Information Technology Laboratory Newsletter

Credit: NIST

January—February 2014

Issue 127

INSIDE THIS ISSUE

ITL Forensics Science Program

ITL Releases Test Tool for Meaningful Use Certification of Electronic Health Records

ITL Collaborates on Design of Rheometers for Dense Suspensions

Staff Recognition

Selected New Publications

Upcoming Technical Conferences

ITL Forensics Science Program

Forensic science provides one of the basic structural elements of the U.S. criminal justice system. It provides the methodologies for understanding crime scenes, analyzing evidence, identifying suspects, and prosecuting and convicting criminals while exonerating innocent people. Led by Dr. Martin Herman, the ITL Forensics Science Program advances the measurements and standards infrastructure for forensic science through the application of computer science, mathematics, statistics, computer engineering, metrology, and human factors.

The program goals include improving the accuracy, reliability, and scientific validity of forensic science as well as enhancing the usability and interoperability of forensic systems and methods. The research fits into four underlying themes that cover the critical areas in which ITL's unique expertise can contribute to forensic science: image and pattern analysis, measurement and uncertainty, interoperability of forensic data, and automated forensic technologies.

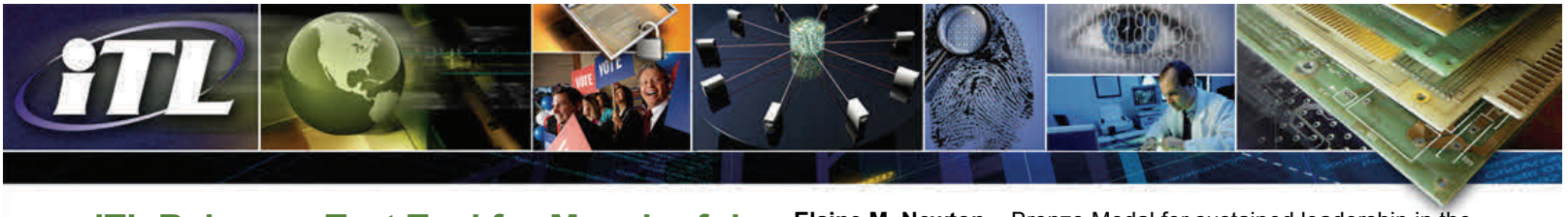
Specific research areas in our program include the following fields. In the area of human identity, we are developing metrics, tests, and standards to accelerate development of technologies that analyze and match latent fingerprints, face images, and voice. These technologies will aid forensic examiners in identifying potential suspects. We are enhancing interoperability of forensic systems through interface standards that include, in addition to the above evidence, DNA, scars, marks, tattoos, bite marks, and dental records. We are also supporting the development and interoperability of large-scale operational automated fingerprint identification systems.

In the area of computer forensics, our research results in methodologies to test and verify the operation and output of automated programs that examine computers, including cell phones and other mobile devices, for evidence. We also provide the National Software Reference Library (NSRL) Reference Data Set, a repository of known software, file profiles, and file signatures that is used by law enforcement and other investigators to determine the identity of files they recover. Finally, we are developing challenges and mitigation approaches that address forensic examination of cloud computing environments.

In the area of image/video technologies, we are applying metrics and testing methodologies to advance technologies that detect and recognize events in video surveillance data, as well as search for specific persons, objects, or places in such data. These technologies will aid forensic examiners who analyze images and video.

Finally, our activities in statistical science provide statistical analysis to various forensics research projects. Examples include uncertainty analysis for ballistic fingerprinting, for seized drug analysis, and for limits of detection for the presence of drugs.

Through research, metrics, tests, and standards, ITL's Forensics Science Program makes significant contributions to the criminal justice system of the United States.



ITL Releases Test Tool for Meaningful Use Certification of Electronic Health Records

ITL recently released an interoperability test tool in support of the 2014 Edition Electronic Health Record (EHR) certification program. ITL researchers developed the tool in response to the Medicare and Medicaid Programs Electronic Health Record Incentive Program--Stage 2, Final Rule. This final rule specifies the Stage 2 criteria (meaningful use objectives and measures) that eligible professionals, eligible hospitals, and critical access hospitals must meet in order to qualify for Medicare and/or Medicaid EHR incentive payments. The "randomizer" tool is designed to match providers with test EHR vendors so that the two parties exchanging the summary of care record use different vendor software, yet demonstrate interoperability. The NIST Randomizer test tool is available to the public at this website.

ITL Collaborates on Design of Rheometers for Dense Suspensions

A team of researchers from ITL and NIST's Engineering Laboratory (EL) have been awarded 40 million hours of supercomputer time for calendar year 2014 from the Department of Energy (DOE) to support the design of rheometers for large-particle dense suspensions such as concrete. The results will benefit the cement and concrete industry as well as a wide array of other industries that use rheometers and mixers on dense suspensions such as food processing, water treatment, coatings, and pharmaceuticals. The award is a Phase III allocation resulting from a series of proposals submitted to DOE's peer-reviewed Innovative and Novel Computational Impact on Theory and Experiment (INCITE).

In Phase III of this project, researchers will perform highly detailed simulations of various rheometer designs, operating on many-particle suspensions with a wide range of particle sizes and shapes suspended in a non-Newtonian fluid matrix. Novel rheometer blade designs suggested by the simulations will be constructed using additive manufacturing techniques for polymers and metals. Experiments using these rheometers will be compared to the simulation results. The research team includes William George, Marc Olano, Steven Satterfield, and Judith Terrill of ITL, Nicos Martys and Edward Garboczi of EL, and Pascal Hebraud of CNRS/ESPCI (France). The simulations will be run in the Leadership Computing Facility of Argonne National Laboratory on the "Mira IBM BlueGene/Q" system, which is currently ranked number 5 in the "Top 500" list of supercomputer installations.

Staff Recognition

At the annual NIST Awards Ceremony on December 11, 2013, the following ITL employees received awards:

Paul E. Black – Bronze Medal for leadership in the development of software assurance test methods and reference data.

Richard Kissel – Bronze Medal for increasing small and medium-size business awareness of information security through NIST's information security outreach program.

Elaine M. Newton – Bronze Medal for sustained leadership in the preservation of the global voluntary consensus standards system for information and communications technologies.

Lori Buckland (posthumously) – Director's Award for Excellence in Administration for support of ITL's Text Retrieval Conference, Text Analysis Conference, and TRECVID Video Retrieval Evaluation.

Frederick (Tim) Boland – Equal Employment Opportunity/ Diversity Award for excellence in promoting diversity and accessibility at NIST, and for dedication to removing barriers for all in information technology use.

In addition, the following ITL staff members will receive the Department of Commerce Gold and Silver Medal Awards at a department awards ceremony in January.

Mark Carson, **Sheila Frankel**, **Douglas Montgomery**, **Stephen Nightingale** and **Darrin Santay** – Gold Medal for development of the USGv6 Program that established the U.S. Government as a world leader in adoption of the next-generation Internet protocol IPv6.

Brian Antonishek, **Athanasios Karygiannis**, **Stephen Quirolgico**, and **Jeffrey Voas** – Gold Medal for developing innovative techniques to secure and measure the performance of smartphones and applications.

Audrey Tong – Silver Medal for developing a novel evaluation framework/metrology and data supporting significant advances in automatic translation of foreign language handwriting.

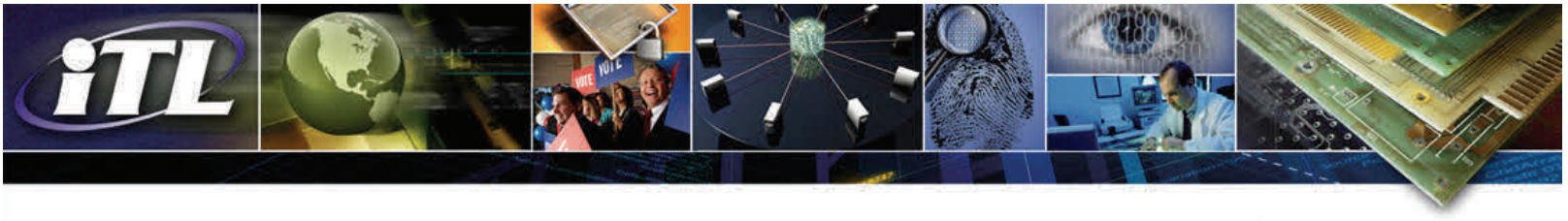
ITL staff also received the following external awards:

FierceGovernmentIT announced its Second Annual Fierce 15 Winners, and the list of 15 creative and innovative federal employees includes three ITL leaders:

- **Patrick Grother**, Biometric Testing Project Leader in ITL's Information Access Division
- **Naomi Lefkovitz**, Senior Privacy Policy Advisor, Office of the ITL Director
- **Kevin Stine,** Leader of the Security Outreach and Integration Group, Computer Security Division

FierceGovernmentIT is a trusted and growing online source for in-depth federal IT reporting. The benchmark for inclusion in the Fierce 15 list is high; the publication recognizes federal employees who have demonstrated groundbreaking creativity and innovation.

NIST Fellow **Ron Ross** has been recognized with the inaugural Lynn F. McNulty Tribute U.S. Government Information Security Leadership Award from the $(ISC)^2$ U.S. Government Advisory Board for Cyber Security. The award recognizes Ross' "key role in establishing cybersecurity requirements for federal agencies for decades." The award was established in 2012 following the death of McNulty, former ITL Associate Director for Computer Security and a leading innovator of information security in the federal arena in the 1990s.



Selected New Publications

Secure Domain Name System (DNS) Deployment Guide
By Ramaswamy Chandramouli and Scott Rose
NIST Special Publication 800-81-2
September 2013

The Domain Name System (DNS) is a distributed computing system that enables access to Internet resources by user-friendly domain names rather than IP addresses, by translating domain names to IP addresses and back. The DNS infrastructure is made up of computing and communication entities called Name Servers each of which contains information about a small portion of the domain name space. The domain name data provided by DNS is intended to be available to any computer located anywhere in the Internet. This document provides deployment guidelines for securing DNS within an enterprise. It provides extensive guidance on maintaining data integrity and performing source authentication.

A Framework for Designing Cryptographic Key Management Systems
By Elaine Barker, Miles Smid, Dennis Branstad, and Santosh Chokhani
NIST Special Publication 800-130
August 2013

This Framework for Designing Cryptographic Key Management Systems (CKMS) contains topics that should be considered by a CKMS designer when developing a CKMS design specification. For each topic, there are one or more documentation requirements that need to be addressed by the design specification. Thus, any CKMS that addresses each of these requirements would have a design specification that is compliant with this Framework.

Effects of JPEG 2000 Lossy Image Compression on 1000 ppi Latent Fingerprint Casework
By Shahram Orandi, John M Libert, John D. Grantham, Frederick R. Byers, Lindsay M. Petersen, and Michael D. Garris
NISTIR 7780 Rev. 1
October 2013

This paper presents the findings of a study conducted to measure the impact of JPEG 2000 lossy compression on the comparison of 1000 ppi latent fingerprint imagery and 1000 ppi exemplar fingerprint imagery. Combinations of image pairs that vary by the compression rate applied to one of the images in the pair are observed and analyzed. The impact of lossy compression to both Galton and non-Galton-based features of a fingerprint is measured by professional judgment of expert fingerprint examiners. The impact of compression is analyzed by quantifying multiple decisions relative to different levels of loss incurred during image compression. In addition to measuring the perceived visual impact of compression on the aforementioned features of the fingerprint, the paper also looks at the impact of lossy compression on the examiner's ability to correctly render their identification decisions.

Fingerprint Scanner Affordances
By Michelle Steves, Brian Stanton, Mary Theofanos, Dana Chisnell, and Hannah Wald
NISTIR 7944
September 2013

This study examines the light emitting diode (LED) indicators and instructional icons on the fingerprint scanner type in place in U.S. ports of entry (at the time of the study) to learn if people interpret these features as intended, are guided through the fingerprint collection process, and whether they can present usable fingerprint samples to the scanner without assistance. The results from this study will be used to inform the development of a "self-service" fingerprinting solution.

A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems
By Eric Simmon, Kyoung-Sook Kim, Eswaran Subrahmanian, Ryong Lee, Frederic de Vaulx, Yohei Murakami, Koji Zettsu, and Ram D. Sriram
NISTIR 7951
August 2013

A key aspect of the next-generation Smart Networked System (SNS) is the bridge between the physical and virtual worlds. These systems that tightly interlink the cyber and physical worlds are often referred to as Cyber-Physical Systems (CPS). A CPS is the "integration of computation with physical processes" and uses sensors and actuators to link the computational systems to the physical world. The interlinked networks of sensors, actuators and processing devices create a vast network of connected computing resources, things, and humans that we will refer to as a Smart Networked System. This publication discusses five technologies that are core to the concept of a SNS: networked computer systems, real-time systems, wireless sensor/actuator networks, social networks, and cloud computing services.

Measurement Uncertainty in Cell Image Segmentation Data Analysis
By Jin Chu Wu, Michael Halter, Raghu N. Kacker, John T. Elliot, and Anne L. Plant
NISTIR 7954
August 2013

Cell image segmentation is a part of quantitative studies regarding cell movement and cell behavior, and it plays a critical role in molecular biology and cellular biochemistry. Therefore, it is fundamentally important to evaluate the performance levels of cell image segmentation algorithms. In our previous study, the performance metrics for cell image segmentation algorithms were proposed. The sampling variability can result in measurement uncertainties. In this article, the uncertainty of the measure, i.e., the total error rate, in the cell image segmentation is computed in terms of standard error and 95 % confidence interval using bootstrap method as well as an analytical method. Examples are provided.

Compensating Operators and Stable Backward in Time Marching in Nonlinear Parabolic Equations
By Alfred S. Carasso
NISTIR 7967
November 2013

Step by step time-marching schemes are fundamental tools in the numerical exploration of well-posed nonlinear evolutionary partial differential equations. However, when the initial value problem is ill-posed, such stepwise numerical schemes are necessarily unconditionally unstable and result in explosive noise amplification. This paper outlines a novel stabilized time-marching procedure for computing nonlinear parabolic equations on 2D rectangular regions, backward in time.

Upcoming Technical Conferences

2014 Cybersecurity Innovation Forum
Dates: January 28-30, 2014
Place: Baltimore Convention Center, Baltimore, Maryland
Sponsors: National Cybersecurity Center of Excellence, Department of Homeland Security, National Security Agency, and NIST
Cost: $495

The forum will cover the existing threat landscape and provide presentations and keynotes on current and emerging practices, technologies and standards. The 2014 forum will provide action-oriented outputs to fuel voluntary principle-driven consensus-based standards efforts, create opportunities for industry growth and drive research activities, and define use cases for subsequent exploration, which in turn will feed back into the coming years' forums, continually evolving the state of the art.
NIST contact: Melanie Cook

Cryptographic Key Management Workshop 2014
Dates: March 4-5, 2014
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $26

The purpose of the workshop is to discuss a draft of NIST Special Publication 800-153, A Profile for U.S. Federal CKMS. Available for public comment prior to the workshop, the document establishes specific requirements for federal organizations wanting to use or operate a CKMS, either directly or under contract. The Profile addresses the topics included in SP 800-130, A Framework for Designing Cryptographic Key Management Systems, and includes discussions on CKMS testing, procurement, installation, administration, operation, maintenance, and use.
NIST contact: Elaine Barker

Cloud Computing Forensic Science Workshop
Date: March 24, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None

This workshop will present experts in the fields of cloud, digital forensics, and measurement for sessions on the perspectives, vision, current state, and future of cloud forensic science. Leaders in cloud computing and digital forensics from government, industry, and academia should attend, as well as architects, researchers, and implementers of cloud computing and digital forensics technologies.
NIST contact: Michaela Iorga,

The Intersection of Cloud and Mobility
Dates: March 25-27, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None

As part of its continuing cloud computing series, ITL is sponsoring a new forum on cloud and mobility. Topics will include federal perspectives on and vision of cloud and mobility, current and future intersections of cloud and mobility, challenges and lessons learned, and the path forward to a federated mobile cloud.
NIST contacts: Michaela Iorga and Frederic de Vaulx

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

The NIST campus in Gaithersburg, Maryland.

Credit: NIST

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

To subscribe to the electronic edition of the ITL Newsletter, go to ITL homepage