DOWNLOAD FORENSICS OF IMAGE TAMPERING BASED ON THE CONSISTENCY OF

Forensic Analysis of Digital Image Tampering

The use of digital photography has increased over the past few years, a trend which opens the door for new and creative ways to forge images. The manipulation of images through forgery influences the perception an observer has of the depicted scene, potentially resulting in ill consequences if created with malicious intentions. This poses a need to verify the authenticity of images originating from unknown sources in absence of any prior digital watermarking or authentication technique. This research explores the holes left by existing research; specifically, the ability to detect image forgeries created using multiple image sources and specialized methods tailored to the popular JPEG image format. In an effort to meet these goals, this thesis presents four methods to detect image tampering based on fundamental image attributes common to any forgery. These include discrepancies in 1) lighting and 2) brightness levels, 3) underlying edge inconsistencies, and 4) anomalies in JPEG compression blocks. Overall, these methods proved encouraging in detecting image forgeries with an observed accuracy of 60% in a completely blind experiment containing a mixture of 15 authentic and forged images.

Digital Image Forensics

This book discusses blind investigation and recovery of digital evidence left behind on digital devices, primarily for the purpose of tracing cybercrime sources and criminals. It presents an overview of the challenges of digital image forensics, with a specific focus on two of the most common forensic problems. The first part of the book addresses image source investigation, which involves mapping an image back to its camera source to facilitate investigating and tracing the source of a crime. The second part of the book focuses on image-forgery detection, primarily focusing on “copy-move forgery” in digital images, and presenting effective solutions to copy-move forgery detection with an emphasis on additional related challenges such as blur-invariance, similar genuine object identification, etc. The book concludes with future research directions, including counter forensics. With the necessary mathematical information in every chapter, the book serves as a useful reference resource for researchers and professionals alike. In addition, it can also be used as a supplementary text for upper-undergraduate and graduate-level courses on “Digital Image Processing”, “Information Security”, “Machine Learning”, “Computer Vision” and “Multimedia Security and Forensics”.

Image Forensics Based on Reverse Engineering

Today with the advent of low-cost imaging devices, such as smart phones, digital cameras and surveillance video systems, digital images become quite common in our everyday life. People tend to believe the scene they have seen, even if the scene is presented in the form of an digital image, as a proverb says, 'Seeing is believing'. However are those images really trustworthy as people have thought? In this mul- timedia world, with the wide-spread availability of those sophisticated image-editing software, such as PhotoShop and Gimp, it is easy for people to modify images to hide some information or to add a non-existing scene. These manipulations usually leave no visual clues in the tampered image. As a result, the above proverb no longer holds. To address this problem, `digital image forensics' was developed. Digital image forensics aims to verify the authentication and integrity of a digital image, without the knowledge of any prior information

about the questioned image. It mainly includes two tasks: to determine whether an image is authentic and to identify the source camera of an image. What distinguishes the original image from the manipulated image is the acqui- sition process inside the digital camera, which should naturally be the only reliable solution to conquer this problem. In this work, we analyze some key operations along the image acquisition pipeline, and use the cracked information to perform forensic tasks. The contributions can be grouped into three categories: white balance(WB), color demosaicking and defocus aberration blurs. The thesis starts with exposing which white balance algorithm has been applied in the imaging pipeline. The theoretical basis lies on the fact that, given an image, applying the same white balance operation again would not change the image. With the proposed approach, the average accuracy of source camera identification is 99.3% for 5 cameras of different brands, 98.6% for 17 cameras of different models, and 98.5% for 15 cameras equally from 3 models. This is the first time white balance has been used in source camera identification, and it leads to an almost perfect result. Most commercial cameras have only one CCD/CMOS sensor, which produces just a gray scale image. In order to get a colored one, cameras apply a process called demosaicking. This thesis estimates the model and parameters of the demosaicking process to detect forgery. With this method, we can identify which part of the image that is inconsistent with the rest, in the form of their corresponding estimation error. This is the first time that the copy-move area from another image can be exposed using demosaicking. The third part of this thesis aims at integrity verification using image defocus blur. We can calculate the image defocus aberration, and estimate its depth information. Also from defocus aberration consistency, we can determine whether an image has been altered. This is the first time defocus blur has been used to perform forensic task. The proposed method increases the average accuracy of splicing detection to 81%, while the best existing published result using the same database is only 68.8%.

Tampering Detection Based on JPEG Analysis for Image Forensics

Photographic imagery has come a long way from the pinhole cameras of the nineteenth century. Digital imagery, and its applications, develops in tandem with contemporary society’s sophisticated literacy of this subtle medium. This book examines the ways in which digital images have become ever more ubiquitous as legal and medical evidence, just as they have become our primary source of news and have replaced paper-based financial documentation. Crucially, the contributions also analyze the very profound problems which have arisen alongside the digital image, issues of veracity and progeny that demand systematic and detailed response: It looks real, but is it? What camera captured it? Has it been doctored or subtly altered? Attempting to provide answers to these slippery issues, the book covers how digital images are created, processed and stored before moving on to set out the latest techniques for forensically examining images, and finally addressing practical issues such as courtroom admissibility. In an environment where even novice users can alter digital media, this authoritative publication will do much so stabilize public trust in these real, yet vastly flexible, images of the world around us.

Digital Image Forensics

This book constitutes the refereed proceedings of the 10th International Conference on Information Systems Security, ICISS 2014, held in Hyderabad, India, in December 2014. The 20 revised full papers and 5 short papers presented together with 3 invited papers were carefully reviewed and selected from 129 submissions. The papers address the following topics: security inferences; security policies; security user interfaces; security attacks; malware detection; forensics; and location based security services.

Information Systems Security

This book constitutes the thoroughly refereed post-proceedings of the 11th International Workshop on Digital-Forensics and Watermarking, IWDW 2012, held in Shanghai, China, during October/November 2012. The 42 revised papers (27 oral and 15 poster papers) were carefully reviewed and selected from 70 submissions. The papers are organized in topical sections on steganography and steganalysis; watermarking and copyright protection; forensics and anti-forensics; reversible data hiding; fingerprinting and

authentication; visual cryptography.

Digital-Forensics and Watermarking

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book’s 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students’ understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.

Introductory Computer Forensics

This book presents a detailed study of key points and block-based copy-move forgery detection techniques with a critical discussion about their pros and cons. It also highlights the directions for further development in image forgery detection. The book includes various publicly available standard image copy-move forgery datasets that are experimentally analyzed and presented with complete descriptions. Five different image copy-move forgery detection techniques are implemented to overcome the limitations of existing copy-move forgery detection techniques. The key focus of work is to reduce the computational time without adversely affecting the efficiency of these techniques. In addition, these techniques are also robust to geometric transformation attacks like rotation, scaling, or both.

Image Tampering Detection for Forensics Applications

In this thesis, we propose several new approaches for image forgery detection. In the first approach, we use inconsistencies in an imaging trace called lateral chromatic aberration (LCA) to detect forged image regions. Lateral chromatic aberration arises due to the wavelength dependence in the refraction angle of light in camera lenses, which causes a predictable misalignment of an image's color channels. During a splicing forgery, inconsistencies in the image's LCA are inherently introduced. To detect forgeries, we first propose a statistical model that captures the inconsistency between global and local estimates of LCA. We then use this model to pose forgery detection as a hypothesis testing problem and derive an optimal detection statistic. We conduct a series of experiments that demonstrate our proposed method significantly outperforms prior art. We additionally propose a new method to anti-forensically remove these inconsistencies to avoid detection, as well as a new anti-forensic counter method that detects this anti-forensic attack. A drawback of many existing deep-learning based forensic approaches is that they assume a closed set of classes. In our second approach, we propose a method to measure forensic similarity between two image patches that is effective on unknown classes (i.e. an open set). We show that this approach is useful for splicing localization and detection. In our forensic similarity approach, we first train a convolutional neural network (CNN) to output generalized features which encode camera model and editing information of an image patch. Then, we learn a similarity measure that maps pairs of these features to a score that quantifies whether the two image patches have the same or different forensic traces. We experimentally show that this approach can determine whether two image patches were captured by the same or different camera model, processed by the same or different manipulation, and even same or different manipulation parameter. Finally, we propose a graph-based method to more accurately perform forgery detection and localization on tampered images. To do this, we propose an

abstract, graph-based representation of an image, which we call the Forensic Graph Representation. In this representation, small image patches are represented by graph vertices with edges assigned according the the forensic similarity between image patches. Localized tampering introduces unique structure into this graph, which align with a concept referred to as ``communities\" in graph-theory literature. These communities correspond to the tampered and unaltered regions in the image, and are each a sub-set of vertices that contain high weight edges within the community, and low weight edges across communities. As a result, forgery is performed by identifying whether multiple communities exist in this graph representation, and forgery localization is performed by partitioning the communities. We experimentally show that this approach outperforms naive implementations that do not consider this community structure, including prior art.

Image Copy-Move Forgery Detection

Imaging for Forensics and Security: From Theory to Practice provides a detailed analysis of new imaging and pattern recognition techniques for the understanding and deployment of biometrics and forensic techniques as practical solutions to increase security. It contains a collection of the recent advances in the technology ranging from theory, design, and implementation to performance evaluation of biometric and forensic systems. This book also contains new methods such as the multiscale approach, directional filter bank, and wavelet maxima for the development of practical solutions to biometric problems. The book introduces a new forensic system based on shoeprint imagery with advanced techniques for use in forensics applications. It also presents the concept of protecting the originality of biometric images stored in databases against intentional and unintentional attacks and fraud detection data in order to further increase the security.

Image Forgery Detection Using Deep Learning and Signal Processing Methods

This book constitutes the revised post-conference proceedings of the 15th International Workshop on Digital Forensics and Watermarking, IWDW 2016, held in Beijing, China, in September 2016. The 45 papers presented in this volume were carefully reviewed and selected from 70 submissions. The contributions are organized in topical sections on digital forensics, visual cryptography, reversible data hiding, and steganography and steganalysis.

Imaging for Forensics and Security

This book constitutes the proceedings of the Second International Conference on Network Computing and Information Security, NCIS 2012, held in Shanghai, China, in December 2012. The 104 revised papers presented in this volume were carefully reviewed and selected from 517 submissions. They are organized in topical sections named: applications of cryptography; authentication and non-repudiation; cloud computing; communication and information systems; design and analysis of cryptographic algorithms; information hiding and watermarking; intelligent networked systems; multimedia computing and intelligence; network and wireless network security; network communication; parallel and distributed systems; security modeling and architectures; sensor network; signal and information processing; virtualization techniques and applications; and wireless network.

Digital Forensics and Watermarking

This book constitutes the refereed proceedings of the 16th International Workshop on Digital Forensics and Watermarking, IWDW 2017, held in Magdeburg, Germany, in August 2017. The 30 papers presented in this volume were carefully reviewed and selected from 48 submissions. The contributions are covering the state-of-the-art theoretical and practical developments in the fields of digital watermarking, steganography and steganalysis, forensics and anti-forensics, visual cryptography, and other multimedia-related security issues. Also included are the papers on two special sessions on biometric image tampering detection and on emerging threats of criminal use of information hiding : usage scenarios and detection approaches.

Network Computing and Information Security

As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

Adversarial Multimedia Forensics

This open access book provides the first comprehensive collection of studies dealing with the hot topic of digital face manipulation such as DeepFakes, Face Morphing, or Reenactment. It combines the research fields of biometrics and media forensics including contributions from academia and industry. Appealing to a broad readership, introductory chapters provide a comprehensive overview of the topic, which address readers wishing to gain a brief overview of the state-of-the-art. Subsequent chapters, which delve deeper into various research challenges, are oriented towards advanced readers. Moreover, the book provides a good starting point for young researchers as well as a reference guide pointing at further literature. Hence, the primary readership is academic institutions and industry currently involved in digital face manipulation and detection. The book could easily be used as a recommended text for courses in image processing, machine learning, media forensics, biometrics, and the general security area.

Copy-move Image Forgery Detection Scheme Based on New Texture Descriptor Utilising Graphical Processing Unit

Security is a major concern in an increasingly multimedia-defined universe where the Internet serves as an indispensable resource for information and entertainment. Digital Rights Management (DRM) is the technology by which network systems protect and provide access to critical and time-sensitive copyrighted material and/or personal information. This book equips savvy technology professionals and their aspiring collegiate protégés with the latest technologies, strategies and methodologies needed to successfully thwart off those who thrive on security holes and weaknesses. Filled with sample application scenarios and algorithms, this book provides an in-depth examination of present and future field technologies including encryption, authentication, copy control, tagging, tracing, conditional access and media identification. The authors present a diversified blend of theory and practice and focus on the constantly changing developments in multimedia applications thus providing an admirably comprehensive book. * Discusses state-of-the-art multimedia authentication and fingerprinting techniques * Presents several practical methodologies from industry, including broadcast encryption, digital media forensics and 3D mesh watermarking * Focuses on the need for security in multimedia applications found on computer networks, cell phones and emerging mobile computing devices

Digital Forensics and Watermarking

The two-volume set LNCS 13833 and LNCS 13834 constitutes the proceedings of the 29th International

Conference on MultiMedia Modeling, MMM 2023, which took place in Bergen, Norway, during January 9-12, 2023. The 86 papers presented in these proceedings were carefully reviewed and selected from a total of 267 submissions. They focus on topics related to multimedia content analysis; multimedia signal processing and communications; and multimedia applications and services.

Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice

This book constitutes refereed proceedings of the International Conference on Security, Privacy and Data Analytics, ISPDA 2022. The volume covers topics, including big data and analytics, cloud security and privacy, data intelligence, hardware security, network security, blockchain technology and distributed ledger, machine learning for security, and many others. The volume includes novel contributions and the latest developments from researchers across industry and academia working in security, privacy, and data analytics from technological and social perspectives. This book will emerge as a valuable reference for researchers, instructors, students, scientists, engineers, managers, and industry practitioners across the globe.

Handbook of Digital Face Manipulation and Detection

The Volume of “Advances in Machine Learning and Data Science - Recent Achievements and Research Directives” constitutes the proceedings of First International Conference on Latest Advances in Machine Learning and Data Science (LAMDA 2017). The 37 regular papers presented in this volume were carefully reviewed and selected from 123 submissions. These days we find many computer programs that exhibit various useful learning methods and commercial applications. Goal of machine learning is to develop computer programs that can learn from experience. Machine learning involves knowledge from various disciplines like, statistics, information theory, artificial intelligence, computational complexity, cognitive science and biology. For problems like handwriting recognition, algorithms that are based on machine learning out perform all other approaches. Both machine learning and data science are interrelated. Data science is an umbrella term to be used for techniques that clean data and extract useful information from data. In field of data science, machine learning algorithms are used frequently to identify valuable knowledge from commercial databases containing records of different industries, financial transactions, medical records, etc. The main objective of this book is to provide an overview on latest advancements in the field of machine learning and data science, with solutions to problems in field of image, video, data and graph processing, pattern recognition, data structuring, data clustering, pattern mining, association rule based approaches, feature extraction techniques, neural networks, bio inspired learning and various machine learning algorithms.

Multimedia Security Technologies for Digital Rights Management

This volume contains articles written by leading researchers in the fields of algorithms, architectures, and information systems security. The first five chapters address several challenging geometric problems and related algorithms. These topics have major applications in pattern recognition, image analysis, digital geometry, surface reconstruction, computer vision and in robotics. The next five chapters focus on various optimization issues in VLSI design and test architectures, and in wireless networks. The last six chapters comprise scholarly articles on information systems security covering privacy issues, access control, enterprise and network security, and digital image forensics.

MultiMedia Modeling

This book constitutes the refereed proceedings of the 12th International Conference on Information Hiding, IH 2010, held in Calgary, AB, Canada, in June 2010. The 18 revised full papers presented were carefully reviewed and selected from 39 submissions.

Security, Privacy and Data Analytics

Unleashing the Art of Digital Forensics is intended to describe and explain the steps taken during a forensic examination, with the intent of making the reader aware of the constraints and considerations that apply during a forensic examination in law enforcement and in the private sector. Key Features: • Discusses the recent advancements in Digital Forensics and Cybersecurity • Reviews detailed applications of Digital Forensics for real-life problems • Addresses the challenges related to implementation of Digital Forensics and Anti-Forensic approaches • Includes case studies that will be helpful for researchers • Offers both quantitative and qualitative research articles, conceptual papers, review papers, etc. • Identifies the future scope of research in the field of Digital Forensics and Cybersecurity. This book is aimed primarily at and will be beneficial to graduates, postgraduates, and researchers in Digital Forensics and Cybersecurity.

Advances in Machine Learning and Data Science

This book constitutes the refereed proceedings of the 10th International Conference on Advances in Brain Inspired Cognitive Systems, BICS 2019, held in Guangzhou, China, in July 2019. The 57 papers presented in this volume were carefully reviewed and selected from 129 submissions. The papers are organized in topical sections named: neural computation; biologically inspired systems; image recognition: detection, tracking and classification; and data analysis and natural language processing.

Algorithms, Architectures and Information Systems Security

The Human Machine Interaction in the Digital Era (ICHMIDE) 2023 conference aims to address the main issues of concern in the design issues with a particular emphasis on the design and development of interfaces for autonomous robots. Its main objective is to provide an international forum for the dissemination and exchange of up-to-date scientific information on research related to integrated human/machine systems at multiple scales, and includes areas such as human/machine interaction, engineering mathematical models, assistive technologies, system modelling, design, testing and validation. The organization of ICHMS is based on the following Track types: Smart Applications for Digital Era, Computational Mathematical and Electronics, Intelligent Systems in Security and Communication Technologies, Technological Interventions using AI and Machine Learning, Applied Science, and IoT Techniques for Industries.

Information Hiding

This volume constitutes the proceedings of the 19th International Workshop on Digital Forensics and Watermarking, IWDW 2020, held in Melbourne, VIC, Australia, in November 2020. The 20 full papers in this volume were carefully reviewed and selected from 43 submissions. They cover topics such as: novel research, development and application of digital watermarking and forensics techniques for multimedia security.

Unleashing the Art of Digital Forensics

This book constitutes the refereed proceedings of seven workshops held at the 18th International Conference on Image Analysis and Processing, ICIAP 2015, in Genoa, Italy, in September 2015: International Workshop on Recent Advances in Digital Security: Biometrics and Forensics, BioFor 2015; International Workshop on Color in Texture and Material Recognition, CTMR 2015; International Workshop on Medical Imaging in Rheumatology: Advanced applications for the analysis of in ammation and damage in the rheumatoid Joint, RHEUMA 2015; International Workshop on Image-Based Smart City Application, ISCA 2015; International Workshop on Multimedia Assisted Dietary Management, MADiMa 2015; International Workshop on Scene Background Modeling and initialization, SBMI 2015; and International Workshop on Image and Video Processing for Quality of Multimedia Experience, QoEM 2015.

Proceedings of Fifth International Conference on Computing, Communications, and Cyber-Security

The 10-volume set LNCS 14254-14263 constitutes the proceedings of the 32nd International Conference on Artificial Neural Networks and Machine Learning, ICANN 2023, which took place in Heraklion, Crete, Greece, during September 26–29, 2023. The 426 full papers, 9 short papers and 9 abstract papers included in these proceedings were carefully reviewed and selected from 947 submissions. ICANN is a dual-track conference, featuring tracks in brain inspired computing on the one hand, and machine learning on the other, with strong cross-disciplinary interactions and applications.

Advances in Brain Inspired Cognitive Systems

The six-volume set comprising the LNCS volumes 11129-11134 constitutes the refereed proceedings of the workshops that took place in conjunction with the 15th European Conference on Computer Vision, ECCV 2018, held in Munich, Germany, in September 2018.43 workshops from 74 workshops proposals were selected for inclusion in the proceedings. The workshop topics present a good orchestration of new trends and traditional issues, built bridges into neighboring fields, and discuss fundamental technologies and novel applications.

Human Machine Interaction in the Digital Era

As multimedia applications have become part of contemporary daily life, numerous paradigm-shifting technologies in multimedia processing have emerged over the last decade. Substantially updated with 21 new chapters, Multimedia Image and Video Processing, Second Edition explores the most recent advances in multimedia research and applications. This edition presents a comprehensive treatment of multimedia information mining, security, systems, coding, search, hardware, and communications as well as multimodal information fusion and interaction. Clearly divided into seven parts, the book begins with a section on standards, fundamental methods, design issues, and typical architectures. It then focuses on the coding of video and multimedia content before covering multimedia search, retrieval, and management. After examining multimedia security, the book describes multimedia communications and networking and explains the architecture design and implementation for multimedia image and video processing. It concludes with a section on multimedia systems and applications. Written by some of the most prominent experts in the field, this updated edition provides readers with the latest research in multimedia processing and equips them with advanced techniques for the design of multimedia systems.

Digital Forensics and Watermarking

This book constitutes the refereed proceedings of the 13th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2023, held in Roorkee, India, in December 2023. The 14 papers included in these proceedings were carefully reviewed and selected from 45 submissions. They focus on various aspects of security, privacy, applied cryptography, and cryptographic engineering.

New Trends in Image Analysis and Processing -- ICIAP 2015 Workshops

The advances of digital cameras, scanners, printers, image editing tools, smartphones, tablet personal computers as well as high-speed networks have made a digital image a conventional medium for visual information. Creation, duplication, distribution, or tampering of such a medium can be easily done, which calls for the necessity to be able to trace back the authenticity or history of the medium. Digital image forensics is an emerging research area that aims to resolve the imposed problem and has grown in popularity over the past decade. On the other hand, anti-forensics has emerged over the past few years as a relatively new branch of research, aiming at revealing the weakness of the forensic technology. These two sides of research move digital image forensic technologies to the next higher level. Three major contributions are

presented in this dissertation as follows. First, an effective multi-resolution image statistical framework for digital image forensics of passive-blind nature is presented in the frequency domain. The image statistical framework is generated by applying Markovian rake transform to image luminance component. Markovian rake transform is the applications of Markov process to difference arrays which are derived from the quantized block discrete cosine transform 2-D arrays with multiple block sizes. The efficacy and universality of the framework is then evaluated in two major applications of digital image forensics: 1) digital image tampering detection; 2) classification of computer graphics and photographic images. Second, a simple yet effective anti-forensic scheme is proposed, capable of obfuscating double JPEG compression artifacts, which may vital information for image forensics, for instance, digital image tampering detection. Shrink-and-zoom (SAZ) attack, the proposed scheme, is simply based on image resizing and bilinear interpolation. The effectiveness of SAZ has been evaluated over two promising double JPEG compression schemes and the outcome reveals that the proposed scheme is effective, especially in the cases that the first quality factor is lower than the second quality factor. Third, an advanced textural image statistical framework in the spatial domain is proposed, utilizing local binary pattern (LBP) schemes to model local image statistics on various kinds of residual images including higher-order ones. The proposed framework can be implemented either in single- or multi-resolution setting depending on the nature of application of interest. The efficacy of the proposed framework is evaluated on two forensic applications: 1) steganalysis with emphasis on HUGO (Highly Undetectable Steganography), an advanced steganographic scheme embedding hidden data in a content-adaptive manner locally into some image regions which are difficult for modeling image statics; 2) image recapture detection (IRD). The outcomes of the evaluations suggest that the proposed framework is effective, not only for detecting local changes which is in line with the nature of HUGO, but also for detecting global difference (the nature of IRD).

Artificial Neural Networks and Machine Learning – ICANN 2023

This two volume set (CCIS 1776-1777) constitutes the refereed proceedings of the 7th International Conference on Computer Vision and Image Processing, CVIP 2022, held in Nagpur, India, November 4–6, 2022. The 110 full papers and 11 short papers were carefully reviewed and selected from 307 submissions. Out of 121 papers, 109 papers are included in this book. The topical scope of the two-volume set focuses on Medical Image Analysis, Image/ Video Processing for Autonomous Vehicles, Activity Detection/ Recognition, Human Computer Interaction, Segmentation and Shape Representation, Motion and Tracking, Image/ Video Scene Understanding, Image/Video Retrieval, Remote Sensing, Hyperspectral Image Processing, Face, Iris, Emotion, Sign Language and Gesture Recognition, etc.

Computer Vision – ECCV 2018 Workshops

This book constitutes the refereed proceedings of the 11th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2020, held in Boston, MA, in October 2020. Due to COVID-19 pandemic the conference was held virtually. The 11 reviewed full papers and 4 short papers were selected from 35 submissions and are grouped in topical sections on digital forensics; cyber-physical system Forensics; event reconstruction in digital forensics; emerging topics in forensics; cybersecurity and digital forensics.

Multimedia Image and Video Processing

Advances in Knowledge Discovery and Data Mining

vespa et4 125 manual
standards for quality assurance in diabetic retinopathy
pipefitter math guide
chapter 7 section 3 guided reading