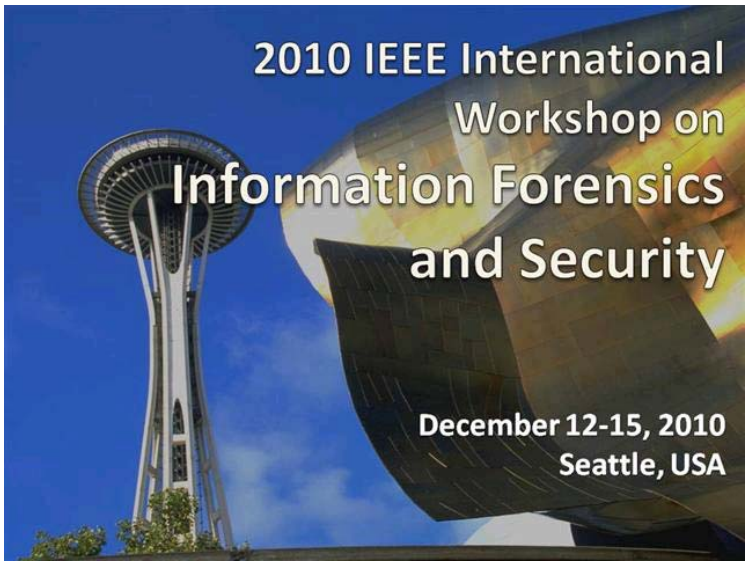
The 2010 IEEE international Workshop on Information Forensics and Security

Workshop Guide



Contents


IEEE
IEEE
Signal Processing Society

Preface

Following the technical and organizational success of the first IEEE Workshop on Information Forensics and Security (WIFS) last year in London, we set out to build upon this exciting foundation. The idea behind hosting the event in the Pacific Northwest was to benefit from its exceptional industrial presence, and we clearly have. Local companies such as Boeing and Microsoft, strikingly at present time running a 66 billion dollar annual business each, have had a long tradition of reliance upon security as a centerpiece to their existence. We trust that the stimulating backdrop of the beautiful Pacific Northwest, and participation of its strong industrial research community, will inspire researchers towards new inventions and research contributions.

This second workshop, WIFS'10, is sponsored by the IEEE Signal Processing Society. The long-term goal of WIFS is to provide a stimulating venue for knowledge exchange that encompasses a broad range of disciplines exploring various aspects of information forensics and computer security, and that facilitates the exchange of ideas across communities and individuals whose regular research paths may not normally intersect. By so doing, we hope that researchers will gain new perspectives, and identify new opportunities for collaboration across disciplines.

We are honoured to have two excellent invited keynotes, by Rico Malvar, Chief Scientist, Microsoft Research, and Yoshi Kohno, of the University of Washington. Their respective talks, looking at the future of computing, and systems security aspects related to medical devices, automobiles and robots, are sure to inspire many researchers young and old alike.

We would like to thank our sponsors for their support: Boeing Corp. and its Ed Wells partnership, Microsoft Research, Technicolor, and Digimarc. We express special thanks to Mauro Barni and Gwenaël Doërr for their relentless efforts to keep us all on track. We thank all those involved in the organization of WIFS'10, especially our Program Committee co-chairs Dinei Florencio and Nasir Memon, the committee itself, our external reviewers, and all authors of submitted papers. Finally, we thank you, our participants for being part of our community.

Darko Kirovski
Paul Van Oorschot

Organization Committee

General Chairs
Darko Kirovski – Microsoft Research, USA
Paul Van Oorschot – Carleton University, Canada

Technical Program Chairs
Dinei Florêncio – Microsoft Research, USA
Nasir Memon – Polytechnic University, USA

Local Arrangements Chair
Daniel Schonberg – Microsoft Research, USA

Tutorials Chair
Ton Kalker – Hewlett Packard, USA

Publications Chair
Z. Jane Wang – University of British Columbia, Canada

Publicity Chair
Min Wu – University of Maryland, USA

Industry Liaison
Gwenael Doerr – Technicolor, France

Asia Liaison
M. Kivanc Mihcak – Bogazici University

Europe Liaison
Mauro Barni – University of Sienna

Latin American Liaison
Ricardo de Queiroz – Universidade de Brasilia

Message from the Technical Chairs

As Technical Program Co-Chairs, we wish to thank everyone who submitted and reviewed papers for WIFS 2010. Not only we received a record number of submissions, the level of the submissions was extremely high. Yet, due to physical limitations of the workshop, we had to limit the number of accepted papers to just 39 (acceptance rate: 28%). The technical committee worked very hard to select the top papers from the submissions, having to reject many well deserving papers. In the end, each paper received a minimum of three independent reviews. The outstanding quality of the submissions implied a cut off at an average review score of 7.25, on a scale where 7 meant "the average WIFS paper". In other words, the average WIFS paper from last year would not make the cut at this year's conference! This is yet another evidence of the increased recognition and impact of WIFS, which, just in its second year, is already the leading forum for reporting breakthrough research in forensics and security, in all its multidisciplinary aspects.

With the conference site just a few miles away from Microsoft headquarters, in Redmond, WA, it is only fitting that Microsoft Research's Chief Scientist, Rico Malvar, will be one of our keynote speakers. In his keynote, Rico will present some highlights of the research being done at Microsoft Research, as well as his personal views of where computing is headed. Our second keynote speaker, Tadayoshi Kohno, from University of Washington, will discuss the challenges associated with security in cyber-physical systems, including medical devices, robots, and automobiles. In a way, interaction with physical systems is the new frontier of computing, and Tadayoshi be able to stretch our thinking on the security and privacy implications of all this.

The keynotes and final accepted papers make an outstanding selection of technical innovation, and we are looking forward to a most exciting event in Kirkland, WA this December. We hope you enjoy the program.

Dinei Florencio and Nasir Memon
Technical Program Co-Chairs, WIFS 2010

Technical Program Committee

Jan P. Allebach - Purdue University
Elisa Bertino - Purdue University
Vijayakumar Bhagavatula - CMU
Shih-Fu Chang - Columbia University
Max Costa - UNICAMP
Ingemar Cox - University College London
Robert Cunningam - MIT
Edward Delp - Purdue University
Jana Dittman - University of Magdeburg
Gwenael Doerr - Technicolor
Jean-Luc Dugelay - EURECOM
Patrick Flynn - University of Notre Dame
Andrew Ker - University of Oxford
Cormac Herley - Microsoft Research
Stefan Katzenbeisser - TU Darmstadt
Farinaz Koushanfar - Rice University
Markus Kuhn - Cambridge University
Deepa Kundur - Texas A&M
C.-C. Jay Kuo - USC
Mark Liao - National I-Lan University
David Molnar - Microsoft Research
Pierre Moulin - UIUC
Helen Nissenbaum - NYU
Fernando Perez-Gonzalez - University of Vigo
Bart Preneel - Katholieke Universiteit Leuven
Stuart Schechter - Microsoft Research
Gaurav Sharma - University of Rochester
Boris Skoric - TU Eindhoven
Francois-Xavier Standaert - Université Catholique de Louvain
Edward Suh - Cornell University
Qibin Sun - Columbia University
James Wayman - San Jose State University
H. Vicky Zhao - University of Alberta

Keynote Talks

A Glimpse at the Future of Computing

Henrique (Rico) Malvar
Microsoft Research, USA

Monday 13rd December, 9:25 - 10:25 am

Abstract: Computing, information, and entertainment technologies evolve and change at an increasingly rapid pace. In this talk we present an overview of some of the technologies developed at Microsoft Research that push the limits of computing. Those include visualization techniques for petabytes of data, touch interfaces and body computing, speech translation, augmented reality, user sentiment analysis, streaming data processing, new wireless networking interfaces, and new tools for design and test of large-scale software.

Security for Cyber-physical Systems: Case Studies with Medical Devices, Robots, and Automobiles

Tadayoshi Kohno
University of Washington, USA

Tuesday 14th December, 9:25 - 10:25 am

Abstract:Today's and tomorrow's emerging technologies and cyber-physical systems have the potential to greatly improve the quality of our lives. Without the appropriate checks and balances, however, these emerging technologies also have the potential to compromise our digital and physical security and privacy. This talk will explore three case studies in the design and analysis of secure cyber-physical systems: wireless medical devices, robots, and automobiles. We will discuss the discovery of vulnerabilities in leading examples of these technologies, the challenges to securing these technologies and the ecosystem leading to their vulnerabilities, and new directions for security

Technical Program

Sunday, December 12th, 2010

18:00 to 20:00 Welcome reception

Monday, December 13th, 2010

09:00 - 09:25 Opening

09:25 - 10:25 Keynote talk #1
Rico Malvar, "A Glimpse at the Future of Computing"

10:25 - 10:50 Coffee break

10:50 - 12:30 Paper Session: **Biometrics: attacks and Countermeasures**

THE EFFECT OF ENVIRONMENTAL CONDITIONS AND NOVEL SPOOFING METHODS ON FINGERPRINT ANTI-SPOOFING ALGORITHMS
Bozhao Tan, Aaron Lewicke, David Yambay, and Stephanie Schuckers, Clarkson University
Abstract: Fingerprint recognition systems have been shown to be vulnerable to spoof attacks. In this study, we collected live fingerprints under various environment weather conditions. Additionally we incorporated more spoofing materials of latex rubber, latex caulk, and latex paint. The algorithms were trained with a baseline dataset for Identix, Crossmatch, and Digital Persona devices with an average spoof/live equal error rate of 3.5%, 5.9% and 5.8%, respectively. Results showed an increase in error to 14.5%, 55.6% and 36.6%, respectively, when data of this type is not included in the training set. Similarly, we found the new spoof approaches

developed defeat the liveness algorithm in almost all cases. When the algorithm is retrained to include new environmental and spoof images, the liveness algorithm is able to achieve an average error rate of 4.0%, 9.6%, and 11.4% for Identix, Crossmatch, and Digital Persona scanners, respectively. The impact of temperature, humidity, and novel spoof materials on anti-spoofing algorithm is significant and degrades performance. Performance can be restored when these factors are included in the training of the anti-spoofing model.

MULTIMODAL FUSION VULNERABILITY TO NON-ZERO EFFORT (SPOOF) IMPOSTERS

Peter Johnson, Bozhao Tan, and Stephanie Schuckers, Clarkson University

Abstract: In biometric systems, the threat of "spoofing", where an imposter will fake a biometric trait, has lead to the increased use of multimodal biometric systems. It is assumed that an imposter must spoof all modalities in the system to be accepted. This paper looks at the cases where some but not all modalities are spoofed. The contribution of this paper is to outline a method for assessment of multimodal systems and underlying fusion algorithms. The framework for this method is described and experiments are conducted on a multimodal database of face, iris, and fingerprint match scores.

BEYOND PKI: THE BIOCRYPTOGRAPHIC KEY INFRASTRUCTURE

Walter Scheirer, University of Colorado; Terrance Boult, University of Colorado;
William Bishop, Securics, Inc.

Abstract: Public Key Infrastructure is a widely deployed security technology for handling key distribution and validation in computer security. Despite PKI's popularity as a security solution, Phishing and other Man-in-the-Middle related network attacks are accomplished with ease. The major problems with PKI come down to trust, and largely, how much faith we must place in cryptographic keys alone to establish authenticity and identity. In this paper, we look at a novel biometric solution that mitigates this problem at both the user and certificate authority levels. More importantly, we examine the trouble with the placement of unprotected biometric features directly into PKI, and propose the integration of a secure, revocable biometric template protection technology that supports transactional key release. A detailed explanation of this new Biocryptographic Key Infrastructure is provided, including composition, enrollment, authentication, and revocation details.

INDEXING IRIS IMAGES USING THE BURROWS-WHEELER TRANSFORM

Ravindra Gadde, Donald Adjeroh, and Arun Ross, West Virginia University

Abstract: In most biometric identification systems, the input biometric data has to be compared against that of every identity in the database in order to determine the identity of the input. A major problem with this approach is the impact on response time which can increase significantly with the size of the database. In certain applications such as real time monitoring, this delay may not be acceptable. In this work, we propose a method for indexing iris images for rapid identity retrieval. Every entry in the database is assigned an index code based on which a small subset is retrieved and matched in response to a query. The basis of our approach is the sorted context property of the Burrows Wheeler Transform, a popular transformation used in data compression. Experiments on the CASIA version 3 iris database show a significant reduction in both search time and search space.

12:30 - 13:40pm: Lunch break

13:40 - 15:20: Paper Session: **Biometrics: Fuzzy extractors**

EFFICIENT STRATEGIES FOR PLAYING THE INDISTINGUISHABILITY GAME FOR FUZZY SKETCHES
Ileana Buhan-Dulman, Philips Research, Europe; Jorge Guajardo Merchan, Philips Research Europe; Emily Kelkboom,
Abstract: One of the fundamental requirements for a fuzzy sketch algorithm is to offer indistinguishability, which ensures that an adversary cannot identify related sketches generated from the same biometric identity. Recently it has been showed that the advantage of an adversary in distinguishing two related sketches generated using the code-offset construction is non-negligible. The main contribution of this work is a new, efficient strategy for playing the indistinguishability game. Furthermore, we analyze the model known in the literature in a more realistic scenario in which classification is not perfect but it is subject to errors. Our results indicate that the advantage of an adversary in the real world depends on the threshold chosen by the distinguisher. Furthermore, we introduce a stronger model in which the adversary is assumed to have no a priori knowledge and we extend the existing framework by modeling the advantage of an adversary in the new model; we show that also in the extended model the new strategy for playing the indistinguishabilityt game is at least as strong as the known strategy.

DIFFERENTIAL TEMPLATE ATTACKS ON PUF ENABLED CRYPTOGRAPHIC DEVICES
Deniz Karakoyunlu, WPI; Berk Sunar, WPI
Abstract: In this paper we provide the first practical attacks on software implementations of fuzzy extractors (FEs). The significance of these attacks stem from the fact that FEs are becoming an essential building block in the implementations of physical unclonable function (PUF) enabled devices. Our attacks exploit the information leaked through the power side-channel in the initial stages of error correction and can be used to recover the FE input which would essentially mean cloning the PUF device. We report two attacks: a simple power analysis (SPA) attack where we make use of conditional checks in a naive implementation to recover the PUF response by simply observing time shifts in the power consumption profile. In our second attack, we assume all conditional executions are removed making the device secure against SPA attacks. Instead, we mount a new kind of template attack on a two instruction sequence to recover the FE input (or PUF output).

A FINGERPRINT CRYPTOSYSTEM BASED ON MINUTIAE PHASE SPECTRUM
Karthik Nandakumar, Institute for Infocomm Research
Abstract: Public acceptance of biometric technology is hindered by security and privacy concerns regarding leakage of biometric templates. Biometric cryptosystems alleviate this problem by storing a secure sketch that is typically derived by binding the template with a cryptographic key. However, designing fingerprint cryptosystems is difficult because fingerprint matching is usually based on unordered sets of minutia features having large intra-user variations. We propose a novel minutiae representation known as the Binarized Phase Spectrum (BiPS), which is a fixed-length

binary string obtained by quantizing the Fourier phase spectrum of a minutia set. We secure the BiPS representation using a fuzzy commitment scheme employing turbo codes. We also propose a technique for aligning fingerprints based on the focal point of high curvature regions. The proposed system achieves a FNMR of 16.2% and 12.6% on FVC2002-DB1 and DB2 databases, respectively, at zero FMR.

IDENTIFICATION AND SECRET-KEY BINDING IN BINARY-SYMMETRIC TEMPLATE-PROTECTED BIOMETRIC SYSTEMS
Frans Willems, Eindhoven University; Tanya Ignatenko,
Abstract: In the system that we investigate here, two terminals observe the enrollment and identification biometric sequences of different individuals. In this paper we determine what identification and secret-key rates can be jointly realized by such a biometric identification and key-binding system. We focus on the binary symmetric case and show that there exist linear codes yielding optimal performance. The setting that we investigate here is closely related to the study of the biometric identification capacity [O'Sullivan and Schmid, 2002, Willems et al., 2003] and the common randomness generation problem [Ahlswede and Csiszar, 1993]. The linear-coding part generalizes the fuzzy commitment scheme [Juels and Wattenberg, 1999].

15:20 - 15:45: Coffee break

15:45 - 17:25 Paper Session: **Privacy and Forensics**

ECG BIOMETRICS: A ROBUST SHORT-TIME FREQUENCY ANALYSIS
Ikenna Odinaka, Po-Hsiang Lai, Alan Kaplan, Joseph O'Sullivan, Erik Sirevaag, Sean Kristjansson, Amanda Sheffield, and John Rohrbaugh, Washington University in Saint Louis
Abstract: We present the results of an analysis of the electrocardiogram (ECG) as a biometric using a novel short-time frequency method with robust feature selection. Our proposed method incorporates heartbeats from multiple days and fuses information. Single lead ECG signals from a comparatively large sample of 269 subjects were collected on three separate occasions over a seven-month period. We studied the impact of long-term variability, health status, data fusion, the number of training and testing heartbeats, and database size on ECG biometric performance. The proposed method achieves 5.58% equal error rate (EER) in verification, 76.9% accuracy in rank-1 recognition, and 93.5% accuracy in rank-15 recognition when training and testing heartbeats are from different days. If training and testing heartbeats are collected on the same day, we achieve 0.37% EER and 99% recognition accuracy for decisions based on a single heartbeat.

PREDICTABILITY AND CORRELATION IN HUMAN METROLOGY
Donald Adjeroh, Deng Cao, Marco Piccirilli, Arun Ross, West Virginia University
Abstract: Human metrology provides an important soft biometric, which can be used in challenging situations such as human identification at a distance, when traditional biometric traits such as fingerprints or iris cannot be easily acquired. We study the problem of predictability and correlation in human metrology, using the tools of uncertainty and differential entropy. We show that while various metrological features are highly correlated with each other, there exists some correlation clusters in human metrology, whereby measurements in a cluster tend to be highly correlated with each other but not with the others. Based on these clusters, we propose a two-step approach

for predicting unknown body measurements. Using the same framework, we study the problem of estimating other soft biometrics such as weight and gender.

ID-PRIVACY IN LARGE SCALE BIOMETRIC SYSTEMS
Abhijit Bendale, MIT; Terrance Boult, University of Colorado
Abstract: Balancing privacy and security concerns in biometric systems is an area of growing importance. This paper introduces the concept of id-privacy, requiring at least i items (e.g. fingers) to be provided to resolve identity to better than d above random chance. We show how using cross-finger representation on unsegmented fingerprint slap data, we can address what may be the single most important "privacy" issue in biometrics, privacy enhanced deduplication. We prove we can achieve (2,0)-id-privacy for fingerprint-based deduplication while preventing searching with a latent print. We introduce the Forest Finger algorithm -- an approach for matching unsegmented slaps and cross-finger representations.

PRIVACY AMPLIFICATION OF CONTENT IDENTIFICATION SYSTEMS BASED ON FINGERPRINT BIT RELIABILITY
Svyatoslav Voloshynovskiy, Oleksiy Koval, Taras Holotyak, Fokko Beekhof, and Farzad Farhadzadeh; University of Geneva
Abstract: In many problems such as privacy-preserving biometrics and multimedia identification, some binary features representing the original biometrics or multimedia content are stored in the public domain or outsourced to the third parties. This naturally raises certain privacy concerns about the privacy leak. To avoid this privacy leak, privacy amplification is used. In the most cases, the privacy amplification is uniformly applied to all binary features resulting in the data degradation and corresponding loss of performance. To avoid this undesirable effect we propose a new privacy amplification technique that benefits from side information about bit reliability. In this paper, we investigate the identification rate-privacy leak trade-off as well as consider several algorithms for fast privacy preserving content identification based on bit reliability.

19:00 - 21:00: Conference dinner

Tuesday, December 14th, 2010

9:25 - 10:25 Keynote talk #2
Tadayoshi Kohno, “Security for Cyber-physical Systems: Case Studies with Medical Devices, Robots, and Automobiles”

10:25 - 10:50 Coffee break

10:50 - 12:30 Paper Session: **Processing in the Encrypted Domain**

PRIVACY PRESERVING STRING COMPARISONS BASED ON LEVENSHTEIN DISTANCE

Shantanu Rane, Wei Sun, Mitsubishi Electric Research Laboratories

Abstract: Alice and Bob possess strings x and y of length m and n respectively and want to compute the Levenshtein distance L(x,y) between the strings under privacy and communication constraints. In this work, we propose an asymmetric two-party protocol in which a lightweight client Bob with a string y interacts with a single powerful server Alice containing string x in its database. We present a privacy-preserving minimum-finding protocol based on semantically secure homomorphic functions and additive secret sharing. This protocol is executed repeatedly, to enable private computation of the edit distance. Our protocol supports arbitrary finite insertion/deletion costs and a variety of substitution costs. While Alice requires similar effort as in previous approaches, the advantage is that Bob incurs far fewer ciphertext operations and transmissions, making the protocol well-suited for client-server querying applications.

ENCRYPTED INTEGER DIVISION

Thijs Veugen, TNO

Abstract: When processing signals in the encrypted domain, homomorphic encryption can be used to enable linear operations on encrypted data. Integer divsion of encrypted data however requires an additional protocol with the server and will be relatively expensive. We present new solutions for dividing encrypted data, having low computational complexity. Two protocols for computing exact division, and two for approximating the division result.

SECURE COMPUTATIONS ON NON-INTEGER VALUES

Martin Franz, CASED; Stefan Katzenbeisser, TU Darmstadt; Somesh Jha, University of Wisconsin; Kay Hamacher, TU Darmstadt; Heike Schroeder, TU Darmstadt; Bjoern Deiseroth, TU Darmstadt

Abstract: In this paper we present for the first time a framework that allows secure two-party computations on approximations of real valued signals. In our solution, we use a quantized logarithmic representation of the signal samples, which enables to represent both very small and very large numbers with bounded relative error. We show that numbers represented in this way can be encrypted using standard homomorphic encryption schemes; furthermore we give protocols that allow to perform all arithmetic operations on such encrypted values. Finally we demonstrate the practicality of our framework by applying it to the problem of filtering encrypted signals.

PRIVACY PRESERVING EVALUATION OF SIGNAL QUALITY WITH APPLICATION TO ECG ANALYSIS

Riccardo Lazzeretti, University of Siena, Italy; Mauro Barni, University of Siena; Jorge Guajardo Merchan, Philips Research Europe

Abstract: A problem often neglected in privacy-preserving protocols is the need to ensure that processed signals are of sufficient quality. This is a particularly pressing need in remote e-health services wherein measurements are performed by consumers, hence raising the need for solutions that assess the quality of the recorded signals to

guarantee correct (medical) decisions. In this paper, we introduce the problem of assessing signal quality in the encrypted domain and propose a privacy-preserving protocol to solve it. We use the Signal-To-Noise Ratio (SNR) between the original signal and a filtered version of the signal itself as the quality measure. The proposed scheme relies on a hybrid multiparty computation protocol based on Homomorphic Encryption and Yao's Garbled Circuits. A central point in the protocol is the application of the logarithm function to the linear SNR. We do so by introducing an efficient protocol for the computation of an integer version of the logarithm function that has linear complexity in the bitsize of the signal energy. We prove the validity of the proposed protocol, both in terms of accuracy and efficiency by applying it to the computation of the quality of ECG signals.

12:30 - 13:40 Lunch break

13:40 - 15:20 Paper Session: **Hardware and Network Security**

A LAYOUT-AWARE APPROACH FOR IMPROVING LOCALIZED SWITCHING TO DETECT HARDWARE TROJANS IN INTEGRATED CIRCUITS
Hassan Salmani, University of Connecticut; Mohammad Tehranipoor, University of Connecticut; Jim Plusquellic, University of New Mexico
Abstract: Malicious activities and alterations to integrated circuits have raised serious concerns to government agencies and the semiconductor industry. The added functionality, known as hardware Trojan, poses major detection and isolation challenges. In this paper, we present a method to localize design switching to any specific region. The new architecture allows activating any target region and keeping others quiet which reduces total circuit switching activity. This helps magnify the Trojan's contribution to the total circuit transient power by increasing Trojan-to-circuit switching activity (TCA) and power consumption. Our simulation results demonstrate the efficiency of the method in significantly increasing TCA.

A PHASE-SPACE RECONSTRUCTION APPROACH TO DETECT COVERT CHANNELS IN TCP/IP PROTOCOLS
Hong Zhao, Fairleigh Dickinson University; Yun-Qing Shi, New Jersey Institute of Technology
Abstract: Covert channels via the TCP/IP protocols have become a new challenge issue for network security. We propose an effective method to detect the existence of hidden information in TCP ISNs, which are known as the most difficult covert channels to be detected. Our method uses phase space reconstruction to characterize dynamic nature of ISNs. A statistical model is then proposed. Based on this proposed model, the classification algorithm is developed to identify the existence of information hidden in ISNs. Simulation results have demonstrated that our proposed detection method outperforms the-state-of-the-art in terms of high detecting accuracy and greatly reduced computational complexity. Instead of off-line processing as the-state-of-the-art does, our new scheme can be used for on-line detection.

SIMILARITY COEFFICIENT GENERATORS FOR NETWORK FORENSICS
Ravi Mukkamala, Old Dominion University; Aditya Telidevara, Sri Sathya Sai University; V Chandrasekaran, Sri Sathya Sai University; Avinash Srinivasan, Bloomsburg University; Sandeep Gampa, Old Dominion University

Abstract: IP spoofing is one of the most common network threats today. While current IP Traceback techniques are capable of identifying the source of a message, they are limited by the huge number of messages that routers have to store to provide this facility. One way to reduce the storage overhead is to store the messages as indices in a Bloom filter. However, often there is a need to know if a similar message has traversed through the router. This calls for similarity measures in the context of Bloom filters. In this paper, we develop such similarity measures (coefficients) in the context of two specialized Bloom filters---Hierarchical Bloom filter (HBF) and Winnowing Block Shingling (WBS). We compare the efficacy of these similarity measures with the Jaccard similarity coefficient. Simulation results indicate that HBF-measure is an optimistic metric and WBS-similarity is a pessimistic measure. We propose a weighted metric that combines all the metrics and is more flexible than the individual measures.

FPGA PUF USING PROGRAMMABLE DELAY LINES
Mehrdad Majzoobi, Rice University; Farinaz Koushanfar, Rice University; Srini Devadas,
Abstract: This paper proposes a novel approach for efficient implementation of a real-valued arbiter-based physical unclonable function (PUF) on FPGA. We introduce a high resolution programmable delay logic (PDL) implemented by lookup table (LUT) internal structure. Using the PDL, we perform fine tuning to cancel out delay skews caused by asymmetries in routing and systematic variations. We devise a symmetric switch structure that can be easily implemented on FPGA. To mitigate the arbiter metastability problem, we present and analyze methods for majority voting of responses. Lastly, a method to classify and group challenges into different robustness sets is introduced, to further increase the corresponding responses' stability in the face of environmental variations. Experimental evaluations show that the responses to robust challenges have an average error rate of less than 2% under temperature variations from -10 Celsius degrees 75 degrees.

15:20 - 15:45 Coffee break

15:45 - 17:25 Paper Session: **Anti-counterfeiting and Forensics**

MODEL BASED PRINT SIGNATURE PROFILE EXTRACTION FOR FORENSIC ANALYSIS OF INDIVIDUAL TEXT GLYPHS
Stephen Pollard, Hewlett Packard; Steven Simske, Hewlett Packard Laboratories; Guy Adams, Hewlett Packard Laboratories
Abstract: Forensic analysis of individual printed items, including single characters, enables the addition of some level of security to any printed item (label, document, package, etc.). In this paper, we present a model-based approach for extracting a signature profile around the outer edge of virtually any text glyph. We show that for two high-resolution imaging devices (the Dyson Relay CMOS Imaging Device, called DrCID, and a high speed line-scan camera) this signature encodes that part of the glyph boundary that is due to the random fluctuation of the print process, enabling significantly higher levels of forensic discrimination than previously shown. The model-based approach enables a security workflow where the line-scan device is integrated into production line inspection with later forensic investigation in the field using the DrCID device. We also develop a simple shape descriptor to encode the

signature profile, making it easier to manipulate, test and store. We argue that the shape descriptor provides forensic-level authentication of a single printed character.

FAST IMAGE CLUSTERING OF UNKNOWN SOURCE IMAGES
Roberto Caldelli, Irene Amerini, Francesco Picchioni, and Matteo Innocenti,
MICC - University of Florence
Abstract: Succeeding in determining information about the origin of a digital image is a basic issue of multimedia forensics. In this paper a new technique which aims at blindly clustering a given set of N digital images is presented. Such a technique is based on a pre-existing one and improves it both in terms of error probability and of computational efficiency. The system is able, in an unsupervised and fast manner, to group photos without any initial information about their membership. Sensor pattern noise is extracted by each image as reference and the successive classification is performed by means of a hierarchical clustering procedure. Experimental results have been carried out to verify theoretical expectations and to witness the improvements with respect to the other technique.

FIRST STEPS TOWARD IMAGE PHYLOGENY
Zanoni Dias, Anderson Rocha, and Siome Goldenstein, UNICAMP
Abstract: In this paper, we introduce and formally define a new problem, Image Phylogeny Tree (IPT): to find the structure of transformations, and their parameters, that generate a given set of near duplicate images. This problem has direct applications in security, forensics, and copyright enforcement. We devise a method for calculating an asymmetric dissimilarity matrix from a set of near duplicate images. We also describe a new algorithm to build an IPT. We also analyze our algorithm's computational complexity. Finally, we perform experiments that show near-perfect reconstructed IPT results when using an appropriate dissimilarity function.

MIX-SPLIT: CONTROLLED MIXING OF SECRETS AND TRACEABLE PSEUDONYM GENERATION USING CODEBOOKS
Kannan Karthik , I. I. T Guwahati; Dimitrios Hatzinakos, University of Toronto
Abstract: A non-perfect secret sharing scheme called MIX-SPLIT is a substitution cipher created by mixing two statistically similar binary sequences (secrets) through a codebook. At the heart of the algorithm are the hidden partitions which define the identity of the shares generated. By imposing certain constraints on the codebook these partitions can be made invisible, opening up the possibility of constructing traceable pseudonyms which are inherently frameproof. These codes by virtue of their parental dependency (inheritance) can be applied towards both content authentication as well as tracking.

18:00 - Evening: optional social activity (details/price to follow)

9:10 - 10:25 Paper Session: **Forensic Analysis – 1**

DIGITAL FORENSICS IN VOIP NETWORKS
Jérôme François, University of Luxembourg; Radu State, ; Thomas Engel, ; Olivier Festor,
Abstract: With VoIP being deployed on large scale, forensic analysis of captured VoIP traffic is of major practical interest. In this paper, we present a new fingerprinting approach that identifies the types of devices (name, version, brand, series) in captured VoIP traffic. We focus only on the signaling plane and discard voice related data. Although we consider only one signaling protocol for the illustration, our tool relies on structural information trees and can easily be adapted to any protocol of that has a known syntax. We have integrated our tool within the well known tshark application in order to provide an easy to use support for forensic analysts.

DETECTING VANISHING POINTS BY SEGMENT CLUSTERING ON THE PROJECTIVE PLANE FOR SINGLE-VIEW PHOTOGRAMMETRY
Fernanda Andaló, Unicamp; Gabriel Taubin, Brown University; Siome Goldenstein, UNICAMP
Abstract: In this paper, we describe how a effective vanishing point detector can be applied to photogrammetry when only a single view of an architectural environment is available. Our method performs automatic segment clustering in projective space - a direct transformation from the image space - instead of the traditional bounded accumulator space. Experiments on real images show the effectiveness of the proposed detector in finding all vanishing points, as well as its application in a photogrammetry algorithm, by recovering the vertical direction of the scene and the vanishing line for the ground plane.

PHISHING AND MONEY MULES
Dinei Florencio, and Cormac Herley, Microsoft Research
Abstract: Data breaches, phishing and spyware have compromised millions of end-user records and credentials. Mules are the preferred means for draining compromised accounts. These are unwitting accomplices who provide a stepping stone between the victim account and the attacker. The key role they play is to turn reversible traceable transactions into irreversible untraceable ones. This, together with the fraud protections enjoyed by US banking customers, generates some surprising findings. First, it is the mule's money not the victim's or the bank's money that the attacker steals. Second, mule recruitment and not credential theft appears the true bottleneck in online fraud. Third, this suggests an explanation of why stolen credentials sell so cheaply: there is a shortage of mules.

10:25 - 10:40 Coffee break

10:40 - 12:20 Paper Session: **Steganography and Forensics**

SEMI NON-INTRUSIVE TRAINING FOR CELL-PHONE CAMERA MODEL LINKAGE

Wei-Hong Chuang, and Min Wu, University of Maryland

Abstract: This paper presents a study of cell-phone camera model linkage that matches digital images against potential makes / models of cell-phone camera sources using camera color interpolation features. The matching performance is examined and the dependency on the content of training image collection is evaluated via variance analysis. Training content dependency can be dealt with under the framework of component forensics, where cell-phone camera model linkage is seen as a combination of semi non-intrusive training and completely non-intrusive testing. Such a viewpoint suggests explicitly the goodness criterion of testing accuracy for training data selection. It also motivates other possible alternative training procedures based on different criteria, such as the training complexity, for which preliminary but promising experiment designs and results have been obtained.

ON ROTATION INVARIANCE IN COPY-MOVE FORGERY DETECTION

Vincent Christlein, Christian Riess, and Elli Angelopoulou, University of Erlangen-Nuremberg

Abstract: The goal of copy-move forgery detection is to find duplicated regions within the same image. In this paper, we present a rotation-invariant selection method, which we call Same Affine Transformation Selection (SATS). It shares the benefits of the shift vectors at an only slightly increased computational cost. As a byproduct, the proposed method explicitly recovers the parameters of the affine transformation applied to the copied region. We evaluate our approach on three recently proposed feature sets. Our experiments on ground truth data show that SATS outperforms shift vectors when the copied region is rotated, independent of the size of the image.

MINIMIZING ADDITIVE DISTORTION FUNCTIONS WITH NON-BINARY EMBEDDING OPERATION IN STEGANOGRAPHY

Tomas Filler, and Jessica Fridrich, SUNY Binghamton

Abstract: Most practical steganographic algorithms for empirical covers embed messages by minimizing a sum of per-pixel distortions. Current near-optimal codes for this minimization problem [Filler et al. 2010 SPIE] are limited to a binary embedding operation. In this paper, we extend this work to embedding operations of larger cardinality. The need for embedding changes of larger amplitude and the merit of this construction are confirmed experimentally by implementing an adaptive embedding algorithm for digital images and comparing its security to other schemes.

A UNIVERSAL DIVERGENCE-RATE ESTIMATOR FOR STEGANALYSIS IN TIMING CHANNELS

Shankar Sadasivam, Pierre Moulin, and Sean Meyn, Univ of IL at Urbana-Champaign

Abstract: This paper proposes new tools for steganalysis of queue-based stegocodes over covert timing channels. We study a universal estimator for the Kullback-Leibler (KL) divergence rate between the covertext process and the stegotext process. We empirically illustrate the performance of our estimator on some simple queue-based stegocodes and study its convergence properties.

12:20 - 13:40 Lunch break

13:40 - 15:20 Paper Session: **Watermarking and Traitor tracing**

MAXIMIN OPTIMALITY OF THE ARCSINE FINGERPRINTING DISTRIBUTION AND THE INTERLEAVING ATTACK FOR LARGE COALITIONS

Yen-Wei Huang, and Pierre Moulin, Univ of IL at Urbana-Champaign

Abstract: Fingerprinting codes provide a means for the digital content distributor to trace the origin of an unauthorized redistribution. The maximum achievable rate, or capacity, has recently been derived as the value of a two-person zero-sum game between the fingerprinting embedder and the pirates. Under the so-called Boneh-Shaw marking assumption, we prove rigorously that the asymptotic capacity is 1/(k^2 2 ln2), where k is the number of pirates. Furthermore, we confirm our earlier conjecture that Tardos' choice of the arcsine distribution asymptotically maximizes the mutual information payoff function while the interleaving attack minimizes it. Along with the asymptotic behavior, numerical solutions to the game for small k are also presented.

SECURITY AND ROBUSTNESS CONSTRAINTS FOR SPREAD-SPECTRUM TARDOS FINGERPRINTING

Benjamin Mathon, GIPSA Lab - TELE; Patrick Bas, LAGIS; François Cayre, GIPSA Lab; Benoît Macq, TELE

Abstract: This paper presents a practical analysis of the impact of robustness and security on Tardos' collusion-secure fingerprinting codes using spread-spectrum watermarking modulations. In this framework, we assume that the coalition has to face an embedding scheme of given security level and consequently has to suffer a probability of wrongly estimating their embedded symbols. We recall the Worst Case Attack associated to this probability, e.g. the optimal attack which minimises the mutual information between the sequence of a colluder and the pirated one. For a given achievable rate of the Tardos' fingerprinting model, we compare the Improved Spread-Spectrum embedding versus a new secure embedding (called rho-Circular Watermarking) considering the AWGN channel. We show that secure embeddings are more immune to decoding errors than non-secure ones while keeping the same fingerprinting capacity.

JOINT ROBUST WATERMARKING AND IMAGE COMPRESSION

Yuhan Zhou, University of Waterloo

Abstract: A joint watermarking and compression (JWC) paradigm is considered for the application of JPEG image compression to achieve an efficient tradeoff among the embedding rate, compression rate, embedding distortion, and robustness against a class of ``natural'' signal processing attacks. This paper makes two novel contributions: First, a new JWC embedding method called joint odd-even watermarking and JPEG compression scheme is proposed to optimize compression rate and embedding distortion when watermarks are embedded into JPEG compressed images. Second, low-density parity-check codes are employed into the JWC system to obtain an efficient tradeoff between the embedding rate and robustness. Experimental results show that the proposed algorithm significantly outperforms the recently designed DEW (differential energy watermarking), DQW (differential quantization

watermarking) and RA-SEC (repeat-accumulate code based selectively embedding in coefficients) schemes.

BAYESIAN WATERMARK DETECTION AND NEW PERCEPTUAL MASK BASED ON A SPATIALLY WEIGHTED TOTAL VARIATION IMAGE PRIOR
Antonis Mairgiotis, University of Ioannina; Nikolaos Galatsanos, University of Patras
Abstract: In this work we propose a class of bayesian watermark detectors based on a spatially weighted Total Variation (TV) image model. The inherent flexibility of the proposed prior in modeling local image variations, provides us with a novel spatial mask capable to perceptually shape the embedded watermark. We also propose methods to estimate the parameters of the proposed mask, creating watermarks with more energy and in consequence with improved robust properties. Numerical experiments are presented that demonstrate the performance of our proposal with regard to detection sensitivity and the superiority of the mask compared with other existing spatial masking schemes.

15:20 - 15:45 Coffee break

15:45 - 17:25 Paper Session: **Forensic Analysis – 2**

EXPOSING DIGITAL FORGERIES FROM 3-D LIGHTING ENVIRONMENTS
Eric Kee, and Hany Farid, Dartmouth College
Abstract: When creating a photographic composite, it can be difficult to match lighting conditions. We describe a technique for measuring lighting conditions in an image, and describe its use in detecting photographic composites. Specifically, we describe how to approximate a 3-D lighting environment with a low-dimensional model and how to estimate the model's parameters from a single image. Inconsistencies in the lighting model are then used as evidence of tampering.

RECOGNITION OF BLURRED LICENSE PLATE IMAGES
Pei-Lun Hsieh, Academia Sinica; Yu-Ming Liang, ; Mark Liao, National I-Lan University
Abstract: In video forensics, to recognize objects in low-resolution frames is a commonly seen problem. In this paper, we propose a systematic way to recognize blurred license plate images. Our method only uses one license plate image and character segmentation is not necessary. The process involves three steps. First, using single-character templates, we identify the positions of characters on a license plate and estimate the corresponding character list. Then, the position of a special symbol on the license plate is estimated. Finally, to refine the recognition results, we expand the single-character templates to multiple-character templates. The experiment results demonstrate the efficacy of our method in recognizing characters in blurred license plate images.

ON CLASSIFICATION OF SOURCE CAMERAS: A GRAPH BASED APPROACH
Bei-bei Liu, KAIST; Heung-Kyu Lee, KAIST; Yongjian Hu, South China University of Tech; Chang-Hee Choi, KAIST
Abstract: Many existing source camera classification methods involve either training a classifier or computing the reference pattern noise of a camera, which means a set of

images of known origins have to be pre-acquired. However, such requirement can not always be satisfied in real-world forensic applications. In this work, we propose a graph based approach that requires no extra auxiliary images nor a prior knowledge about the constitution of the image set. By formulating the classification task as a graph partitioning problem, a set of images can be classified according to their source cameras in an entirely blind way, with the number of source cameras automatically estimated. Experimental results have verified the validity of the proposed approach.

TOWARDS A FEATURE SET FOR ROBUST PRINTING-IMAGING CYCLE DEVICE IDENTIFICATION USING STRUCTURED PRINTED MARKINGS

Matthew Gaubatz, Hewlett-Packard; Steven Simske, Hewlett Packard Laboratories

Abstract: Device identification is an emerging field where technologies used to create a digital image are inferred by strategic image analysis. Some of the more well understood topics in this area include techniques to identify cameras, scanners and printers. The goal of printing-imaging cycle device identification is to gather information about the printing and imaging devices used to create then digitally reacquire a physical document. It has been shown that accurate printer-scanner identification is possible using a specific type of marking composed of oriented, colored tiles. This paper discusses a set of features based on histogram analysis that can be applied to printing-imaging device identification problems using a wider range of small structured markings (color tile deterrents and Guilloche curve patterns). The features are robust to a number of different effects, including changes in perspective and scan resolution. The approach results in superior identification performance in comparison to other state-of-the-art strategies, and more robustness to marking orientation. Performance as a function of scan resolution is also discussed in detail.

17:25 - 17:30 Closing remarks

Financial Supporters

The organizers would like to express their deepest thanks to the various organizations which supported IEEE WIFS'10. The event would not have been possible without their help.

Microsoft Research

technicolor

DIGIMARC

IEEE

IEEE Signal Processing Society