Special issue on soft computing for digital information forensics

Shiguo Lian · Gregory L. Heileman ·
Afzel Noore

Published online: 28 October 2009
© Springer-Verlag 2009

1 Introduction

The emergence and evolution of new digital technologies are dramatically changing how information is captured, processed, analyzed, interpreted, transmitted, and stored. While digital technology has greatly improved the collection and analysis of evidences, the underlying research challenges primarily focus on the integrity and the reliability of validating the resulting forensic decisions accurately. Furthermore, digital evidences can be easily tampered, altered, or forged to commit fraud, identity theft, or impersonate someone else, to remain elusive from law enforcement. Using image processing techniques, it is easy to tamper the original image by replacing an individual's face, and making the change difficult to detect. Image forensic techniques use natural properties of image to determine forgery or locate tampering. In another example, it is possible to determine whether an image is generated by a digital camera, a cell-phone camera, or a computer by analyzing the image properties and characteristics and comparing the statistics of various digital devices.

With the rise of digital crime (signature forgery, image forgery, illegal transaction, etc.) and the pressing need for methods to combat these forms of criminal activities, there is an increasing awareness of the importance of information forensics for security applications. Fundamental areas of interest include attack models, cryptanalysis, steganalysis, authentication, human identification, signal classification, surveillance, transaction tracking, etc. In many practical applications, the evidences collected from a crime scene may be non-ideal due to poor quality or availability of partial information. It is imperative for new research approaches to fuse information from multiple evidences to make a forensic decision or reliably classify as genuine or imposter.

In all these forensic applications, soft computing techniques such as neural networks, fuzzy logic, evolutionary computing, and rough set, play an important role in learning complex data structures and patterns, and classifying them to make intelligent decisions. Soft computing has been widely used in various applications, such as machine vision, pattern detection, data segmentation, data mining, adaptive control, biometrics, and information assurance.

This special issue of the Soft Computing Journal invited authors to submit their original work that communicates current research on soft computing for digital information forensics regarding both the novel solutions and future trends in the field. In this special issue, we have 8 papers, which can demonstrate advanced works in the field.

2 The papers in this special issue

This special issue's papers can be grouped into four categories: (1) person identification based on soft computing,

S. Lian (✉)
Human–Computer Interface (HCI) Lab, France Telecom R&D
(Orange Labs), Beijing, China
e-mail: shiguo.lian@orange-ftgroup.com

G. L. Heileman
Electrical and Computer Engineering Department,
University of New Mexico, Albuquerque, USA
e-mail: heileman@ece.unm.edu

A. Noore
Lane Department of Computer Science and Electrical
Engineering, West Virginia University, Morgantown, USA
e-mail: afzel.noore@mail.wvu.edu

(2) multimedia forensics based on soft computing and (3) network forensics based on soft computing.

2.1 Person identification based on soft computing

This part consists of 4 papers, investigating person identification based on face recognition, heartbeat identification and mark identification.

The first two papers focus on face reconstruction and recognition. In the first paper, “2D Face Fitting Assisted 3D Face Reconstruction for Pose-Robust Face Recognition” by L. Wang, L. Ding, X. Ding and C. Fang, a 2D face fitting assisted 3D face reconstruction algorithm is presented, aiming at recognizing faces of different poses when each face class has only one frontal training sample. For each frontal training sample, a 3D face is reconstructed by optimizing the parameters of 3D Morphable Model. Thus, the training set of face recognition is enlarged by rotating the reconstructed 3D face to different views. The key innovation is to utilize automatic 2D face fitting to assist 3D face reconstruction, where 88 sparse points of the frontal face are located by 2D face fitting algorithm. The experimental results show that the proposed method is effective and the face recognition results towards pose-variant are promising. The second paper, “Construction of Human Faces from Textual Descriptions” by D. Bhattacharjee, S. Halder, M. Nasipuri, D. Basu and M. Kundu, presents a novel face construction approach based on textual description with the stored facial components extracted from different face databases. Here, two types of databases are adopted, including Full Face Database (DB-F) and Facial Component Database (DB-C). If the desired face is not available in DB-F, then a new face is constructed with the help of DB-C. The experiments based on 200 male and female face images are done, which obtains the average facial component extraction rate of 93% and average face construction rate of 80%. Additionally, some hardware based implementations have been done for practical applications.

The third paper, “Classification of Heartbeats Using Correlation for Individual Identification” by Y. Singh and P. Gupta, presents a method to identify individuals by the heartbeats. Firstly, new techniques are proposed to delineate P and T waves efficiently from heartbeats. Then, these delineators are used to extract various features, such as time interval, amplitude and angle, from clinically dominant fiducials on each heartbeat. Finally, the identification system is constructed, which uses these features and make the decision on the identity of an individual with respect to a given database. The decision is made on the basis of correlation between heartbeat features among individuals. The system has been tested, which obtains the equal error rate less than 1.01 with the accuracy of 99%.

The fourth paper, “Method of verifying declared identity in optical answer sheets” by J. Levi, Y. Solewicz, Y. Dvir and Y. Steinberg, presents a method to identify imposters in examinations by investigating the marks in optical answer sheets. The method characterizes personal quality of mark shapes in optically-read answer sheets. Firstly, all the marks are segmented and measured in multiple parameters including area, dimensions, perimeter, and optical density. Then, imposter decisions are made on the collected data by comparing an identified test form against the form in question in comparison with a population using Support Vector Machine modeling. The experiments are done on 300 test forms from 100 examinees, which obtain the Equal Error Rate of 15–17%.

2.2 Multimedia forensics based on soft computing

This part consists of 3 papers, investigating multimedia analysis and forensics.

The paper, “Automatic Video Temporal Segmentation Based on Multiple Features” by S. Lian, investigates automatic video temporal segmentation techniques, also named Shot Boundary Detection (SBD) techniques. It reviews the existing SBD algorithms in detail, proposes a new algorithm to obtain fast and accurate detection, and evaluates its performances by comparative experiments. Based on multiple features, such as pixel difference, histogram difference and motion-based difference, the video sequence is partitioned into adjacent shots. Each shot is composed of continuous frames. This technique can be used to segment a news program into different stories. Additionally, the segmented contents can be used for further processing, such as key frame extraction, video summary or highlight extraction.

The paper, “Effective Fuzzy Clustering Techniques in Segmentation of Breast MRI” by S. Kannan¹, A. Sathya and S. Ramathilagam, proposes an image segmentation method for breast Contrast-Enhanced Magnetic Resonance Breast Imaging (ce-MRI). The segmentation method is developed based on the improved Standard Fuzzy clustering techniques. In the improved method, an effective way of predicting membership grades for objects is presented. Some experiments are done to test the technique’s performances. The technique can be used to segment the breast into deferent regions, each corresponding to a different tissue, and to identify tissue regions judged abnormal.

The paper, “Image Authentication based on Perceptual Hash using Gabor Filters” by L. Wang, X. Jiang, S. Lian, D. Hu and D. Ye, presents an image forensic method based on perceptual hash. In this method, the perceptual characters of the image are extracted using Gabor filter, including the reference scale, direction and block. These characters can survive rotation, scale, translation (RST) attacks while

be sensitive to local malicious manipulations. Then, the perceptual hash is computed based on these characters, and used to detect the image's originality. Experimental results and theoretical analysis show that this method can not only tell whether the image is changed or not but also locate the content-altering changes.

2.3 Network forensics based on soft computing

This part contains only one paper, investigating network forensics. In this paper, "RSTEG: Retransmission Steganography and Its Detection" by W. Mazurczyk, M. Smolarczyk and K. Szczypiorski, a steganographic method called Retransmission Steganography is presented for network information hiding and extraction. At sender side, the information is embedded into data packets by utilizing retransmission mechanisms. At receiver side, the

information is extracted from the network packets. The method for transmission control protocol (TCP) retransmission mechanisms is also proposed and described in detail. Additionally, some analysis methods for attacking or detecting the information hiding system are also investigated and tested. Simulations in different network environments are done, and the results show the method's performances suitable for practical applications.

Acknowledgments The guest editors wish to thank Prof. Antonio D. Nola (Editor-in-Chief), Prof. Vincenzo Loia (Co-Editor-in-Chief) and Dr. Brunella Gerla (Managing Editor) for providing the opportunity to edit this special issue on Soft Computing for Digital Information Forensics. We would also like to thank the authors for submitting their works as well as the referees who have critically evaluated the papers within the short stipulated time. Finally, we hope the reader will share our joy and find this special issue very useful.