

Preface

It is our great pleasure to compile the Platinum Jubilee Commemorative Monograph Series of the Indian Statistical Institute: Volume 3, titled Algorithms, Architectures, and Information Systems Security. This volume contains mostly a collection of invited papers from leading researchers. It also includes the extended versions of a few papers, which were presented at the Second International Conference on Information Systems Security (December 18–20, 2006), and in Track I of the International Conference on Computing: Theory and Applications (March 5–7, 2007), both held in Kolkata as part of the Platinum Jubilee celebration of the Institute (1931–2006).

There are sixteen chapters in this volume. The first five chapters (Chapters 1–5) address several challenging geometric problems and related algorithms. The next five chapters (Chapters 6–10) focus on various optimization issues in VLSI design and test architectures, and in wireless cellular networks. The last six chapters (Chapters 11–16) comprise scholarly articles on Information Systems Security.

Chapter 1 by Li and Klette presents two important rubberband algorithms for computing Euclidean shortest paths in a simple polygon, which have major applications in 2D pattern recognition, picture analysis, and in robotics. The second chapter by Cheng, Dey, and Levine contains the theoretical analysis of a Delaunay refinement algorithm for meshing various types of 3D domains such as polyhedra, smooth and piecewise smooth surfaces, volumes enclosed by them, and also non-manifold spaces. In Chapter 3, Pach and Tóth characterize the families of convex sets in a plane that are not representable by a point set of the same order type. Further, they establish the size of the largest subfamily representable by points and discuss related Ramsey-type geometric problems. The fourth chapter by Asano, Katoh, Mehlhorn, and Tokuyama describes efficient algorithms for some generalizations of least-squares method. These are useful in approximating a data set by a polyline with one joint that minimizes the total sum of squared vertical errors. A few other related geometric optimization problems have also been studied. Chapter 5 by Wei and Klette addresses the depth recovery problem from gradient

vector fields. This has tremendous significance in 3D surface reconstruction and has several applications in computer vision. The authors present three schemes: a two-scan method, a Fourier-transform based method, and a wavelet-transform based method.

In Chapter 6, Börner, Leininger, and Gössele present a new design of a single-output convolutional compactor for guaranteed 6-bit error detection. In Electronic Design Automation, such detectors are of importance for compressing test and diagnostic data of large VLSI circuits. Bhattacharya, Seth, and Zhang address the problem of low-energy pattern generation for random testing VLSI chips in Chapter 7. The method suits well in scan-based systems, and reduces test application time significantly. Chapter 8 by Taghavi and Sarrafzadeh has a review of existing methodologies for estimation and reduction of routing congestion at the floorplanning and placement phases of VLSI design cycle, followed by a novel contribution on a more general and accurate approach. The ninth chapter by Sinha and Audhya deals with the channel assignment problem in a hexagonal cellular network with two-band buffering that supports multimedia services. New lower bounds on minimum bandwidth requirement are derived and algorithms for channel assignment are presented. Chapter 10 by Das, Das, and Nandy contains an extensive survey on range assignment problems in various types of wireless networks, and their computational geometric solutions.

Focusing on the emerging problems of privacy in the electronic society, Ardagna, Cremonini, Damiani, De Capitani di Vimercati, and Samarati have highlighted in Chapter 11, the issues related to the protection of personal data released in an open public network. This chapter considers the combination of different security policies and their enforcement against a laid down privacy policy or a possible privacy law. It also considers the protection of location information in location-based services. In Chapter 12, Chen and Atluri discuss a situational role-based access control and risk-based access control mechanism in a networked environment where personal data often kept with third parties, need stringent security measures to be relaxed only in case of an emergency. In Chapter 13, Jajodia and Noel propose a framework for Topological Vulnerability Analysis (TVA) of a network connecting individual components of a distributed system. It simulates the possible ways for incremental network penetration and builds complete maps of multi-step-attacks discovering all possible attack paths. TVA also computes network hardening options to protect critical resources against minimal network changes. Chapter 14 by Dash, Reddy, and Pujari presents a new malicious code detection technique using variable length n -grams based on the concept of episodes. The authors have pointed out that proper feature extraction and selection technique can help in efficiently detecting virus programs. The next

chapter (Chapter 15) addresses an important area of research called digital image forensics, which stems from the need for creation, alteration and manipulation of digital images. Sencar and Memon provide an excellent survey of the recent developments covering image source identification, discrimination of synthetic images, and image forgery detection. The last chapter (Chapter 16) by Butler, Enck, Traynor, Plasterr, and McDaniel deals with privacy preserving web-based email. In spite of the privacy policies stipulated by the service providers of web-based applications, personal information of the users collected by them may have indefinite life and can later be used without restriction. The authors have proposed a method to create virtual channels over online services, through which messages and cryptographic keys are delivered for preserving privacy.

We take this opportunity to express our heartfelt gratitude to all the eminent contributors of this monograph on Algorithms, Architectures, and Information Systems Security. We are also grateful to Prof. Sankar K. Pal, Director of the Indian Statistical Institute, for his support and encouragement in preparing the volume. We earnestly hope that this collection of technical articles would be of archival value to the peer community. Finally, the help of Mr. Indranil Dutta to prepare the camera-ready version is gratefully acknowledged.

Bhargab B. Bhattacharya
Susmita Sur-Kolay
Subhas C. Nandy
Aditya Bagchi