Novel Research and Development Approaches in Heterogeneous Systems and Algorithms

Santanu Koley
Haldia Institute of Technology, India

Subhabrata Barman
Haldia Institute of Technology, India

Subhankar Joardar
Haldia Institute of Technology, India

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

A volume in the Advances in Systems Analysis, Software Engineering, and High Performance Computing (ASASEHPC) Book Series

Copyrighted material

Table of Contents

Foreword xv

Preface xvi

Acknowledgment xx

Chapter 1
Comparative Study of Some Nature-Inspired Meta-Heuristics for Task Scheduling in a Computational Grid System 1
Tarun Kumar Ghosh, Haldia Institute of Technology, India
Krishna Gopal Dhal, Midnapore College, India
Sanjoy Das, University of Kalyani, India

Chapter 2
Wavelet Energy-Based Adaptive Retinex Algorithm for Low Light Mobile Video Enhancement 16
Vishalakshi G. R., Dayananda Sagar College of Engineering, India
Gopala Krishna, SJB Institute of Technology, India
Hanumantha Raju, BMS Institute of Technology and Management, India

Chapter 3
Identification and Segmentation of Medical Images by Using Marker-Controlled Watershed Transformation Algorithm, XAI, and ML 40
Tahamina Yesmin, Haldia Institute of Management, India
Pinaki Pratim Acharjya, Haldia Institute of Technology, India

Chapter 4
Cataract Classification and Gradation From Retinal Fundus Image Using Ensemble Learning Algorithm 59
Moumita Sahoo, Haldia Institute of Technology, India
Somak Karan, Haldia Institute of Technology, India
Soumya Roy, Haldia Institute of Technology, India

Chapter 5
Study of the Image Segmentation Process Using the Optimized U-Net Model for Drone-Captured Images 81

Copyrighted material

Gunjan Mukherjee, Brainware University, India
Arpitam Chatterjee, Jadavpur University, India
Bipan Tudu, Jadavpur University, India
Sourav Paul, Ramakrishna Mission Vidyamandira, India & Swami Vivekananda Research Centre, India

Chapter 6
Distributed Technologies and Consensus Algorithms for Blockchain 100
Cynthia Jayapal, Kumaraguru College of Technology, India
Clement Sudhahar, Karunya Institute of Technology and Sciences (Deemed), India

Chapter 7
A Novel Steganography Approach Using S-CycleGAN With an Improvement of Loss Function 123
Minakshi Sarkar, Haldia Institute of Technology, India
Indrajit Banerjee, Indian Institute of Engineering Science and Technology, Shibpur, India
Tarun Kumar Ghosh, Haldia Institute of Technology, India
Anirban Samanta, Haldia Institute of Technology, India
Anirban Sarkar, Guru Nanak Institute of technology, India

Chapter 8
AI-Based DBMS Controlled Speech Recognition Model for Some Common Computing Commands 143
Mrinmoy Sen, Haldia Institute of Technology, India
Sunanda Jana, Haldia Institute of Technology, India
Swarnajit Bhattacharya, Haldia Institute of Technology, India
Gitika Maity, Dr. Meghnad Saha Institute of Technology, India

Chapter 9
MEDA-Based Biochips: Proposed New Structural Testing Techniques for Fault Detection 155
Priyatosh Jana, Haldia Institute of Technology, India
Pranab Roy, Institute of Engineering and Technology, J. K. Laxmipat University, Jaipur, India
Sarit Chakraborty, Government College of Engineering and Leather Technology, India
Tanmoy Biswas, Shyamaprasad College, India
Soumen Ghosh, Haldia Institute of Technology, India

Chapter 10
A Radical Image Steganography Method Predicated on Intensity and Edge Detection..... 173
Abhijit Sarkar, Haldia Institute of Technology, India
Sabyasachi Samanta, Haldia Institute of Technology, India

Chapter 11
Secure Cryptography Using Chaotic Algorithm..... 191
Uday Kumar Banerjee, Dr. B.C. Roy Engineering College, Durgapur, India
Anup Kumar Das, Dr. B.C. Roy Engineering College, Durgapur, India
Rajdeep Ray, Dr. B.C. Roy Engineering College, Durgapur, India

Copyrighted material

Chandan Koner, Dr. B.C. Roy Engineering College, Durgapur, India

Chapter 12
An Image Steganography Approach Using Arnold Transformation 217
Solanki Pattanayak, Haldia Institute of Management, India
Sabyasachi Samanta, Haldia Institute of Technology, India
Dipankar Dey, Global Institute of Science and Technology, India
Abhijit Sarkar, Haldia Institute of Technology, India
Souvik Bhattacharyya, University Institute of Technology, Burdwan, India

Chapter 13
Machine Learning-Based Algorithms Towards Crop Recommendation Systems..... 236
Soumya Roy, Haldia Institute of Technology, India
Yuvika Vatsa, Haldia Institute of Technology, India
Moumita Sahoo, Haldia Institute of Technology, India
Somak Karan, Haldia Institute of Technology, India

Chapter 14
House Rent Prediction Using Ensemble-Based Regression With Real-Time Data..... 258
Kuntal Mukherjee, Haldia Institute of Technology, India
Syed Saif Ahmed, Haldia Institute of Technology, India
Mohammad Aasif, Haldia Institute of Technology, India
Sumana Kundu, Dr. B.C. Roy Engineering College, India
Soumen Ghosh, Haldia Institute of Technology, India

Chapter 15
A Survey on Energy-Efficient Routing in Wireless Sensor Networks Using Machine Learning Algorithms 272
Prasenjit Dey, Coochbehar Government Engineering College, India
Arnab Gain, Coochbehar Government Engineering College, India

Compilation of References 292

About the Contributors 314

Index..... 321

Copyrighted material

out with specified layout dimensions and variable droplet size.

Chapter 10

A Radical Image Steganography Method Predicated on Intensity and Edge Detection 173
Abhijit Sarkar, Haldia Institute of Technology, India
Sabyasachi Samanta, Haldia Institute of Technology, India

The internet has grown to be widely used by billions of individuals in our digital age. The internet is required for a variety of platforms, online apps, and standalone applications. Numerous methods, including cryptography, encryption/decryption, and data concealment algorithms, are developed for this goal. However, the employment of these methods was not very secure, making it simple for hackers to get the secret message. A new method called "steganography" was developed to offer the highest level of protection for sensitive data. Steganography's primary goal is to conceal the presence of concealed messages. Additionally, it seeks out concealed messages using factors like the kind of embedding method, the message's length, its content, or the carrier's secret key. At this point in the chapter, a single bit of data has been embedded into edge-based pixel positions with arbitrary bit positions. The authors have compared their method to three standard edge detection algorithms for a more comprehensive assessment. Different statistical measures also have been made for the uniqueness of the technique.

Chapter 11

Secure Cryptography Using Chaotic Algorithm 191
Uday Kumar Banerjee, Dr. B.C. Roy Engineering College, Durgapur, India
Anup Kumar Das, Dr. B.C. Roy Engineering College, Durgapur, India
Rajdeep Ray, Dr. B.C. Roy Engineering College, Durgapur, India
Chandan Koner, Dr. B.C. Roy Engineering College, Durgapur, India

A chaotic cryptographic method and bit shuffle methodology for image encryption and decoding have both been suggested. In order to evaluate the encryption's effectiveness and determine whether it met the desired standard, a number of performance analysis tools were also used. These included the number of pixel change rate (NPCR), the unified average changing intensity (UACI), the entropy analysis, which is a component of an encryption scheme that shows how random the image is, and the correlation coefficient. These results reveal the safety of the suggested cryptographic technique.

Chapter 12

An Image Steganography Approach Using Arnold Transformation 217
Solanki Pattanayak, Haldia Institute of Management, India
Sabyasachi Samanta, Haldia Institute of Technology, India
Dipankar Dey, Global Institute of Science and Technology, India
Abhijit Sarkar, Haldia Institute of Technology, India
Souvik Bhattacharyya, University Institute of Technology, Burdwan, India

Sleuthing images that conceal information has continuously been a stimulating and difficult problem in cyber security. Finding hidden data in nursing image is called steganalysis. In this chapter, the authors explore the method employed in the study. The investigational results are have included followed by a discussion with prospect analysis. Several 2×2 blocks are recycled to implant the data bits within the stego-image, and using the Arnold Map, four quadrants of the pixels of each block is selected to embed the data in nonlinear bit position. Different measures with the change of BPP (bits per pixel) are also

Copyrighted material

Chapter 11
Secure Cryptography Using Chaotic Algorithm

Uday Kumar Banerjee
Dr. B.C. Roy Engineering College, Durgapur, India

Anup Kumar Das
Dr. B.C. Roy Engineering College, Durgapur, India

Rajdeep Ray
Dr. B.C. Roy Engineering College, Durgapur, India

Chandan Koner
Dr. B.C. Roy Engineering College, Durgapur, India

ABSTRACT

A chaotic cryptographic method and bit shuffle methodology for image encryption and decoding have both been suggested. In order to evaluate the encryption's effectiveness and determine whether it met the desired standard, a number of performance analysis tools were also used. These included the number of pixel change rate (NPCR), the unified average changing intensity (UACI), the entropy analysis, which is a component of an encryption scheme that shows how random the image is, and the correlation coefficient. These results reveal the safety of the suggested cryptographic technique.

INTRODUCTION

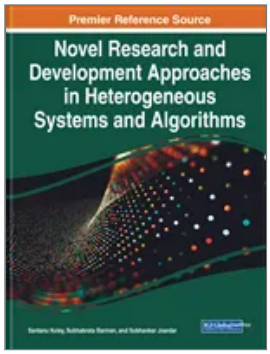
Secure Cryptography: An Overview

Security is not only a word; it is a very important aspect in today's world especially for communication and data or information transmission. As the increase of online transmission not for only simple information but for economic data, the protection of this information becomes very crucial. To do so security techniques like cryptography becomes more and more important as well before. Information security has emerged as the most fascinating and interesting technological sector in the modern world in the informa-

DOI: 10.4018/978-1-6684-7524-9.ch011

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Copyrighted material



Secure Cryptography Using Chaotic Algorithm

Uday Kumar Banerjee, Anup Kumar Das, Rajdeep Ray, Chandan Koner

Source Title: Novel Research and Development Approaches in Heterogeneous Systems and Algorithms (/book/novel-research-development-approaches-heterogeneous/308298)

Copyright: © 2023

Pages: 26

DOI: 10.4018/978-1-6684-7524-9.ch011

OnDemand:
(Individual Chapters) $37.50

() Available

Current Special Offers

Abstract

A chaotic cryptographic method and bit shuffle methodology for image encryption and decoding have both been suggested. In order to evaluate the encryption's effectiveness and determine whether it met the desired standard, a number of performance analysis tools were also used. These included the number of pixel change rate (NPCR), the unified average changing intensity (UACI), the entropy analysis, which is a component of an encryption scheme that shows how random the image is, and the correlation coefficient. These results reveal the safety of the suggested cryptographic technique.

Chapter Preview

Top

Introduction

Secure Cryptography: An Overview

Security is not only a word; it is a very important aspect in today’s world especially for communication and data or information transmission. As the increase of online transmission not for only simple information but for economic data, the protection of this information becomes very crucial. To do so security techniques like cryptography becomes more and more important as well before. Information security has emerged as the most fascinating and interesting technological sector in the modern world in the information age as a result of widespread computerization and their interaction via networks. Confidentiality, authentication, integrity, non-repudiation, access control, and availability are the guiding principles of every security mechanism. A crucial component of secure communications is cryptography, which was designed with the intention of providing secret communication since it shields information transmission from the impact of adversaries. The concept of security and its characteristics have come to the forefront due to the overabundance of digital content and the ossification of internet technology. For instance, telemedicine provides interactive healthcare in far-off places while transmitting patient health information and imaging data over an insecure connection. Second, the satellite image provides time-specific data that is useful for a variety of purposes, including environmental protection, meteorology, defence and remote sensing. The government, private detectives and criminal organizations may now closely monitor people and public behavior online thanks to the development of surveillance technology. The security of picture data during transmission and storage is a key factor in determining the quality of the service in the aforementioned applications. The word, cryptography came from ancient Greek which contains two words: “kryptos” means “hidden” or “vault” and “graphy” means “writing” or “study”. Cryptography is the study of secure communication between the sender and the receiver and it allow viewing the message to intended recipient without intervention of the adversary element.

The history of cryptography is really old. At the time of ancient Egyptian civilization around 2000 B.C. the hieroglyphic language makes complex by using cryptography picture and only the elite community knew the meaning then. At the time of Julius Caesar at 100 B.C. to 44 B.C. the modern-day cipher concept was found. Julius Caesar did not want that the message should read by the messenger or anyone so he changes the original letter by its next third letter and make a coded form of message which can only be understood by those who knew the decoding process. The modern day’s techniques come along lot of paths and it becomes a strong mechanism to protect information. Nowadays the different mathematical concepts with the help of different rule base calculation are used which are called cryptographic algorithm. By applying these algorithms different text, image, audio, video or other type of files can be encoded such a way that the original meaning of this file is hidden in a masking and cannot be understood easily.