Studies in Computational Intelligence

Volume 901

Series Editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series "Studies in Computational Intelligence" (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

The books of this series are submitted to indexing to Web of Science, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink.

More information about this series at http://www.springer.com/series/7092

Jyotsna Kumar Mandal

Reversible Steganography and Authentication via Transform Encoding

Springer

Jyotsna Kumar Mandal
Department of Computer Science
and Engineering
University of Kalyani
Kalyani, West Bengal, India

ISSN 1860-949X ISSN 1860-9503 (electronic)
Studies in Computational Intelligence
ISBN 978-981-15-4396-8 ISBN 978-981-15-4397-5 (eBook)
https://doi.org/10.1007/978-981-15-4397-5

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Dedicated
to
My sweet daughter Pragati and beloved wife Shyamali

Preface

This book entitled *Reversible Steganography and Authentication via Transform Encoding* contains fourteen chapters. Out of fourteen chapters, Chap. 1 contains the introductory remarks. This chapter reflects the aspects of introductory literature about cryptography, steganography, authentication and related issues in various domains. The genesis of steganography and authentication starting from the ancient era to the digital era is addressed in this chapter. State-of-the-art neural cryptography, tuning of neural machine, is also given in this chapter.

In Chap. 2, the state-of-the-art literature survey in respect of reversible steganography and authentication has been outlined. The survey of the literature from 2005 to 2019 is incorporated.

In Chap. 3, the details about steganography and authentication in different domains, e.g., spatial, spectral and composite domains, have been explained. The explanations are substantiated by examples in terms of fabrication and extraction in detail. Aspects of steganographic applications in spatial domain, spectral domain and also in composite domain have been discussed in detail.

In Chap. 4, DFT-based reversible encoding with the formula for FDT and IDFT has been discussed. The problem of transformation for the whole image matrix is addressed. To reduce the computational complexity, the reduction in generalized equation of DFT and IDFT into 2×2 window-based computation has been done and the generalized equation is converted to a simpler form. The reversible encoding for application of steganography and authentication is also given. Detailed computational aspects of this reversible process are highlighted. Steganographic applications based on these reversible computations along with its process of authentication are given.

In Chap. 5, DCT-based reversible computation and image matrix-based transform computation are incorporated. Sliding window using 2×2 size to compute reversible computation and reduction in generalized DCT equation into a simpler form based on small size windows is the main focus of this chapter. Steganographic applications for embedding and extraction in real components of transform coefficients using LSB and hash functions have been elaborated. The process of authentication and its applications in various real fields are also given.

In Chap. 6, wavelet transformation is discussed in detail. This book has been emphasized on Haar wavelets for reversible computations. Reversible computations in smaller size windows are the prime focus of this chapter. The process of embedding and authentication is discussed in detail. Embedding and extraction of binary strings for authentication and invisible communication along with related applications of the same for various real-time applications are given.

Z-transformation-based reversible encoding is done in Chap. 7. Detailed computation of Z-transform has been addressed in this chapter. Computational aspects of Z-transform with varying ROC have been taken care of in detail. Embedding of binary bits in real components in transform coefficients of Z-transform is the main focus area for embedding and authentication. Extraction of embedded bits from the embedded image is also elaborated in detail along with examples for reversibility to ensure authentication. This chapter also addresses the higher ROC of Z-transform with embedding and extraction to/from imaginary components of transformed coefficients using different values of r.

Reversible transform encoding via discrete binomial transform has been embodied in Chap. 8. Here, the reversibility of computations has also been done taking 2×2 subimages. Detailed algorithmic approach with 1.5 bpB embedding payload has been given in detail with the implementation of results.

Computation of Grouplet transformation for reversible computation based on its rotation and reflection properties has been done in Chap. 9. Various dihedral groups like D_3, D_4, D_5 … D_{10} are used for computation of reversibility along with implementation in each case. Embedding and extraction of information into transform coefficients of various G-Lets based on its reflection and rotation properties are given in detail. Process of authentication based on various G-Let functions is given along with explicit examples. A complete algorithm for embedding and extraction with implementation results is given in this chapter.

The utility of nonlinear dynamics in steganography and authentications is discussed in Chap. 10. Use of various logistic maps and computations of series of real values using various logistic maps and encoding it into binary sequence and embedding this binary sequence into various transform coefficients of different transformations is the primary goal of this chapter. Decoding of binary sequence at the receiving end using the logistic equation has been given. Some glimpse of testing of binary sequence for their randomness in terms of Monobit, Serial and Poker tests is given. Optimization of seeds for the generation of the better pseudorandom sequence using various evolutionary algorithms such as genetic algorithm has also been discussed.

In Chap. 11, various matrices to evaluate the performances of various reversible transform techniques in terms of embedding, quality of embedding, image fidelity (IF), PSNR, SSIM, standard deviations (SD), etc. are discussed in detail. NIST test suit containing 15 tests are also discussed.

In Chap. 12, implementation issues of all reversible transform encodings, embedding and extraction along with results are discussed in detail. Comparative study of various transformations in terms of reversible encoding and extraction is also given.

An analysis in terms of performances with respect to embedding, extraction along with various quality factors is the main focus of this analysis.

Concluding remarks on transform encoding along with their limitations, possibilities and concern are outlined in Chap. 13. Chapter 14 addresses the future scope of this study.

I would like to express my sincere gratitude to the Department of Computer Science and Engineering and the University of Kalyani for encouraging me continuously to complete such massive work.

I shall remain grateful to my scholars who encouraged me a lot and helped me in preparing this manuscript. Particularly Dr. Arindam Sarkar, Sujit Das, Dr. Amrita Khamrui, Khondeker Lutful Hassan, Dr. Parthajit Roy, Dr. Kousik Dasgupta, Rajeev Chatterjee, Sadhu Prasad Kar, Debarpita Santra, Dr. Somnath Mukhopadhyay, Dr. Rajdeep Chakraborty, Dr. Madhumita Sengupta, Dr. Uttam Mondal and Dr. Utpal Nandi. I would also like to express my sincere gratitude to Dr. Biswapati Jana of Vidyasagar University for his assistance.

I am grateful to Mr. Ashes Saha, Senior Assistant of IQAC and other staff members of IQAC, University of Kalyani, for extending their help and cooperation in various stages of preparing the manuscript.

My dearest daughter Pragati and my beloved wife Shyamali who never questioned me during my study through my life except extending their love and affection.

This book is the outcome of the research of the last 15 years with all of my beloved scholars and students without whom I could not able to complete this book.

My main source of inspiration of writing this book is Mr. Aninda Bose of Springer who encouraged me to write such a book three years back. Thanks to Aninda Bose for his constant encouragement so that I could complete this book. I am always blessed by my teacher Prof. Atal Choudhuri, Vice Chancellor, BSSUT, Odisha, India. My sincere regards to him. I always received enormous encouragement from Dr. Aloke K. Gupta and Mrs. Chayya Gupta during the preparation of this book. Their positive suggestions always inspired me a lot.

This book is basically for the undergraduate and postgraduate students and for the research scholars who will be inspired from this literature for their work and research in the field of invisible communication. Practicing engineers will also find this book helpful for them.

Hope this book will serve as very good material in the domain of security and authentication through invisible communication.

Kalyani, India
February 2020

Jyotsna Kumar Mandal

Contents

About the Author

Jyotsna Kumar Mandal received his M.Tech. in Computer Science from the University of Calcutta in 1987, and his Ph.D. (Engineering) in Computer Science and Engineering from Jadavpur University in 2000. He is a Professor of Computer Science & Engineering, and was Dean of the Faculty of Engineering, Technology & Management at Kalyani University from 2008–2012. He has also served as the Director of IQAC at Kalyani University; Chairman of CIRM; a Professor of Computer Applications at Kalyani Government Engineering College; Associate Professor and Lecturer of Computer Science at North Bengal University; and a Lecturer at NERIST, Itanagar India. He has 33 years of teaching and research experience in the field of coding theory, data and network security and authentication, remote sensing & GIS-based applications, data compression, error correction, visual cryptography and steganography. He is Guest Editor of Springer's MST Journal (SCI indexed). He has published more than 400 research articles in national and international journals. He has also published 7 books, organized 34 international conferences. In addition, he has served as a Corresponding Editor and Volume Editor for leading international publishing houses. He received the SikshaRatna Award for outstanding teaching from the Government of West Bengal, India in 2018; Vidyasagar Award from the International Society for Science Technology and Management at the Fifth International Conference on Computing, Communication and Sensor Networks 2016; Chapter Patron Award, CSI Kolkata Chapter at the CSI Annual Convention in 2014; Bharat Jyoti Award for meritorious services, outstanding performance and remarkable role in the field of Computer Science & Engineering in 2012 from International Friendship Society (IIFS), New Delhi; and the A. M. Bose Memorial Silver Medal and Kali Prasanna Dasgupta Memorial Silver Medal from Jadavpur University India.