-07775-8 ISBN 978-3-319-07776-5 (eBook)
DOI 10.1007/978-3-319-07776-5
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014940737

Printed on acid-free paper

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

Preface

This volume composes the proceedings of the First Euro-China Conference on Intelligent Data Analysis and Applications (ECC 2014), which was hosted by Shenzhen Graduate School of Harbin Institute of Technology and was held in Shenzhen City on June13–15, 2014. ECC 2014 was technically co-sponsored by Shenzhen Municipal People's Government, IEEE Signal Processing Society, Machine Intelligence Research Labs, VSB-Technical University of Ostrava (Czech Republic), National Kaohsiung University of Applied Sciences (Taiwan), and Secure E-commerce Transactions (Shenzhen) Engineering Laboratory of Shenzhen Institute of Standards and Technology. It aimed to bring together researchers, engineers, and policymakers to discuss the related techniques, to exchange research ideas, and to make friends.

113 papers were accepted for the final technical program. Four plenary talks were kindly offered by: Ljiljana Trajkovic (IEEE SMC president), C.L. Philip Chen (IEEE Fellow, University of Macau), Jhing-Fa Wang (Tajen University, Taiwan), and Ioannis Pitas (University of Thessaloniki, Greece).

We would like to thank the authors for their tremendous contributions. We would also express our sincere appreciation to the reviewers, Program Committee members and the Local Committee members for making this conference successful. Finally, we would like to express special thanks for the financial support from Shenzhen Municipal People's Government and Shenzhen Graduate School of Harbin Institute of Technology in making ECC 2014 possible.

June 2014

Jeng-Shyang Pan
Vaclav Snasel
Emilio S. Corchado
Ajith Abraham
Shyue-Liang Wang

Conference Organization

Honorary Chairs

Han-Chieh Chao	National Ilan University, Taiwan

Advisory Committee Chairs

Tzung-Pei Hong	National University of Kaohsiung, Taiwan
Bin-Yih Liao	National Kaohsiung University of Applied Sciences, Taiwan

Conference Chairs

Jeng-Shyang Pan	Harbin Institute of Technology Shenzhen Graduate School, China
Vaclav Snasel	VSB-Technical University of Ostrava, Czech Republic

Program Committee Chairs

Emilio S. Corchado	University of Salamanca, Spain
Ajith Abraham	Machine Intelligence Research Labs, USA
Shyue-Liang Wang	National University of Kaohsiung, Taiwan

Invited Session Chairs

Wu-Chih Hu	National Penghu University of Science and Technology, Taiwan
Kuo-Kun Tseng	Harbin Institute of Technology Shenzhen Graduate School, China

Electronic Media Chairs

Jiun-Huei Ho	Cheng Shiu University, Taiwan
Tsu-Yang Wu	Harbin Institute of Technology Shenzhen Graduate School, China

Local Organizing Chairs

Yanfeng Zhang	Harbin Institute of Technology Shenzhen Graduate School, China
Chun-Wei Lin	Harbin Institute of Technology Shenzhen Graduate School, China
Chien-Ming Chen	Harbin Institute of Technology Shenzhen Graduate School, China

Publication Chairs

Shu-Chuan Chu	Flinders University, Australia

Finance Chairs

Linlin Tang	Harbin Institute of Technology Shenzhen Graduate School, China

International Program Committee

Abdel hamid Bouchachia	University of Klagenfurt, Austria
Abd. Samad Hasan Basari	Universiti Teknikal Malaysia Melaka, Malaysia
Abraham Duarte	Universidad Rey Juan Carlos, Spain
Akira Asano	Kansai University, Japan
Alberto Alvarez	European Centre for Soft Computing, Spain
Alberto Cano	University of Cordoba, Spain
Alberto Fernandez	Universidad de Jaen, Spain
Alberto Bugarin	University of Santiago de Compostela, Spain
Alex James	Indian Institute of Information Technology and Management – Kerala, India
Alexandru Floares	Cancer Institute Cluj-Napoca, Romania
Alma Gomez	University of Vigo, Spain
Amelia Zafra Gomez	University of Cordoba, Spain
Amparo Fuster-Sabater	Institute of Applied Physics (C.S.I.C.), Spain
Ana Lorena	Federal University of ABC, Brazil
Anazida Zainal	Universiti Teknologi Malaysia, Malaysia
Andre Carvalho	University of Sao Paulo, Brazil

Andreas Koenig	Technische Universitat Kaiserslautern, Germany
Anna Bartkowiak	University of Wroclaw, Poland
Anna Fanelli	Universita di Bari, Italy
Antonio Peregrin	University of Huelva, Spain
Antonio J. Tallon-Ballesteros	University of Seville, Spain
Anusuriya Devaraju	Forschungszentrum Julich GmbH, Germany
Aranzazu Jurio	Universidad Publica de Navarra, Spain
Ashish Umre	University of Sussex, United Kingdom
Ashraf Saad	Armstrong Atlantic State University, United States
Ayeley Tchangani	University Toulouse III, France
Aymeric Histace	Universite Cergy-Pontoise, France
Azah Kamilah Muda	Universiti Teknikal Malaysia Melaka, Malaysia
Bartosz Krawczyk	Politechnika Wrocławska, Poland
Beatriz Pontes	University of Seville, Spain
Brijesh Verma	Central Queensland University, Australia
Carlos Barranco	Pablo de Olavide University, Spain
Carlos Cano	University of Granada, Spain
Carlos Fernandes	GeNeura Team, Spain
Carlos Garcia-Martinez	University of Cordoba, Spain
Carlos Lopezmolina	Universidad Publica de Navarra, Spain
Carlos Morell	Universidad Central Marta Abreu de Las Villas, Cuba
Cesar Hervas-Martinez	University of Cordoba, Spain
Chang-Shing Lee	National University of Tainan, Taiwan
Chao-Chun Chen	Southern Taiwan University, Taiwan
Chia-Feng Juang	National Chung-Hsing University, Taiwan
Chien-Ming Chen	Harbin Institute of Technology Shenzhen Graduate School, China
Chin-Chen Chang	Feng Chia University, Taiwan
Chris Cornelis	Ghent University, Belgium
Chuan-Kang Ting	National Chung Cheng University, Taiwan
Chu-Hsing Lin	Tunghai University, Taiwan
Chun-Wei Lin	Harbin Institute of Technology Shenzhen Graduate School, China
Coral del Val	University of Granada, Spain
Crina Grosan	Norwegian University of Science and Technology, Norway
Cristina Rubio-Escudero	University of Sevilla, Spain

Cristobal Romero	University of Cordoba, Spain
Cristobal J. Carmona	University of Jaen, Spain
Dalia Kriksciuniene	Vilnius University, Lithuania
David Becerra-Alonso	ETEA-INSA, Spain
Detlef Seese	Karlsruhe Institut of Technology (KIT), Germany
Edurne Barrenechea	Universidad Publica de Navarra, Spain
Eiji Uchino	Yamaguchi University, Japan
Eliska Ochodkova	VŠBTechnical University of Ostrava, Czech Republic
Elizabeth Goldbarg	Federal University of Rio Grande do Norte, Brazil
Emaliana Kasmuri	Universiti Teknikal Malaysia Melaka, Malaysia
Enrique Herrera-Viedma	University of Granada, Spain
Enrique Yeguas	University of Cordoba, Spain
Eulalia Szmidt	Systems Research Institute Polish Academy of Sciences, Poland
Eva Gibaja	University of Cordoba, Spain
Federico Divina	Pablo de Olavide University, Spain
Fernando Bobillo	University of Zaragoza, Spain
Fernando Delaprieta	University of Salamanca, Spain
Fernando Gomide	University of Campinas, Brazil
Fernando Jimenez	University of Murcia, Spain
Francesc J. Ferri	Universitat de Valencia, Spain
Francesco Marcelloni	University of Pisa, Italy
Francisco Fernandez Navarro	University of Cordoba, Spain
Francisco Herrera	University of Granada, Spain
Francisco Martinez-Alvarez	Pablo de Olavide University, Spain
Francisco Martinez-Estudillo	University Loyola Andalucia, Spain
Frank Klawonn	University of Applied Sciences Baunschweig, Germany
Gabriel Luque	University of Malaga, Spain
Gede Pramudya	Universiti Teknikal Malaysia Melaka, Malaysia
Giacomo Fiumara	University of Messina, Italy
Giovanna Castellano	Universita di Bari, Italy
Giovanni Acampora	University of Salerno, Italy
Girijesh Prasad	University of Ulster, United Kingdom
Gladys Castillo	University of Aveiro, Portugal
Gloria Bordogna	CNR IDPA, Italy
Gregg Vesonder	AT&T Labs Research, United States
Huiyu Zhou	Queen's University Belfast, United Kingdom
Ilkka Havukkala	Intellectual Property Office of New Zealand, New Zealand

Imre Lendak	University of Novi Sad, Serbia
Intan Ermahani A. Jalil	Universiti Teknikal Malaysia Melaka, Malaysia
Isabel Nunes	UNL/FCT, Portugal
Isabel S. Jesus	Instituto Superior de Engenharia do Porto, Portugal
Ivan Garcia-Magarino	Universidad a Distancia de Madrid, Spain
Jae Oh	Syracuse University, United States
Jan Martinovic	VŠB Technical University of Ostrava, Czech Republic
Jan Plato	VŠB Technical University of Ostrava, Czech Republic
Javier Perez	University of Salamanca, Spain
Javier Sedano	Technological Institute of Castilla y Leon, Spain
Jesus Alcala-Fdez	University of Granada, Spain
Jesus Serrano-Guerrero	University of Castilla-La Mancha, Spain
Jitender S. Deogun	University of Nebraska, United States
Joaquin Lopez Fernandez	University of Vigo, Spain
Jorge Nunez Mc Leod	Institute of C.E.D.I.A.C., Argentina
Jose Luis Perez de la Cruz	University of Malaga, Spain
Jose M. Merigo	University of Barcelona, Spain
Jose-Maria Luna	University of Cordoba, Spain
Jose Pena	Universidad Politecnica de Madrid, Spain
Jose Raul Romero	University of Cordoba, Spain
Jose Tenreiro Machado	Instituto Superior de Engenharia do Porto, Portugal
Jose Valente De Oliveira	Universidade do Algarve, Portugal
Jose Villar	Oviedo University, Spain
Juan Botia	Universidad de Murcia, Spain
Juan Gomez-Romero	Universidad Carlos III de Madrid, Spain
Juan Vidal	Universidade de Santiago de Compostela, Spain
Juan J. Flores	Universidad Michoacana de San Nicolas de Hidalgo, Mexico
Juan-Luis Olmo	University of Cordoba, Spain
Julio Cesar Nievola	Pontificia Universidade Catolica do Parana, Brazil
Jun Zhang	Waseda University, Japan
Jyh-Horng Chou	National Kaohsiung First Univ. of Science and Technology, Taiwan
Kang Tai	Nanyang Technological University, Singapore
Kaori Yoshida	Kyushu Institute of Technology, Japan
Kazumi Nakamatsu	University of Hyogo, Japan
Kelvin Lau	University of York, United Kingdom
Kubilay Ecerkale	Turkish Air Force Academy, Turkey

Kumudha Raimond	Karunya University, India
Kun Ma	University of Jinan, China
Leandro Coelho	Pontificia Universidade Catolica do Parana, Brazil
Lee Chang-Yong	Kongju National University, Korea
Leida Li	University of Mining and Technology, China
Leon Wang	National University of Kaohsiung, Taiwan
Liang Zhao	University of Sao Paulo, Brazil
Liliana Ironi	IMATI-CNR, Italy
Luciano Stefanini	University of Urbino "Carlo Bo", Italy
Ludwig Simone	North Dakota State University, United States
Luigi Troiano	University of Sannio, Italy
Luka Eciolaza	European Centre for Soft Computing, Spain
Macarena Espinilla Estevez	Universidad de Jaen, Spain
Manuel Grana	University of Basque Country, Spain
Manuel Lama	Universidade de Santiago de Compostela, Spain
Manuel Mucientes	University of Santiago de Compostela, Spain
Marco Cococcioni	University of Pisa, Italy
Maria Nicoletti	Federal University of Sao Carlos, Brazil
Maria Torsello	Universita di Bari, Italy
Maria Jose Del Jesus	Universidad de Jaen, Spain
Mariantonietta Noemi La Polla	IIT-CNR, Italy
Maria Teresa Lamata	University of Granada, Spain
Mario Giovanni C.A. Cimino	University of Pisa, Italy
Mario Koeppen	Kyushu Institute of Technology, Japan
Martine De Cock	Ghent University, Belgium
Michael Blumenstein	Griffith University, Australia
Michal Kratky	VŠB Technical University of Ostrava, Czech Republic
Michal Wozniak	Wroclaw University of Technology, Poland
Michela Antonelli	University of Pisa, Italy
Mikel Galar	Universidad Publica de Navarra, Spain
Milos Kudelka	VŠB Technical University of Ostrava, Czech Republic
Min Wu	Oracle, United States
Noor Azilah Muda	Universiti Teknikal Malaysia Melaka, Malaysia
Norberto Diaz-Diaz	Pablo de Olavide University, Spain
Norton Gonzalez	University of Fortaleza, Brazil
Nurulakmar Emran	Universiti Teknikal Malaysia Melaka, Malaysia
Olgierd Unold	Wroclaw University of Technology, Poland
Oscar Castillo	Tijuana Institute of Technology, Mexico
Ovidio Salvetti	ISTI-CNR, Italy
Ozgur Koray Sahingoz	Turkish Air Force Academy, Turkey
Pablo Villacorta	University of Granada, Spain

Patrick Siarry	Universit de Paris, France
Paulo Carrasco	Universidade do Algarve, Portugal
Paulo Moura Oliveira	University of Tras-os-Montes and Alto Douro, Portugal
Pedro Gonzalez	University of Jaen, Spain
Philip Samuel	Cochin University of Science and Technology, India
Pierre-Francois Marteau	Universite de Bretagne Sud, France
Pietro Ducange	University of Pisa, Italy
Punam Bedi	University of Delhi, India
Qieshi Zhang	Waseda University, Japan
Qinghan Xiao	Defence R&D Canada, Canada
Radu-Codrut David	Politehnica University of Timisoara, Romania
Rafael Bello	Universidad Central de Las Villas, Cuba
Ramin Halavati	Sharif University of Technology, Iran
Ramiro Barbosa	Instituto Superior de Engenharia do Porto, Portugal
Ramon Sagarna	University of Birmingham, United Kingdom
Richard Jensen	Aberystwyth University, United Kingdom
Robert Berwick	Massachusetts Institute of Technology, United States
Roberto Armenise	Poste Italiane, Italy
Robiah Yusof	Universiti Teknikal Malaysia Melaka, Malaysia
Roman Neruda	Institute of Computer Science, Czech Republic
S. Ramakrishnan	Dr. Mahalingam College of Engineering and Technology, India
Sabrina Ahmad	Universiti Teknikal Malaysia Melaka, Malaysia
Sadaaki Miyamoto	University of Tsukuba, Japan
Santi Llobet	Universitat Oberta de Catalunya, Spain
Satrya Fajri Pratama	Universiti Teknikal Malaysia Melaka, Malaysia
Saurav Karmakar	Georgia State University, United States
Sazalinsyah Razali	Universiti Teknikal Malaysia Melaka, Malaysia
Sebastian Ventura	University of Cordoba, Spain
Selva Rivera	Institute of C.E.D.I.A.C., Argentina
Shang-Ming Zhou	University of Wales Swansea, United Kingdom
Shyue-Liang Wang	National University of Kaohsiung, Taiwan
Siby Abraham	University of Mumbai, India
Silvia Poles	EnginSoft, Italy
Silvio Bortoleto	Federal University of Rio de Janeiro, Brazil
Siti Rahayu Selamat	Universiti Teknikal Malaysia Melaka, Malaysia
Steven Guan	Xi'an Jiaotong-Liverpool University, China
Sung-Bae Cho	Yonsei University, Korea
Swati V. Chande	International School of Informatics and Management, India

Sylvain Piechowiak	Universite de Valenciennes et du Hainaut-Cambresis, France
Takashi Hasuike	Osaka University, Japan
Teresa Ludermir	Federal University of Pernambuco, Brazil
Thomas Hanne	University of Applied Sciences Northwestern Switzerland, Switzerland
Tsu-Yang Wu	Harbin Institute of Technology Shenzhen Graduate School, China
Tzung-Pei Hong	National University of Kaohsiung, Taiwan
Vaclav Snasel	VŠB Technical University of Ostrava, Czech Republic
Valentina Colla	Scuola Superiore Sant'Anna, Italy
Victor Hugo Menendez Dominguez	Universidad Autonoma de Yucatan, Mexico
Vincenzo Loia	University of Salerno, Italy
Vincenzo Piuri	University of Milan, Italy
Virgilijus Sakalauskas	Vilnius University, Lithuania
Vivek Deshpande	MIT College of Engineering, India
Vladimir Filipovic	University of Belgrade, Serbia
Wei Wei	Xi'an University of Technology, China
Wei-Chiang Hong	Oriental Institute of Technology, Taiwan
Wen-Yang Lin	National University of Kaohsiung, Taiwan
Wilfried Elmenreich	University of Klagenfurt, Austria
Yasuo Kudo	Muroran Institute of Technology, Japan
Ying-Ping Chen	National Chiao Tung University, Taiwan
Yun-Huoy Choo	Universiti Teknikal Malaysia Melaka, Malaysia
Yunyi Yan	Xidian University, China
Yusuke Nojima	Osaka Prefecture University, Japan

Contents

Part I
Data Security and Its Applications

A Robust Audio Zero-Watermarking Algorithm Based on Wavelet Packet Analysis

Xueying Zhang, Wei Zhang, Fenglian Li, and Guangyu Liu

College of Information Engineering, Taiyuan University of Technology
Taiyuan, China
tyzhangxy@163.com

Abstract. This paper proposed a new robust audio zero-watermarking algorithm which can be used to authenticate the copyright of digital audio. This algorithm has the following features: (1) it extracts the low frequency components of original audio to construct zero-watermarking by using the wavelet packet analysis method, ensures the imperceptibility of watermarking algorithm; (2) it uses cubic spline interpolation and multilevel scrambling technology to construct a meaningful zero-watermarking with a binary text image; it improves its safety and the robustness toward the attacks. Meanwhile, it is fairly straightforward to finish the authentication. The experimental result shows that this algorithm has strong robustness against typical common attacks and hostile attacks.

Keywords: zero-watermark, robust watermarking, copyright authentication, cubic spline interpolation, wavelet packet analysis.

1 Introduction

As a popular research, digital audio watermarking technology[1],[2]has been widely used in many fields, such as copyright authentication[3], content authenticity, secure communication. At present, it is mainly depending on robust watermarking to realize the digital audio copyright authentication. According to the difference of forming mechanism, the robust watermarking can be divided into two types: embedded watermarking[4] and zero-watermarking[5]. Zero-watermarking is a typical digital watermarking system. It solved the conflict between the imperceptibility and robustness of digital watermarking. Meanwhile, it reduced the security breach which exists in reversible watermarking system[6].

This paper proposed a new robust audio zero-watermarking algorithm which has strong robustness toward typical common attacks and hostile attacks. In this algorithm, a binary text image is used as watermarking. The algorithm extracts the low frequency components of host audio to construct zero-watermarking. First of all, the binary text image is scrambled and reduced dimensions to a one-dimensional sequence as watermarking information. This step is to eliminate the correlation of the watermarking images, improves its safety and robustness. Then, it extracts low frequency coefficients of the host audio signals after three-layer wavelet packet decomposition to construct a binary sequence by cubic

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_1,

spline interpolation. Combining this binary sequence and watermarking information by using an XOR operator, the zero-watermarking is constructed. In the watermarking extraction process, the binary image is reconstructed by using an XOR operator with zero-watermarking and the binary sequence which uses the same method as constructing process to get. At last, copyright authentication is finished by the similarity testing. Throughout the process, the algorithm did not modify the original audio data. That ensures its imperceptibility and achieves blind detection.

2 Theoreticle Basis

2.1 Wavelet Packet Analysis

Wavelet packet transform is a further development based on wavelet transform [7,8,9]. It has been widely used in signal analysis. Fig. 1 is a schematic diagram of three-layer wavelet packet decomposition, where X is the signal, A represents low frequency components, D represents high frequency components, the serial number in the end represents the number of layers of wavelet decomposition.

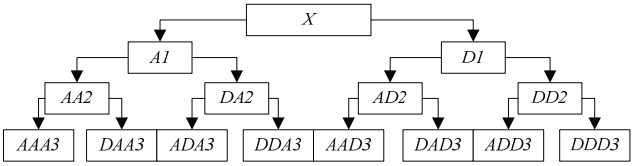


Fig. 1. Schematic diagram of three-layer wavelet packet decomposition of signal X

Low-frequency components of wavelet have strong robustness against various attacks. Therefore, the algorithm uses the first M low-frequency components after wavelet packet decomposition to construct zero-watermarking.

2.2 Cubic Spline Interpolation

Suppose $a < x_0 < x_1 < \cdots < x_n < b$ exists on $[a, b]$.If the function meets the demands:

(1) $s(x) \in C^2[a, b]$;

(2)$s(x)$ is a cubic polynomial in each little section $[x_i, x_i + 1](i = 0, 1, \ldots, n - 1)$,$s(x)$ is called "Cubic Spline Function" on nodes $x_0, x_1, \cdots, x_n$; And if the function meets the interpolation demand:

(3) $s(x) = f_i, i = 0, 1, \ldots, n$; $s(x)$ is called "Cubic Spline Interpolation Function" on the interval$[a, b]$.

Section cubic spline interpolation is a smooth curve that goes through the given points.It is concluded from the above three conditions: It is secondorder

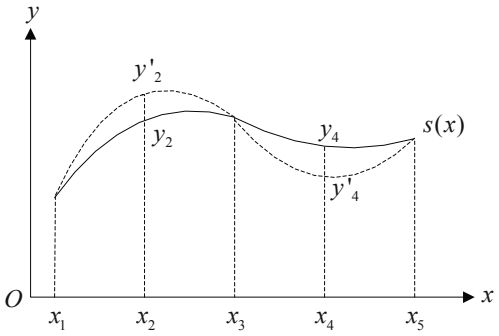


Fig. 2. Cubic spline interpolation schematic

continuous on the interval. It is a cubic polynomial in each little section and goes through the given points. Cubic spline interpolation can be readily finished by the function "interp1(x,y,x_i,'spline')" in Matlab.

As shown in Fig. 2, according to the given points (x_1, x_3, x_5) on the function $s(x)$, an interpolation function can be obtained by using cubic spline interpolation. The dotted line is drawn to show the interpolation function. Two values y_2', y_4' can be obtained by the interpolation points x_2, x_4 . The purpose of getting interpolation is to construct a binary sequence according to comparing the interpolation y_2', y_4' and the values of the original curve.

3 Algorithm Description

3.1 Pretreatment of the Watermark Image

Watermark image is a meaningful binary image $V(N*N)$,$V = \{v(i,j), 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant N\}, V(i,j) \in \{0,1\}$ represents pixel grayscale value of the watermark image matrix(i-th row, j-th column).

Step 1 Matrix V is processed by Arnold scrambling operation.

Step 2 After scrambling operation, watermark image is to be reconstructed into a binary sequence$p(i), i = 1, 2, \cdots N*N$.

3.2 Zero-Watermarking Construction

Fig. 3 is a flowchart of the process of watermarking construction.The original audio processing on the dotted line, under the dotted line is the watermark image preprocessing.Concrete steps are as follows:

Step 1 Decomposes original audio signal $x(n)$ in three-layer wavelet packet[10] and selects 'db4' as the wavelet function.Let $K_2 = N*N$, and extracts the $2K_2$+1 -th wavelet low frequency coefficients denoted as $c(i), i = 1, 2, \cdots, 2K_2$+1 Then mark the odd item $c_{ood}(i), i = 1, 2, \cdots, K_2$+1 and the even item$c_{even}(i), i = 1, 2, \cdots, K_2$;

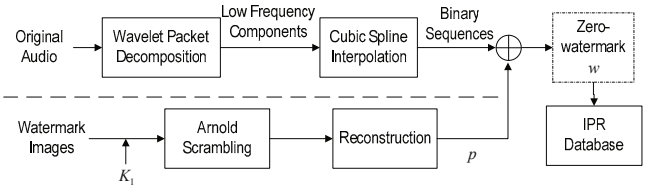


Fig. 3. The flow chart of watermarking construction

Step 2 The one-dimensional array $c_{ood}(i), i = 1, 2, \cdots, K_2+1$ can be construct into another one-dimensional array measuring $2K_2 + 1$ in length. To extract its even item and mark it $a(i), i = 1, 2, \cdots, K_2$;

Step 3 According to the relationship between$a(i)$and $c_{even}(i)$,to form the binary sequence$u(i)$:

$$u(i) = \begin{cases} 0, a(i) \geq c_{even}(i) \\ 1, a(i) < c_{even}(i) \end{cases}, i = 1, 2, \cdots, K_2 \tag{1}$$

Step 4 To do XOR operator with $u(i)$ and $p(i)$, then form the zero-watermarking $w(i), i = 1, 2, \cdots k_2$

$$w(i) = p(i) \bigoplus u(i), i = 1, 2, \cdots k_2. \tag{2}$$

At last, register the IPR information database with the current zero-watermarking, and send and as keys.

3.3 Zero-Watermarking Extraction

Fig. 4 is a flowchart of the process of watermarking extraction.Audio processing is tested on the dotted line, Under the dotted line is watermark image reconstruction and detection process.Concrete steps are as follows:

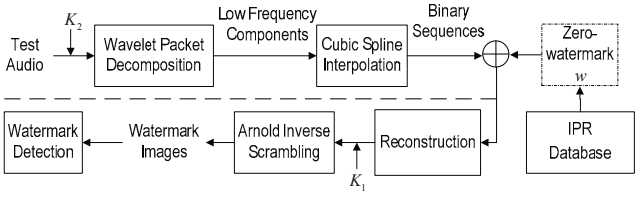


Fig. 4. The flow chart of watermarking extraction

Step 1 Suppose $x'(n)$ is the audio to be checked that attacked in the transmission process. Enter the Key K_2.and decomposes signal $x'(n)$ in three-layer wavelet packet and selects 'db4' as the wavelet function. Let $K_2 = N * N$, and extracts the $2K_2 + 1$ -th wavelet low frequency coefficients denoted as

$c'(i), i = 1, 2, \cdots, 2K_2 + 1$ Then mark the odd item $c'_{ood}(i), i = 1, 2, \cdots, K_2 + 1$ and the even item$c'_{even}(i), i = 1, 2, \cdots, K_2$;

Step 2 The one-dimensional array $c'_{ood}(i), i = 1, 2, \cdots, K_2+1$, can be construct into another one-dimensional array measuring $2K_2 + 1$ in length. To extract its even item and mark it $a'(i), i = 1, 2, \cdots, K_2$;

Step 3 According to the relationship between$a'(i)$and $c'_{even}(i)$, to form the binary sequence $u'(i)$:

$$u'(i) = \begin{cases} 0, a'(i) \geq c_e ven'(i) \\ 1, a'(i) < c_e ven'(i) \end{cases}, i = 1, 2, \cdots, K_2 \tag{3}$$

Step 4 To do XOR operator with $u'(i)$ and the zero-watermarking$w(i)$, then form the zero-watermarking $p'(i), i = 1, 2, \cdots k_2$

$$p'(i) = w(i) \bigoplus u'(i), i = 1, 2, \cdots k_2. \tag{4}$$

Step 5 Insert the Key K_1 and reform $p'(i)$ as a binary matrix, and do Arnold inverse scrambling with it. The matrix $V' = \{v'(i, j, 1 \leq i, j \leq N)\}$ (size N*N) is the watermarking image extracted.

4 Experimental Results and Performance Analysis

Experiment selects Matlab7.8 as simulation software, a digital audio signal (44.1kHz,16bits) as original audio and a binary image(size 6464) as watermarking image. Take $K_1 = 10$,as shown below:

Fig. 5. Watermarking image

Experiment compares the original watermarking image with the extracted watermarking image by calculating the Normalized Correlation Coefficient (NC). The formula as follows:

$$NC(W, W') = \frac{\sum\limits_i w(i)w'(i)}{\sqrt{\sum\limits_i w^2(i)}\sqrt{\sum\limits_i w'^2(i)}} \tag{5}$$

Where W is original watermarking,W' is the extracted watermarking.

4.1 Common Attacks Testing

To do common attacks with the original audio: 1) Adding white Gaussian noise (mean 0, variance 0.01 or 0.02); 2) Filtering with 6-tap Butterworth filter (cutoff frequency 15 kHz); 3) Re-quantification (32 bits or 8 bits); 4) MP3 compression (128 Kbps or 64 Kbps). The experimental results (NC and extracted watermarking image)algorithm in literature[11]results are shown in Table 1.

Table 1. Common attack experimental results

	Algorithm in literature[12]	This algorithm	
	NC	NC	Extracted watermark
Without attack	1	1	
Add noise(0.01)	0.9676	0.9904	
Add noise(0.02)	0.8781	0.9840	
Filtering (15kHZ)	0.8955	0.9849	
Re-quantification 16816bits	0.9978	0.991	
Re-quantification 163216bits	1	0.9991	
MP3 compression 128kbps	0.9944	0.9935	
MP3 compression 64kbps	0.9242	0.9818	

Experimental data show that the algorithm for a typical common attack are reflected robustness. In addition, a number of other common attacks(such as amplitude zoom in, zoom, etc.) anti-attack performance experiments, the results also improved. From the point of view watermarked image: After the audio

being common attack, the extracted watermark image is still clearly visible and uniform distribution of pixels,missing piece of the image did not occur,does not affect the identification of audio watermarking.Proved relatively stable algorithm for common attack, enabling audio copyright authentication. Further,the results from the comparison with the literature[12]can be seen, for most conventional attack, the present algorithm has increased the robustness, particularly because of the low complexity of the algorithm,the program running time is also very improvements.

4.2 Hostile Attacks Testing

Original audio is attacked by the two most typical hostile attacks[12] (cutting and replacement attack). Then the experiment tests the robustness of the algorithm against hostile attacks,according to similarity(NC)and the extracted watermark image.

(1) Cutting Attack

Cut 1/16 length (0-10000 sampling points) of the original audio, the test audio is generated. The extracted watermarking image is shown in Fig. 6 (NC=0.8858).

Fig. 6. Experimental results of cutting attack

(2) Substitution Attack Replace 1/16 length (0-10000 sampling points) of the original audio by a audio segment of the same sampling rate and quantization precision, the test audio is generated. The extracted watermarking image is shown in Fig. 7 (NC=0.8951).

Fig. 7. Experimental results of substitution attack

The experimental results show that when the original audio is processed by hostile attacks, there is a wide gap between the extracted watermarking image and the original.But the image is not one-piece missing. Watermarking identification will not be affected. This proves that algorithm has strong robustness against typical hostile attacks, and can achieve the certification of the audio copyright.

5 Conclusion

This paper proposed a new robust audio zero-watermarking algorithm which can be used to authenticate the copyright of digital audio.It extracts the low frequency components of original audio to construct zero-watermarking by wavelet packet decomposition and cubic spline interpolation. Combining with a binary text images, a meaningful zero-watermarking is constructed and extracted. That completes copyright authentication of the original audio copyright. The zero-watermarking detection process is intuitive, accurate, and with good security. The experimental result shows that this algorithm has strong robustness against typical common attacks and hostile attacks. The algorithm is simple, easy to implement, so it has a high application value.

Acknowledgments. This research supported by the National Nature Science Foundation of China (No.61072087,No.61371193).

References

1. Wu, S., Huang, J., Huang, D.: Efficiently Self-Synchronized Audio Watermarking for Assured Audio Data Transmission. IEEE Transactions on Broadcasting 51(1), 69–76 (2005)
2. Nutzinger, M.: Real-time Attacks on Audio Steganography. Journal of Information Hiding and Multimedia Signal Processing 3(1), 47–65 (2012)
3. Lahouari, G., Ahmed, B., Mohammad, K.I.: Digital Image Watermarking using Balanced Multiwavelets. IEEE Transactions on Signal Processing 54(4), 1519–1536 (2006)
4. Yang, Y., Niu, X.: Multimedia Information Pretend Summarization. Journal of China Institute of Communication 23(5), 32–38 (2002)
5. Wen, Q., Sun, T., Wang, S.: Concept and Application of Zero-Watermark. Acta Electronica Sinica 31(2), 214–216 (2003)
6. Weng, S., Chu, S., Cai, N., Zhan, R.: Invariability of Mean Value Based Reversible Watermarking. Journal of Information Hiding and Multimedia Signal Processing 4(2), 90–98 (2013)
7. Paquet, A., Ward, R., Pitas, I.: Wavelet Packets-based Digital Watermarking for Image Verification and Authentication. Signal Processing 83(10), 2117–2132 (2003)
8. Gao, Z., Hai, X.: Matlab Wavelet Analysis and Application. National Defense Industry Press, Beijing (2007)
9. Zhang, D.: Matlab Wavelet Analysis. China Machine Press, Beijing (2009)
10. Zhong, X., Tang, X.: A DWT Domain Zero-watermark Algorithm Based on Audio's Character. Journal of Hangzhou Dianzi University 27(2), 33–36 (2007)
11. Yang, J., Ma, Z., Zhang, X.: Digital Audio Dual Watermarking Scheme Based on Wavelet Packet Analysis. Journal of Computer Applications 30(5), 1218–1220 (2010)
12. Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., Fates, N., Ferri, L.C.: Stirmark Benchmark:Audio Watermarking Attacks. In: Int. Conference on Information Technology: Coding and Computing, pp. 49–54. IEEE Press (2001)

Information Security Management for Higher Education Institutions

Simon K.S. Cheung

The Open University of Hong Kong
Good Shepherd Street, Homantin, Kowloon, Hong Kong
kscheung@ouhk.edu.hk

Abstract. Information security aims at protecting the information assets of an organization from any unauthorized access, disclosure and destruction. For information security to be effectively enforced, good management practices comprising policies and controls should be established. This paper investigates the information security management for higher education institutions. Based on the conventional CIA (confidentiality, integrity and availability) triad of information, eight control areas on information security are identified. They include information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. A governance framework is important for establishing the policies and executing the controls of information security. It is necessary to maintain a right balance between the technical feasibility and the flexibility and efficiency in administration.

Keywords: information security management, information security policies, information security controls.

1 Introduction

Nowadays, computer systems are highly connected through the internal networks (Intranet) and external networks (Internet) to facilitate accesses to information. This however creates the issue of information security – the protection of information assets from any unauthorized access, disclosure, modification and destruction, in order to ensure its confidentiality, integrity and availability [1, 2]. Information security is conventionally defined as the assurance of the CIA triad of information (confidentiality, integrity and availability) [1, 3], and its extension (authenticity, non-repudiation and accountability) [4, 5].

With the recent advances of communication and mobile technologies, Internet and Intranet accesses to information from client-end devices (especially mobile devices) via wired or wireless networks are very popular, such as on e-mail communication, and e-commerce and e-government services. This inevitably adds more technical complexity in ensuring that the information assets of an organization can be well protected [6, 7, 8], and therefore, some intelligent and sophisticated access protocols are developed [9, 10, 11, 12].

J.–S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_2,

Although there are many technical solutions to help protect the information assets of an organization, the risk of information leakage, modification or destruction cannot be completely eliminated. As this may incur great losses, information security is essential to any organization which counts information assets as critical to their business operation. This is especially important for government and public bodies because the adverse impacts are much greater than that of other organizations [7, 8, 13]. Similarly, for a higher education institution where a large amount of student information is hosted student administrative systems, learning management systems and platforms [14, 15, 16], any information leakage or loss would have large impacts. Information security compliance and awareness have become emerging issues in higher education institutions [17, 18, 19].

In many countries, there are laws, regulations and policies, governing information security, such as the Data Protection Act and Computer Misuse Act in the United Kingdom and the Federal Information Security Management Act in the United States. In Hong Kong, a set of baseline policies have been established for enforcing information security in government offices [20]. Besides, many national and international standards for information security management have been established. Among these standards, the ISO 27001 Information Security Management System is the most widely adopted one [21].

This paper investigates the information security management for higher education institutions. Eight control areas for providing the rules of governance and control of information security are identified, and a framework for governance and control is discussed. These control areas include information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. The rest of this paper is organized as follows. Section 2 states the principles of information security. Section 3 elaborates the eight key control areas on information security for higher education institutions. Section 4 then discusses the governance of information security. Section 5 briefly concludes this paper.

2 Principles of Information Security

Conventionally, the CIA triad (confidentiality, integrity and availability) forms the principles of information security [1, 3]. In the literature, it has been argued that the CIA triad should be extended with three more principles, namely, authenticity, non-repudiation and accountability [4, 5]. Figure 1 shows these principles.

Confidentiality is the ability to protect information from unauthorized accesses. A typical example of unauthorized accesses is the use of another person's account and password to access an online banking system, which he or she does not possess the necessary access rights. Integrity is the ability to protect information from undetected modification or deletion. For example, in an e-mail communication, some information in the e-mail message is intercepted, modified or omitted during the message sending process. Availability is the ability to protect information from attacks denying or inconveniencing authorized accesses. It ensures that information is readily accessible to the authorized users at all times.

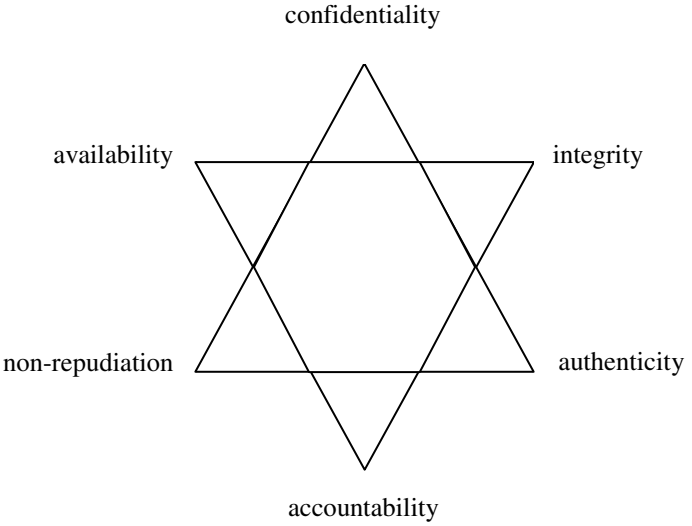


Fig. 1. Six principles of information security

Authenticity is the ability to ensure that transactions or communications of information are genuine. In order to validate accesses to information, authentication system with proper access control and password protection is adopted. Non-repudiation refers to one's intention to fulfill the accepted obligations. For example, in the transmission of information, the sender cannot deny having sent the information and the receiver cannot deny having received the information. Digital signature is often used to ensure non-repudiation. Accountability is the ability to track user identity and actions applied to the information. Accountability is a useful element for executing non-repudiation that proves the performance of an action, for example, sending or receiving information, and when and where the action was performed.

3 Information Security Controls

It is necessary for a higher education institution to establish policies and control measures for ensuring information security [17, 18]. These essentially transform the principles of information security to implementation.

The ISO 27001 Information Security Management System provides a thorough coverage of the key control areas of information security [21]. By making reference to ISO 27001, there are at least eight control areas for a higher education institution, namely, information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity.

3.1 Information Asset Controls

Policies should be established to ensure that appropriate levels of protection and accountability are maintained for information assets. This should be made in accordance with the sensitivity, criticality and values of information assets, regardless of the media on which they are stored, the manual or automated systems that process them, and the methods by which they are distributed. In a higher education institution, information assets should be classified, and the owner, custodian and users of the information assets should be well defined. It is a good practice that an institution should maintain a master record control table which shows a full list of information assets and the owner, custodian and users of the information assets. This control table is referenced in implementing control measures.

3.2 Personnel Controls

Policies should be established to ensure that everyone in an organization clearly understand his or her roles and responsibilities to reduce the risk of theft, fraud or misuse of information assets. For a higher education institution, all staff should be aware of the information security threats and concerns, and are equipped to support information security in the course of their normal work and reduce the risk of human errors. For example, staff in the Registry and Student Affair Office used to handle a large amount of student information. They have the responsibilities of protecting the student information from theft, fraud and misuse. Control measures should be in place to reduce the risk of theft, fraud or misuse of student information. In many institutions, downloading of student information to portable storage is prohibited, unless absolutely required.

3.3 Physical Controls

Policies should be established to ensure that appropriate physical security and control should be maintained to protect against any unauthorized accesses to some defined secure areas such as data centres. For a higher education institution, computer systems and storage of critical and sensitive information shall be housed in data centres with proper physical access controls. Only authorized persons are allowed to have physical accesses to the data centres, and the access logs should be maintained. Besides, proper environment controls should be in place to protect the computer systems and storage from physical damage. Temperature and humidity should be kept at an acceptable level. Gas-based fire extinguishing systems, instead of water-based fire extinguishing systems, should be installed in data centres to minimize the risk of physical damage to data storage devices in case of fire.

3.4 Access Controls

Policies should be established to ensure that access control to information systems and information processing facilities, and that access rights are properly authorized,

allocated and maintained. Control measures should be implemented to enforce authorized accesses to information as well as to reduce the risks of unauthorized access, loss or damage to information. These measures should also be applied to mobile and remote accesses. In a higher education institution, there should be proper access controls for information systems and information processing facilities, where student information and financial information are stored. An access control table should be defined for each information system. Besides, password controls should be enforced, for example, adoption of strong passwords and compulsory changes of passwords over a certain time period.

3.5 Communication Controls

Policies should be established to define procedures for the management and operation of network and communication facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of communication facilities, such as electronic mailing systems and network storage for information exchange. For a higher education institution, electronic communication is very common. Electronic mails containing student information or sensitive information should be handled with care. It is a good practice to use secured electronic mail systems to protect sensitive information from undetected interception, modification or omission. Encryption and password protection should also be applied to data files on network storage as well as mobile and portable storage devices.

3.6 Operation Controls

Policies should be established to define procedures for the management and operation of computer systems and information processing facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of the computer systems and information processing facilities. System fixes and patches, especially those related to information security, should be timely applied. Backup procedures should be tightly followed, and tapes and disks should be properly stored. It is a good practice to arrange regular system drills to ensure that all critical systems and facilities can be correctly restored in case of information security incidents. System administrator passwords should be properly maintained, and strict password controls, such as the use of strong passwords and compulsory periodical password changes, should be enforced.

3.7 Information System Controls

Policies should be established to ensure proper controls to prevent information systems from any unauthorized modification and misuse of information. Information security requirements should be clearly identified at the beginning of system development. For a higher education institution, the input, processing and output of student information should be properly defined and implemented. These should be enforced during the acquisition, development and maintenance of information

systems. All changes on information systems should be logged. It is a good practice that regular review on these information systems should be conducted to identify and fix information security loopholes if any.

3.8 Incident Management and Business Continuity

Policies should be established to ensure that information security incidents are communicated in an appropriate manner, allowing timely corrective actions to be taken. Clear procedures should be set out for handling incidents that might have an impact on information security. Incidents should be classified in term of severity and impact. According to the level of severity and the scope and impact of an incident, an appropriate incident coordinator should be appointed. On the other hand, it is a good practice that critical business processes identified and integrated with information security requirements, in order to minimize the impact to an acceptable level. For a higher education institution, teaching and learning are critical, and hence, control measures should be enforced to maintain continuity of teaching and learning activities in case of information security incidents.

4 Governance of Information Security

A governance framework is important for establishing the policies and executing the controls of information security. This section discusses the governance of information security in a higher education institution.

It is a good practice to appoint an information security officer who is responsible for the overall governance of information security. In practice, there are two models for information security governance, namely, executive-led model and committee-led model. In the executive-led model, the information security officer is a senior officer who takes the overall responsibility of information security for the institution, including decision-making and policy-making. In the committee-led model, an information security committee is established to take up the roles of an information security officer. Chaired by a senior officer, the committee comprises the owners and custodian of major information repositories, such as the Registrar, Secretary, and the Director of Information Technology.

The information security officer or information security committee is wholly responsible for the design, implementation and execution of the policies and measures on information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. It is important that appropriate authority should be given to the information security officer or information security committee for discharging these duties and responsibilities, especially in handling information security incidents and problems.

Besides implementing the policies and executing the controls, the information security officer or information security committee should conduct regular review on the compliance of information security. A typical way to review the compliance is to

conduct an information security audit. Like many security audits, an information security audit aims to check the compliance of information security with respect to the established policies, guidelines and procedures [22, 23, 24, 25]. It is a good practice for a higher education institution to establish its own audit schedule on information security. Some well-known standards can be referenced in establishing an information security audit framework [24, 25].

Finally, a higher education institution should always ensure that all its staff and students have the awareness on information security, and a thorough understanding of the prevailing policies and controls of information security. To serve this purpose, regular trainings and briefing sessions on information security should be conducted. They are especially useful for new staff and new students, and therefore better be held at the start of each semester. In addition to these trainings and briefing sessions, from time to time, any updates on the information security policies and controls should be communicated to all staff and students.

5 Conclusion

Information security is essential to higher education institutions as any information leakage and damage would incur great losses. There is a need for a higher education institution to enforce information security. Based on the principles of information security, we identify eight control areas on information security, namely, information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. Policies, guidelines and control measures should be established. While the policies provide rules of governance of information security, the guidelines and control measures help execute and implement the policies.

It is important to address a salient point in establishing the policies, guidelines and controls on information security. In reality, flexibility and control are contradictory to each other. In order to enforce information security, it is necessary to implement control measures which inevitably create inflexibility and inconvenience. A right balance between flexibility and control is however difficult to achieve. There are also administrative considerations in implementing the policies, guidelines and control measures, such as on the availability of resources and efficiency in administration. A strong support from senior management is absolutely necessary.

References

[1] Bishop, M.: Computer Security, Art and Science. Addison-Wesley (2003)
[2] Raggad, B.G.: Information Security Management: Concepts and Practices. CRC Press (2010)
[3] Peltier, T.: Information Security Policies and Procedures: A Practitioner's Reference. CRC Press (2004)

[4] Parker, D.B.: Toward a New Framework for Information Security. In: Kabay, M.E. (ed.) The Computer Security Handbook. John Wiley (2002)
[5] Anderson, J.M.: Why We Need a New Definition of Information Security. Computer and Security 22(4), 308–313 (2003)
[6] Matbouli, H., Gao, Q.: An Overview on Web Security Threats and Impact to e-Commerce Success. In: Proceedings of the International Conference on Information Technology and e-Services, pp. 1–6. IEEE Press (2012)
[7] Singh, S., Karaulia, D.S.: E-Governance: Information Security Issues. In: Proceedings of the International Conference on Computer Science and Information Technology, pp. 120–124. IEEE Press (2011)
[8] Hwang, M.S., Li, C.T., Shen, J.J., Chu, Y.P.: Challenges in e-Government and Security of Information. Information & Security 15(1), 9–20 (2004)
[9] Akhawe, D., Barth, A., Lam, P.E., Mitchell, J.: Towards a Formal Foundation of Web Security. In: Proceedings of the IEEE Symposium on Computer Security Foundations, pp. 290–304. IEEE Press (2010)
[10] Pansa, D., Chomsiri, T.: Web Security Improvement by using Dynamic Password Authentication. In: Proceedings of the International Conference on Network and Electronic Engineering, pp. 32–36. IACSIT Press (2011)
[11] Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M.: A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices. IEEE Transactions on Information Forensics and Security 8(8), 1318–1330 (2013)
[12] Chen, C.M., Chen, Y.H., Lin, Y.H., Sun, H.M.: Eliminating Rouge Femtocells based on Distance Bounding Protocol and Geographic Information. Expert Systems with Applications 41(2), 426–433 (2014)
[13] Cheung, K.S.: Development of Organizational Information Security Policies. In: Proceedings of the International Conference on Intelligent Computing and Intelligent Systems, pp. 753–756. IEEE Press (2011)
[14] Cheung, K.S.: A Comparison of WebCT, Blackboard and Moodle for the Teaching and Learning of Continuing Education Courses. In: Tsang, P., et al. (eds.) Enhancing Learning Through Technology, pp. 219–228. World Scientific (2006)
[15] Yau, J., Lam, J., Cheung, K.S.: A Review of E-Learning Platforms in the Age of E-Learning 2.0. In: Wang, F.L., Fong, J., Zhang, L., Lee, V.S.K. (eds.) ICHL 2009. LNCS, vol. 5685, pp. 208–217. Springer, Heidelberg (2009)
[16] Cheung, K.S., Lam, J., Yau, J.: A Review of Functional Features of E-Learning Platform in the Continuing Education Context. International Journal of Continuing Education and Lifelong Learning 2(1), 103–116 (2009)
[17] Rezgui, Y., Marks, A.: Information Security Awareness in Higher Education: An Exploratory Study. Computers & Security 27(7), 241–253 (2008)
[18] Kvavik, R.B.: Information Technology Security: Governance, Strategy and Practice in Higher Education, Center for Applied Research, EDUCAUSE (2004)
[19] Kam, H.J., Katerattanakul, P., Gogolin, G., Hong, S.: Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective. In: Proceedings of the Pacific Asia Conference on Information Systems. Association for Information Systems (2013)
[20] OGCIO, Baseline IT Security Policy, The Office of the Government Chief Information Officer, The Government of the Hong Kong Special Administrative Region, Hong Kong (2009)

[21] ISO, ISO 27000 : Information Security Management System : Family of Standards, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission (2005)
[22] Onwubiko, C.: A Security Audit Framework for Security Management in the Enterprise. In: Jahankhani, H., Hessami, A.G., Hsu, F. (eds.) ICGS3 2009. CCIS, vol. 45, pp. 9–17. Springer, Heidelberg (2009)
[23] Lo, E.C., Marchand, M.: Security Audit: A Case Study. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering, pp. 193–196. IEEE Press (2004)
[24] Kelson, N.: Information Security Management Audit and Assurance Programme. In: ISACA (2010)
[25] ISO, ISO 27007 : Guidelines for Information Security Management Systems Auditing, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission (2011)

Laser Induced Breakdown Spectroscopy Data Processing Method Based on Wavelet Analysis

Lu Muchao

Taiyuan University of Technology College of Information Engineering, Taiyuan 030024, China

Abstract. In this paper, we present a data processing approach for Laser induced breakdown spectroscopy(LIBS). This method is based on wavelet analysis and pattern matching. First, it uses wavelet transforms to decompose the laser induced spectrum data which comes from the sample and obtain the decomposition coefficient of spectrum, then reconstructs the feature background spectrum by means of low frequency coefficient. Through using pattern cluster method to divide the spectrum data of calibration sample into some subsets, then do the calibration for each spectra data in each subsets. Second, we extract effective measurement pattern class template and calibration parameter from the spectrum subset which has the minimum differ between the result of calibration sample and the reality value. In practical process of measurement, we use effective measurement pattern class template to match the spectra data to identify the effectiveness of the measurement. Therefore, we can calculate element contents with the calibration parameter achieved before. This method can decrease the times of laser excitation and increase the measurement accuracy effectively.

1 Introduction

Laser Induced Breakdown Spectroscopy (LIBS) is an analysis technique, in which spectra of laser-produced plasmas were used for qualitative as well as quantitative spectrochemical analysis of material[1]. During the past decade, related technology has produced more reliable lasers, charge coupled detectors, and miniature spectrographs with its capabilities of recording spectra over a wide range of wavelengths. The combination of these technologies has produced unprecedented enhancements in the signal-to-noise ratio. LIBS has rapidly developed into a major analytical technology with the capability of detecting all chemical elements in a sample without any preparation, of real-time response, and of close-contact or stand-off analysis of targets. So it will be used widespread in the future.

But since the spectrum plasma may be disturbed by matrix effect and some objective factors which are difficult to avoid, such as laser intensity fluctuation, characteristics of the sample surface, laser-induced breakdown spectroscopy has some problems which are large random and poor reproducibility and it influence the accuracy of the quantitative analysis.

This paper uses wavelet transform method to obtain the effective measurement pattern class template. Then using this template to match the measured spectra

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_3,

data, identify the validity of the spectrum and calculate the element contents of material. It can increase the accuracy of measurement and reduce the stimulating times of laser.

2 Measuring Principle of Laser-Induced Spectroscopy

LIBS uses a beam of intense pulsed laser irradiation to the measuring material after focusing, the focal point of the measurement object ionization and generate high temperature, high-density plasma. In this method, a solid target is vaporized by a powerful laser pulse to form partially ionized plasma that contains atoms and small molecules. In the high temperature system, the fierce collision between the particles makes the molecular or atomic ionized into ions, and the molecular, atomic and ions can distribute on all energy level, high energy level transition to low level so as to make the laser plasma generate strong spectrum. The LIBS system diagram is shown in the Fig. 1.

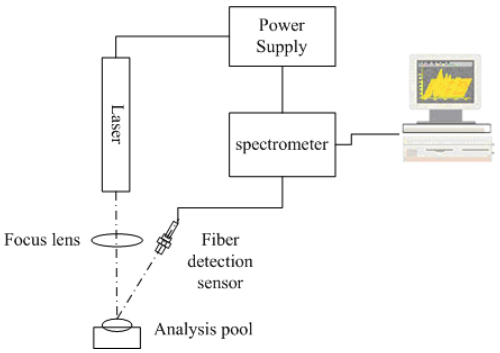


Fig. 1. LIBS system diagram

If local thermodynamic equilibrium (LTE) condition is assumed, the reabsorption effects are negligible (i.e. the plasma is optically thin)[2], the spectrally integrated line intensity, corresponding to the transition between levels E_k and E_i of the generic atomic species with concentration , can be expressed as

$$I_{\lambda}^{K_i} = N_s A_{ki} \frac{g_k e^{-(E_i/K_a T)}}{U_s(T)} \tag{1}$$

where λ is the transition wavelength, N_s is the density of emission atomic, A_{ki} is the transition probability of this spectral line, $U_s(T)$ is the partition function under the plasma temperature, the intensity unit of the line of departure is photon number/cm^3, in the actual measurement process, take the efficiency of optical receiver system into consideration, the intensity of experimental spectral line is indicated as[3]

$$\overline{I_{\lambda}^{K_i}} = FC_s A_{ki} \frac{g_k e^{-(E_i/K_a T)}}{U_s(T)} \tag{2}$$

$\overline{I_{\lambda}^{K_i}}$is the line intensity of the measurement , C_s is the atomic content correspond to this emission line, F is the experimental system parameters including optics efficiency of the receiving system and plasma temperature and its volume. In order to intensify the intensity of spectrum signal and increase the SNR, it calculates the average value of multi-spectrum. The formula (2) only contains C_s as unknown parameters and C_s is related to the element contents of the measured material, the other parameters are known . So when obtaining the $\overline{I_{\lambda}^{K_i}}$, the intensity of this correspond spectral line expresses the concentration of the analysis element by using calibration.

LIBS requires the measuring system under a strict stable environment, such as the laser energetic and point focusing must stand stable[4]. Unfortunate the system cannot keep stable under numbers of conditions in the actual measurement, so it will make a difference between every stimulate results and the simple average method cannot make the efficient handling.

3 The Method Based on Wavelet Feature Extraction

Because the laser induced spectrum contains many spectrum lines, so it is hard to classify and identify the effective or not. In order to solve this problem, we use wavelet decomposition and reconstruction to obtain the background spectrum. After that we classify the background spectrum and obtain the effective measurement pattern, which is used as a template to judge effective of measurement data. And next, we extract the calibration parameters which come from the effective schema. In the actual measuring process, we use the template as the criteria to determine each measurement result whether it is effective or not. If the data set is effective, then calculate the element content via calibration parameters. It is important that this method can obtain effective measuring data in a few excitation processes and increase the measuring accuracy. The data handle process is shown as Fig. 2.

3.1 Wavelet Decomposition and Reconstruction

Recently, the wavelet transform has received considerable attention from researchers in many areas such as signal processing, image processing, pattern recognition, communication, etc. The primary attractive feature of wavelet transform is its capacity for multiresolution analysis. It achieves low-frequency resolution and high time resolution in the high-frequency band, and high-frequency resolution and low time resolution in the low-frequency bands in an adaptive manner. at the same time,Wavelet transform (WT) exhibits very attractive features that make it ideal for studying spectrum signals,so in recent year,wavelet has been used widely in spectrum data processing[6][7][8].

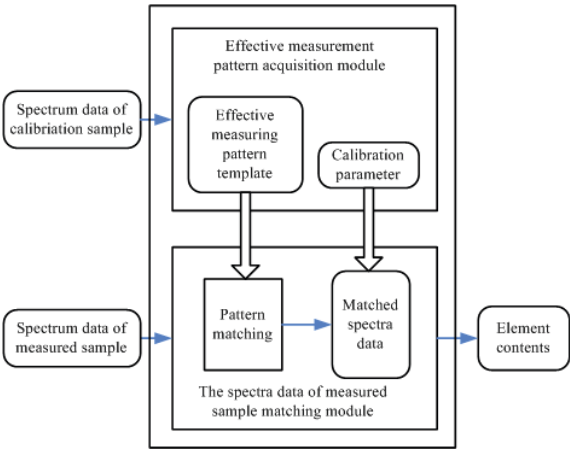


Fig. 2. Diagram of LIBS spectra data processing

Wavelet transform decomposes a signal into localized contributions labeled by a scale and a position parameter. And each of the contributions at different scale represents the information of different frequency contained in the original signal. The discrete wavelet transform(DWT) decomposes the time record $x(t)$ (t=1,2, ..., N) into dyadic wavelet functions $\psi_{j,k}(t)$ and scaling functions $\varphi_{j,k}(t)$. The basis for this decomposition is formed from mother wavelet $\psi(t)$ and father wavelet $\varphi(t)$, by translating in time and dilating in scale[5].

$$\begin{aligned} \psi_{j,k}(t) &= 2^{-j/2}\psi\left(2^{-j}t-k\right) \\ \varphi_{j,k}(t) &= 2^{-j/2}\varphi\left(2^{-j}t-k\right), \qquad j,k \in Z \end{aligned} \tag{3}$$

where k=1, 2, ..., $N/2$, N is the length of data queue . j=1, 2, ...,J, J is often a natural number, Z is the set of integers. Wavelet decomposition produces a family of hierarchically organized decompositions.

At each level j, the j-level approximation $A_j(t)$, and a deviation signal called the j-level detail $D_j(t)$ can be calculated according to the following equations.

$$D_j(t) = \sum_{k\in Z} W(j,k)\psi_{j,k}(t) \qquad j,k \in Z \tag{4}$$

where, $W(\ j,\ k)$ is the wavelet coefficients, and

$$W(j,k) = \int_{-\infty}^{+\infty} x(t)\psi_{j,k}(t)dt \tag{5}$$

The signal $x(t)$ is the sum of all the details:

$$x(t) = \sum_{j\in Z} D_j(t) \tag{6}$$

Then, take a reference level called J; there are two sorts of details. Those associated with indices $j \leq J$ correspond to the fine details, the others, which correspond to $j > J$, are the coarser details, we group these latter details into

$$A_J(t) = \sum_{j>J} D_j(t) \tag{7}$$

which defines what is called an approximation of the signal $x(t)$ Apparently, with the increase of the level J, the resolution defined as 2^{-J}decreases, and $A_J(t)$ will only contain the "lower frequency" components of $x(t)$[5].

3.2 Extraction of Effective Model Class

In experiment, We uses laser to excite m times to each sample which comes from a set of calibration samples of n, every spectra data denoted as $G_{i,j}$,$i = 1, 2, \cdots, n, j = 1, 2, \cdots, m$, and it forms the calibration sample measuring spectra data set $\mathbf{G} = \{G_{i,j}\}$. Every spectrum data sequence is expressed as $G_{i,j}(k) = [X_1, X_2, \cdots, X_k, \cdots X_N]$, N is the length of the spectrum data sequence. The flowchart of extracting effective pattern is shown in Fig. 3.

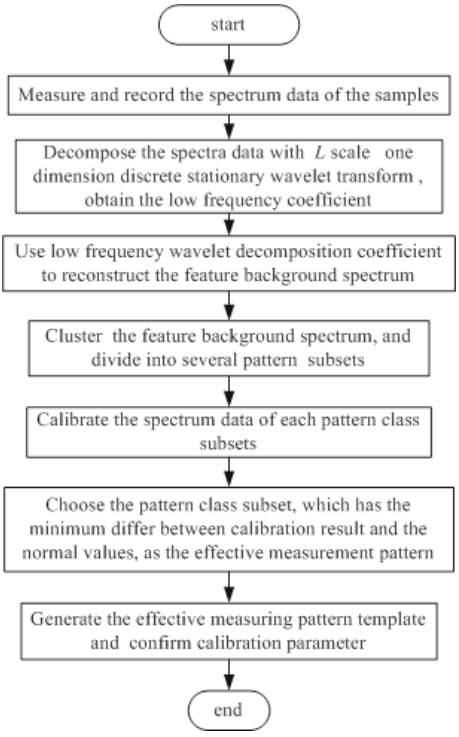


Fig. 3. Flowchart of extracting effective measurement pattern

(1) It decompose each spectrum data sequence $G_{i,j}$, which in the calibration sample spectrum data set, by using L scale one-dimension discrete stationary wavelet and obtains low frequency decomposition coefficient $W^a_{i,j} = [w^a_{l,k}]_{L\times N}$.

(2) Using low frequency decomposition coefficient $W^a_{i,j}$ to reconstruct the spectrum and obtain the feature background spectrum $G^b_{i,j}$ correspond to the spectrum $G_{i,j}$. The feature background data sequence $G^b_{i,j}$ can express as $G^b_{i,j}(k) = [X^b_1, X^b_2, \cdots, X^b_k, \cdots, X^b_N]$. All of the feature background spectrum $G^b_{i,j}$ compose the feature background spectrum set $\mathbf{G}^b = \{G^b_{i,j}\}$.

(3) Carries on the cluster analysis to the background spectrum data $G^b_{i,j}$ in the feature background spectrum data set $\mathbf{G}^b$, and dividing the feature background spectrum data set into several pattern class subsets $\mathbf{G}^b_h$, that is $\mathbf{G}^b = \{\mathbf{G}^b_1, \mathbf{G}^b_2, \cdots, \mathbf{G}^b_h, \cdots, \mathbf{G}^b_H\}$, $h = 1, 2, \cdots, H$. Here H is the number of pattern class subsets which are obtained by analyzing the feature background spectrum data set. According to the correspondence relationship between the spectrum measuring data $G_{i,j}$ and the feature background spectrum data $G^b_{i,j}$, and the partition of background spectrum data set $\mathbf{G}^b = \{G^b_{i,j}\}$, we can divide the calibration sample spectrum measuring data set $\boldsymbol{G}$ into several pattern class subsets $\mathbf{G}_h$ which are correspond to the pattern class subset $\mathbf{G}^b_h$ of feature background data set $\mathbf{G}^b$, that is $\mathbf{G}^{=}\{\mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_h, \cdots, \mathbf{G}_H\}$.

(4) Using reality element content to calibrate the spectrum data contained in each subset $\mathbf{G}_h$, each subset $\mathbf{G}_h$ can obtain a set of calibration parameter β_h and calibration calculating result. Choosing the subset which has the minimum differ between the calibration calculation result and reality value, then extract the feature parameters of this pattern class to form effective measuring pattern G_m. The method of extract effective measuring pattern G_m as fellows:

Suppose the subset $\mathbf{G}_h$ has the minimum differ between the calculated result and reality value. The calibration sample measuring data subset $\mathbf{G}_h$ correspond to the feature background spectrum subset $\mathbf{G}^b_h$ which has E numbers feature background spectrum and the sequence length of each feature background spectrum data is N. Choosing the maximum value of the k locations among all the spectrum sequence of $\mathbf{G}^b_h$ as the higher limit of the effective measuring pattern class sequence $G^m_h(k)$, and choosing the minimum value of the k locations among all the spectrum sequence of $\mathbf{G}^b_h$ as the lower limit of the effective measuring pattern class sequence $G^m_l(k)$, programming language described by the following:

for k = 1 to N

$$G^m_h(k) = \max_{i=1}^{E}(G^b_i(k)); \qquad G^m_l(k) = \min_{i=1}^{E}(G^b_i(k));$$

end

The effective measuring pattern class model defined as $G_m = [G^m_l(k), G^m_h(k)]$.

(5) Choosing the calibration results of $\mathbf{G} = \{\mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_h, \cdots, \mathbf{G}_H\}$ and the calibration parameter β_h (correspond to the subset $\mathbf{G}_h$ which has minimum differ between the results and calibration sample element content reality value) as the calibration parameter used in the actual measuring, and involved in calculating the measured sample element content.

3.3 The Application of Effective Pattern Template

Excite the actual sample to obtain the single laser induced spectrum data G_j, $j = 1, 2, \cdots$.

(1) Process L scale one-dimension discrete stationary wavelet transform to decompose the laser induced spectrum data and obtain the low frequency decomposition coefficient $W^a_{i,j} = [w^a_{l,k}]_{L\times N}$.

(2) Use low frequency wavelet decomposition coefficients W^a_j to reconstruct the spectrum and obtain the feature background spectrum G^b_j which is correspond to the spectrum G_j .

(3) Use effective measuring pattern class template to match the feature background spectrum G^b_j, if this feature background spectrum G^b_j belongs to the effective measuring pattern class, this measured spectrum data is regarded as effective. Feature background spectrum G^b_j and the effective measuring pattern class template matching method is: If the data (location k) in the feature background spectrum data sequence $G^b_j(k)$ fulfill the condition $G^m_l(k) \le G^b_j(k) \le G^m_h(k)$,then match the feature background spectrum G^b_j and the effective measuring pattern class template.

(4) Excite the measured sample until the numbers of effective measuring spectrum data beyond the predefined numbers.

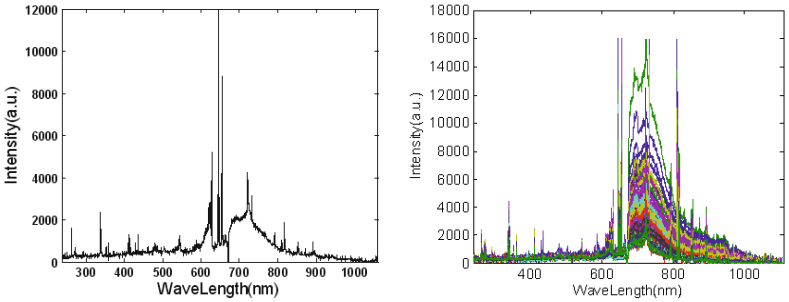
(5) Calculate the element content of the obtained effective measuring spectrum data according to the calibration parameters and use the average value of measured results as the analysis output results.

4 Experiment and Analysis

This paper use LIBS to measure the unburned carbon contents of fly ashes in the thermal power plant. The experiment uses passively Q-type Nd:YAG laser, center wavelength is 1064nm, pulse width is 10ns, pulse repetition frequency is 1∼10 Hz, laser energetic are 120∼160 mJ/Pulse. The spectrograph is AvaSpec-2048FT, communicate with the computer through the USB interface to transfer spectrum data and receive the control order. The spectrograph sends trigger signal to control laser.

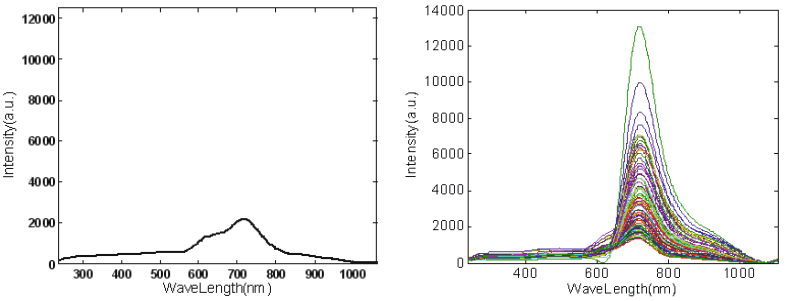
We collect 70 fly ash samples from different regions. Before measure the samples, we grind and stir the samples to make them equality. Then we choose 20 kinds of samples as the calibration samples and performing 100 times laser induced spectrum measuring to each calibration samples and obtain 20×100 laser induced spectrum data. Fig. 4(a) is the spectrum of one time exciting to sample, Fig. 4(b) is the laser induced spectra sets of 100 times exciting to one sample, we can see from the Fig. 4(b) that the random factor and laser energetic fluctuation can affect the stability of spectrum data.

According to this method, a feature background spectrum is reconstructed shown in Fig. 5(a),which corresponding to Fig. 4(a). Fig. 5(b) is the feature background spectrum sets corresponding to Fig. 4(b). Following the next step, the effective measurement pattern template is achieved, which is shown in Fig. 6.



(a) Laser induced spectrum of a single measurement (b) Laser induced spectrum of 100 times measurement to one sample

Fig. 4. Laser induced spectrum of one fly ash sample



(a) Feature background spectrum corresponding to Fig. 4(a) (b) Feature background spectrum corresponding to Fig. 4(b)

Fig. 5. Feature background spectrum of one fly ash sample

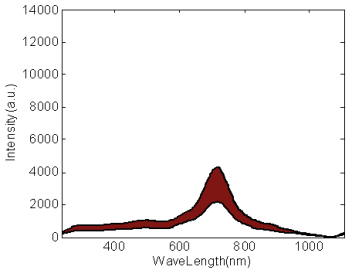
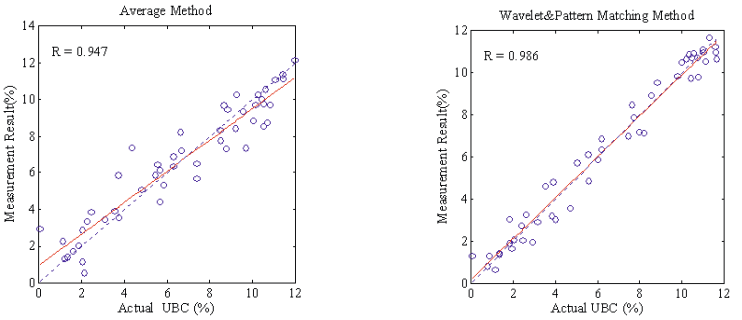


Fig. 6. Sketch map of effective pattern class template

In the measuring process, we use the effective pattern class template to match the measuring data, and if the laser induced spectrum we obtained is effective, then using relevant calibration parameters to calculate the element content. In order to check the effectiveness of this method, we compare the method with the traditional data average method. The traditional method process 50 times

measurement and wipe out 5maximum values and 5 minimum values, then using the 40 remaining measurement results to calculate the average value, the linear regression result is shown in Fig. 7(a). The method in this paper is using 10 pattern class templates matching effective results to calculate the average, the linear regression result is shown in Fig. 7(b). Comparing Fig. 7(a) and Fig. 7(b), we can clearly figure out that the method of this paper is effective than the average method, also the laser excite times to 50 samples are decrease from 2500 to 956, so it can not only increase the measurement efficiency , but also extend life span of the laser at the same time.



(a) Average Method Result

(b) Wavelet&Pattern Matching Method

Fig. 7. Result comparison

5 Conclusion

LIBS is widely used in qualitative and quantitative analysis the element contents of various kinds of subjects and LIBS has great practical value. But it has lots of factors which are difficult to avoid, such as laser intensity pulse, feature of sample surface and cardinal effect, so the consequence is that it has large randomness and negative repeatability and the accuracy of quantitative analysis will also be affected. On one hand, we can improve the method by improving the hardware device, on the other hand we can take some proper technique method to process the data of laser induced spectrum. This paper uses wavelet analysis and pattern recognition method to obtain the laser induced spectrum and pick up the effective measuring pattern template and correspond calibration parameter. In measuring process, this paper uses template matching method to identify the effectiveness of measuring data and calculate the effective data. This improvement can increase the measurement effective and accuracy, also can decrease the stimulate times of laser and increase the life span of laser at the same time. The experiment indicate the this method is effective.

References

1. Yao, M., Liu, M., Zhao, J., et al.: Identification of Nutrition Elements in Orange Leaves by Laser Induced Breakdown Spectroscopy. In: Third International Symposium on Intelligent Information Technology and Security Informatics, IITSI 2010, pp. 398–401. IEEE Computer Society, Jinggangshan (2010)
2. Kompitsas, M., Roubani-Kalantzopoulou, F., Bassiotis, I.: Laser Induced Plasma Spectroscopy (Lips) as an Efficient Method for Elemental Analysis of Environmental Samples. In: Proceedings of EARSeL-SIG-Workshop LIDAR, Dresden/FRG, June 16-17, pp. 130–138 (2000)
3. Ciucci, A., et al.: New Procedure for Quantitative Elemental Analysis by Laser-Induced Plasma Spectroscopy. Appl. Spectrosc. 53, 960–964 (1999)
4. Ramil, A., Lpez, A.J., Yez, A.: Application of artificial neural networks for the rapid classification of archaeological ceramics by means of laser induced breakdown spectroscopy (LIBS). Applied Physics A: Materials Science and Processing 92(1), 197–202 (2008)
5. Hu, Y., Jiang, T., Shen, A., Li, W., Wang, X., Hu, J.: A background elimination method based on wavelet transform for Raman spectra. Chemometrics and Intelligent Laboratory Systems 85(1), 94–101 (2007)
6. Esteban-Diez, I., Gonzalez-Saiz, J.M., Gomez-Camara, D., Pizarro Millan, C.: Multivariate calibration of near infrared spectra by orthogonal wavelet correction using a genetic algorithm. Analytica Chimica Acta 555, 84–95 (2006)
7. Yiou, P., Sornette, D., Ghil, M.: Data-adaptive wavelets and multi-scale singular-spectrum analysis. Physica D 142, 254–290 (2000)
8. Zhang, X., Zheng, J., Gao, H.: Curve fitting using wavelet transform for resolving simulated overlapped spectra. Analytica Chimica Acta 443, 117–125 (2001)

Towards Time-Bound Hierarchical Key Management in Cloud Computing

Tsu-Yang Wu[1,2], Chengxiang Zhou[1], Eric Ke Wang[1,2], Jeng-Shyang Pan[1,2], and Chien-Ming Chen[1,2,⋆]

[1] Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, 518055, China
[2] Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen, 518055, China
{wutsuyang,hitcms2009,jengshyangpan,chienming.taiwan}@gmail.com, 962982698@qq.com

Abstract. Nowadays, data outsourcing in the cloud is used widely and popularly by people. It also arises several security problems. To control access of outsourced data with different priority becomes an important research issue. Recently, Chen et al. proposed the first hierarchical access control scheme in cloud computing. However, they did not concern with the time-bound property. In some applications such as Pay-TV, the time-bound property is necessary because subscriber may subscribe some channels during one month. In this paper, we propose the first time-bound hierarchical key management scheme in cloud computing without tamper-resistant devices. The security analysis demonstrates that the proposed scheme is provably secure against outsider and insider attacks.

Keywords: Time-bound hierarchical key management, cloud computing, bilinear pairing, security.

1 Introduction

Cloud storage services [1] have been received much attention recently. They provide relative techniques for data outsourcing, access [2], and sharing [3]. In data outsourcing, data provider (DP) outsources her/his data to cloud server (CS) rather than storing data locally. Any authorized user can access these data form CS via Internet. However, data outsourcing arises some security problems: (1) DP do not want to disclose her/his data to CS and (2) DP should control access of outsourced data with different priority.

The access control problem is to control users who are able to access the resources in a system. In the system, users may be organized in a hierarchy formed by several disjoint classes. These classes have different limitations on the resources. In other words, some users own more access rights than others.

⋆ Corresponding author.

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*, Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_4,

Up to now, several hierarchical key management schemes have been published in [4,5,6,7]. However, in some applications, time-bound property should be concerned. For example, in Pay-TV system, a subscriber may want to subscribe the news channel in some time period such as one week, one month, or one year. Hence, time-bound property needs involved in hierarchical key management schemes.

In 2002, Tzeng [8] proposed the first time-bound hierarchical key assignment scheme. However, his scheme was proved insecure against the collusion attack Yi and Ye in 2003 [9]. In 2004, Chien [10] proposed an efficient time-bound hierarchical key assignment scheme. Unfortunately, his scheme was also proved insecure in [11]. In 2005, Yeh [12] proposed an RSA-based hierarchical key assignment scheme. In the same year, Wang and Laih [13] proposed a time-bound hierarchical scheme by using merging. In 2006, Ateniese et al. [14] considered the unconditionally secure and computationally secure setting for a time-bound hierarchical scheme. They proved that Yeh's scheme [12] is insecure and proposed a provably-secure time-bound hierarchical key assignment scheme based on the discrete logarithm problem with a tamper-resistant device. In 2009, Sui et al. [15] proposed a time-bound access control scheme for dynamic access hierarchical. This scheme is the first one to support dynamics of access hierarchical. In 2012, Chen et al. [16] proposed a time-bound hierarchical key management scheme without tamper-resistant device. In the same year, Tseng et al. [17] proposed two pairing-based time-bound key management schemes without hierarchy. The first scheme used Lucas function for continuous time period and the second scheme is based on RSA for discrete time period. In 2013, Chen et al. [18] proposed the first hierarchical access control scheme in cloud computing. In their scheme, the encrypted data provided by DP can be transformed by using proxy re-encryption method such that authorized users can decrypt them. Unfortunately, they did not concern the time-bound issue. It means that the user revocation is complex and all established keys must be reset.

In this paper, we based on Chen et al.'s scheme [16] propose the first pairing-based time-bound hierarchical key management scheme in cloud computing. The advantage of our scheme does not require any tamper-resistant devices and is suitable for cloud environments. The security analysis is demonstrated that our scheme is secure against outsider and insider attacks. Finally, the performance analysis is given.

The rest of this paper is organize as follows: In Section 2, we introduce the necessary preliminaries which contain bilinear pairings, the hierarchical access control policy, and all-or-nothing transformation. The concrete scheme is proposed in Section 3. In Section 4, we present the security analysis of our scheme. The performance analysis is given in Section 5 and the conclusions are draw in Section 6.

2 Preliminaries

2.1 Bilinear Pairings

Let G_1 and G_2 be two groups with a same order q, where q is a large prime. Here, G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group. A bilinear pairing e is a map defined by $e : G_1 \times G_1 \rightarrow G_2$ which satisfies the following three properties:

(1) Bilinear: For all P, $Q \in G_1$, a, $b \in Z_q$, we have $e(aP, bQ) = e(P, Q)^{ab}$.
(2) Non-degenerate: For all $P \in G_1$, there exists $Q \in G_1$ such that $e(P, Q) = 1_{G_2}$.
(3) Computable: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

For the details of bilinear pairings, readers can refer to [19,20,21].

2.2 HAC Policy

The hierarchical access control (HAC) policy enables data access in a hierarchy [22]. According to the HAC policy, data is organized into n classes $C_1, C_2, \ldots, C_n$. The relation between these classes is defined as a binary relation $\prec$. Note that $C_j \prec C_i$ means that the security level of C_i is higher than C_j. In other words, if a user is allowed to access data in C_i, he can also access data in C_j. However, the opposite is forbidden.

2.3 *AONT*

An all-or-nothing transformation ($AONT$) [23] maps an α-blocks message $X = X_1||X_2||\cdots||X_\alpha$ with a random string r into an α'-blocks message $Y = Y_1||Y_2||\cdots||Y_{\alpha'}$. $AONT$ satisfies the following three properties:

(1) $Y \leftarrow AONT(X, r)$ can be computed efficiently for given X and r.
(2) $X \leftarrow AONT^{-1}(Y)$ can be computed efficiently for given Y.
(3) It is infeasible to recover X for any block of Y lost.

2.4 Notations

The following notations which are used throughout this paper:

- e: a bilinear map, $e : G_1 \times G_1 \rightarrow G_2$.
- P: a generator of group G_1.
- z: the maximum life cycle of system.
- T: the maximum subscribing time of user.
- B_i: public parameters, $B_i = \{D_{i,u} | D_{i,u} = a^u b^{i-u} P, \forall u \in [0, i]\}$ for $i = \{1, 2, \ldots, T\}$.
- $K_{i,t}$: a class key for class C_i, $K_{i,t} = e(P, P)^{a^t b^{z-t} e_i}$, where t is a time period.
- AES: the advanced encryption standard.
- $AONT$: an all-or-nothing transformation.
- K_{i,t_1,t_2}: a decryption key subscribed by user, $K_{i,t_1,t_2} = e_i a^{t_1} b^{z-t_2} P$, where i denotes class C_i and t_1, t_2 denote user's subscribing time from t_1 to t_2.

3 Proposed Scheme

In our scheme, there are three entities: data provider (DP), cloud server (CS), and user. Note that DP outsources his data to CS and it has endless storage capacity but is "honest-but-curious". In other words, it honestly follows the proposed scheme but is curious to know the content of outsourced data. The proposed scheme consists of following five phases.

Initialization. In this phase, DP provides a set of data $D = \{D_1, D_2, \ldots, D_n\}$ and defines an HAC policy for D. In this policy, a set of class $C = \{C_1, C_2, \ldots, C_n\}$ is defined. These classes form a directional graph $G = (V, E)$ with the relation $\prec$ mentioned in Subsection 2.2. Then, DP chooses a bilinear map $e : G_1 \times G_1 \rightarrow G_2$ and a generator $P \in G_1$. Assume that the maximum life cycle of system is $z < q$ and the maximum subscribing time is T, where $T < z$. DP selects two random values a, $b \in {Z_q}^*$ and computes $B = \{B_1, B_2, \ldots, B_T\}$, where $B_i = \{D_{i,u} | D_{i,u} = a^u b^{i-u} P, \forall u \in [0, i]\}$ for $i = \{1, 2, \ldots, T\}$. Finally, DP publishes public parameters $\{e, G_1, G_2, q, P, B\}$.

Class Key Assignment Phase. For each class C_i, DP firstly assigns a secret value $e_i \in {Z_q}^*$ as a key. At each time period t, DP generates a class key $K_{i,t} = e(P, P)^{a^t b^{z-t} e_i}$. For each pair $C_j \prec C_i$, DP computes $N_{i,j,t} = AES_{K_{i,t}}(K_{j,t})$, where AES denotes the advanced encryption standard [24]. Note that $N_{i,j,t}$ is published in each time period t.

Data Outsourcing Phase. Without loss of generality, we assume that each D_i is put into class C_i for $i = 1, 2, \ldots n$. When DP wants to outsource her/his data D_i to CS in C_i, DP firstly selects a random value $k_i \in Z_q^*$ and random string r_i for D_i. Then, DP proceeds D_i with $AONT$ to get $D_i^{'} = D_{i,1} || D_{i,2} || \ldots || D_{i,\alpha'}$. Then, DP encrypts D_i to generate a ciphertext

$$\Phi_i = (\{k_i || \rho\}_{K_{i,t}}^{AES}, \{D_{i,1}\}_{k_i}^{AES} || \cdots || \{D_{i,(\rho-1)}\}_{k_i}^{AES} || \{D_{i,\rho}\}_{K_{i,t}}^{AES} || \{D_{i,(\rho+1)}\}_{k_i}^{AES} || \cdots || \{D_{i,\alpha'}\}_{k_i}^{AES})$$

where ρ is a random value, $1 < \rho < \alpha^{'}$. Finally, DP sends $(ID_{D_i}, ID_{DP}, C_i, \Phi_i)$ to CS.

User Subscribing Phase. When a user U wants to subscribe class C_i from t_1 to t_2, DP generates a decryption key $K_{i,t_1,t_2} = e_i a^{t_1} b^{z-t_2} P$ and sends it to U via a secure channel.

Decrypting Phase. Suppose that a user U subscribes class C_i in $[t_1, t_2]$. Then, she/he not only accesses D_i in C_i but also can access D_j in C_j with $C_j \prec C_i$ in any time $t \in [t_1, t_2]$. Hence, there are two cases should be concerned.

Case 1. U wants to access D_i in t. Upon receiving the request from U, CS sends the related ciphertext Φ_i to U. The user firstly compute the class key $K_{i,t} = e(K_{i,t_1,t_2}, D_{\lambda,x})$, where $t_1 + x = t = t_2 - y$, $t_2 - t_1 = \lambda = x + y$. Then, U decrypts

$\{k_i||\rho\}^{AES}_{K_{i,t}}$ to obtain k_i and ρ. Finally, all $D_{i,1}, D_{i,2}, \ldots D_{i,\alpha'}$ are obtained and thus the data D_i can be derived by using $AONT^{-1}(D_{i,1}||D_{i,2}||\cdots||D_{i,\alpha'})$.

Case 2. U wants to access D_j in t. Upon receiving the request from U, CS sends the related ciphertext Φ_j to U. The user firstly computes the class key $K_{i,t}$ and then decrypts $N_{i,j,t}$ to obtain $K_{j,t}$. By the similar method in Case 1, the data D_j can be derived.

4 Security Analysis

In this section, we demonstrate the security of our scheme. Here, we consider the two types of attacks: outsider and insider attacks.

Theorem 1. *Under the security of AES and the AONT assumption, the proposed scheme is secure against outsider attacks.*

Proof. Here, there two cases should be concerned.

Case 1. A user U who does not subscribe any class C_i from DP cannot compute the class key $K_{i,t}$ because U has no the decryption key K_{i,t_1,t_2}. Furthermore, U cannot generates a fake decryption key K'_{i,t_1,t_2} in some time interval $[t_1, t_2]$ because e_i, a, b are secret values kept by DP. In other aspect, U cannot break the ciphertext Φ_i directly to obtain D_i under the security of AES and the $AONT$ assumption.

Case 2. CS cannot obtain D_i from the ciphertext Φ_i. This case is a special case of Case 1.

Theorem 2. *Under the security of AES and the AONT assumption, the proposed scheme is secure against insider attacks.*

Proof. Firstly, we consider a simple case that a user U who subscribe class C_i in $[t_1, t_2]$ cannot access D_i in time t_3 for $t_3 > t_2$ or $t_3 < t_1$. Here, U has got the key $K_{i,t_1,t_2} = e_i a^{t_1} b^{z-t_2} P$. In order to access D_i in time t_3, U must obtain the class key $K_{i,t_3} = e(P,P)^{a^{t_3} b^{z-t_3} e_i}$. Hence, U may find a point $D = a^{t_3-t_1} b^{t_2-t_3} P \in G_1$ such that $K_{i,t_3} = e(K_{i,t_1,t_2}, D)$. However, it is impossible because a and b are secret values kept by DP.

Then, we consider the colluding attacks. Assume that there exist two users U_1 and U_2 who collude to access the data which is not subscribed by them. Here, there four cases should be concerned.

Case 1. Assume that U_1 subscribes C_j from t_1 to t_2 and U_2 subscribes C_k in the same time interval, where $C_j \prec C_i$ and $C_k \prec C_i$. They want to compute the class key $K_{i,t}$ which can access D_i in the class C_i from t_1 to t_2. Now, U_1 has the key $K_{j,t_1,t_2} = e_j a^{t_1} b^{z-t_2} P$ and U_2 has the key $K_{k,t_1,t_2} = e_k a^{t_1} b^{z-t_2} P$. However, it is impossible to compute $K_{i,t_1,t_2} = e_i a^{t_1} b^{z-t_2} P$ because e_i, a, b are secret values kept by DP.

Case 2. Assume that U_1 subscribes C_j from t_1 to t_3 and U_2 subscribes C_k from t_2 to t_4, where $C_j \prec C_i$, $C_k \prec C_i$, and $t_1 < t_2 < t_3 < t_4$. They want to compute the class key $K_{i,t}$ which can access D_i in the class C_i from t_2 to t_3. Now, U_1

has the key $K_{j,t_1,t_3} = e_j a^{t_1} b^{z-t_3} P$ and U_2 has the key $K_{k,t_2,t_4} = e_k a^{t_2} b^{z-t_4} P$. However, it is impossible to compute $K_{i,t_2,t_3} = e_i a^{t_2} b^{z-t_3} P$ because e_i, a, b are secret values kept by DP.

Case 3. From Case 1, assume that the cloud server (CS), U_1, and U_2 collude. They want to access D_i in the class C_i from t_1 to t_2. By Case 1, to compute $K_{i,t_1,t_2} = e_i a^{t_1} b^{z-t_2} P$ is infeasible. By Theorem 1, they cannot break the ciphertext Φ_i directly to obtain D_i under the security of AES and the $AONT$ assumption.

Case 4. From Case 2, assume that the cloud server (CS), U_1, and U_2 collude. They want to access D_i in the class C_i from t_2 to t_3. By Case 2, to compute $K_{i,t_2,t_3} = e_i a^{t_2} b^{z-t_3} P$ is infeasible. By Case 3, they cannot break the ciphertext Φ_i directly to obtain D_i under the security of AES and the $AONT$ assumption.

5 Performance Analysis

For convenience to evaluate the performance of our scheme, we first define the following notations:

- TG_e: The time of executing a bilinear pairing operation, $e : G_1 \times G_1 \to G_2$.
- TG_{mul}: The time of executing a scalar multiplication operation of point in G_1.
- T_{exp}: The time of executing a modular exponentiation operation.
- T_{AES}: The time of executing the AES algorithm.
- l: The number of blocks for a outsourced file.
- d: The path length between the subscribing class and its lower level classes.

Here, we demonstrate the executing time in each phase of our scheme in Table 1.

Table 1. The executing time in each phase of our proposed scheme

Phases	Executing time
Data outsourcing	$n(l+1)T_{AES}$
User subscribing	$TG_{mul} + 2T_{exp}$
Decrypting for subscribing class	$TG_e + (l+1)T_{AES}$
Decrypting for lower class of subscribing class	$TG_e + (l+d)T_{AES}$

6 Conclusions

In this paper, we have proposed the first time-bound hierarchical key management scheme in cloud computing. Our scheme does not require any tamper-resistant devices and is suitable for cloud environments. The security analysis is demonstrated that our scheme is secure against outsider and insider attacks. For the future work, we will design a new scheme for discrete time period.