FY 2005 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in previous ITL Technical Accomplishment reports are not repeated.

Anderson, D.M., Cermeli, P., Fried, E., Gurtin, M.E., McFadden, G.B., *General Dynamical Sharp-interface Conditions for Phase Transformations in Viscous Heat-Conducting Fluids*, Journal of Fluid Mechanics, to be published

The purpose of this paper is to develop, from basic considerations, a complete set of equations governing the evolution of a sharp interface separating two fluid phases undergoing transformation. For situations in which a phase transformation does not occur, so that the phase interface is a material surface, the governing bulk and interfacial equations are well-developed and agreed upon. Focusing on the interface, the relevant equations are the conventional balances for mass, linear momentum, and energy, augmented by suitable constitutive equations. But when a phase transformation does occur, the interfacial expressions for balance of mass, momentum, and energy fail to provide a closed description and must be supplemented by an equation that accounts for the microphysics underlying the exchange of material between phases. For this purpose we employ the formalism of configurational forces to derive the appropriate generalization of the Gibbs-Thomson equation for a fluid-fluid interface under non-equilibrium conditions.

Avilés, A.I., Ankenman, B.E., Pinheiro, J.C., *Assembled Designs for Estimation of Location, Dispersion, and Random Effects*, Technometrics, to be published

In many experimental settings, different types of factors affect the measured response. The factors that can be set independently of each other are called crossed factors. Nested factors cannot be set independently because the level of one factor takes on a different meaning when other factors are changed. Random nested factors arise from quantity designations and from sampling and measurement procedures. The variances of the random effects associated with nested factors are called variance components. Factor effects on the average are called location effects. Dispersion effects are the effects of the crossed factors on the variance of a response. For situations where crossed factors have effects on the different variance components, then sets of dispersion effects must be identified and estimated to achieve robustness. The main objective of this research is to provide nearly D-optimal experimental design procedures for estimating the location effects of crossed factors, the variance components associated with two nested factors, and the dispersion effects that crossed factors may have on the two variance components. A general class of experimental designs for mixed-effects models with random nested factors, called assembled designs, is introduced in Ankenman, Avilés, and Pinheiro (2003). The use of assembled designs for robustness experiments is introduced. When there are dispersion effects, a heuristic algorithm for finding a nearly D-optimal assembled design with two variance components for a given budget is provided. Ready to use computer programs for the presented experimental design procedures and analysis technique are discussed. This research provides the practitioner with clear guidelines about the best design available for their needs.

Barker, W.C., Dray, J., Chandramouli, R., Schwarzhoff, T., Polk, T., Dodson, D., Mehta, K., Gupta, S., Burr, W., Grance, T., *Personal Identity Verification of Federal Employees and Contractors*, Federal Information Processing Standard (FIPS) 201, http://csrc.nist.gov/publications/fips/index.html, February 25, 2005

FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that issue smart cards as identification credentials and that use the cards to authenticate an individual's identity. FIPS 201 has been issued in two parts to allow for a smooth migration to a secure, reliable personal identification process. The first part of FIPS 201 (PIV I) describes the minimum requirements needed to meet the control and security objectives of HSPD 12, including the process to prove an individual's identity. The second part (PIV II) of FIPS 201 explains the many components and processes that will support a smart-card-based platform, including the PIV card and card and biometric readers. The specifications for PIV components support interoperability between components in systems and among the different department and agency systems. FIPS 201 responds to Homeland Security Presidential Directive (HSPD) 12, issued by President Bush on August 27, 2004, which cited the wide variations in the quality and security of the forms of identification used to gain access to federal and other facilities, and called for the development of a mandatory standard for secure and reliable forms of identification to be used throughout the federal government. The directive stated the government's requirements for a common government-wide identification system that would enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The FIPS was approved by Carlos M. Gutierrez, the U.S. Secretary of Commerce, on February 25, 2005.

Barker, W.C., *E-Government Security Issues and Measures*, Handbook of Information Security, John Wiley & Sons, Hossein Bidgoli (Ed.), California State University at Bakersfield, to be published

The Handbook will be a three-volume, 2,400-page reference source providing state-of-the-art information concerning the information, computer and network security with coverage of the core topics. The audience is four-year colleges and universities with Computer Science, MIS, IT, IS, E-commerce, and Business departments, and public, private, and corporate libraries and a diverse group of professionals interested in this fast-growing field. The Handbook will be available as a printed work as well as in an online version. Approximately 200 articles will comprise this publication. This chapter identifies current security issues associated with implementation of E-Government initiatives and the security measures needed for, and available to, address these issues. The set of E-Government services that this chapter treats includes electronic publishing, interactive information services, transaction processing, and delivery of government services. The classes of security issues addressed include availability, integrity, confidentiality, and privacy. Security measures discussed include security mechanisms (e.g., cryptography, firewalls, and operating system security), system design and configuration principles (e.g., hardware, software, and data backups), and policy and procedural measures (e.g., planning, testing, certification, monitoring/auditing, and accreditation).

Beichl, I., Bullock, S., Song, D., *A Quantum Algorithm Detecting Concentrated Maps*, NIST Journal of Research, to be published

Let for , some number of quantum bits. Using calls to a classical oracle evaluating and an -bit memory, it is possible to determine whether is one-to-one. For some radian angle , we say is -concentrated iff for some given and any . This manuscript presents a quantum algorithm that distinguishes a -concentrated from a one-to-one in calls to a quantum oracle function with high probability. For radians, the quantum algorithm outperforms the obvious classical algorithm on average, with maximal outperformance at radians. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant .

Black, P.E., Software Write Block, *Testing Support Tools Validation – Part A – Test Plan, Test Design, and Test Case Specification*, NISTIR 7207-A, to be published

This NIST Internal Report consists of two parts. Part A covers the planning, design, and specification of testing and reviewing the Software write block (SWB) support tools. Part B, which is a companion document, covers the test and code review support report. Part A gives a test plan, test design specification, and test case specification for validation of the disk drive software write block testing support tools. The test plan defines the scope, including specific items and features to be validated, the methodology or approach for validating the SWB test support tools, and some technical background. The test design specification gives requirements for validating SWB tools. These requirements yield assertions. Each assertion leads to one or more code reviews or test cases consisting of preconditions, values, and method(s) for gaining confidence that the SWB test support tools correctly assess those assertions, a test procedure and the expected results. The test case specification gives details of test and review procedures for setting up the test, performing the test, and assessing the results. Appendices include a code review checklist and source code for validation programs. Part B reports the results of reviewing the source code of the SWB test tools and testing them against Part A of the companion NIST Internal Report entitled Software Write Block Testing Support Tools validation – Test Plan, Test Design Specification, and Test Case Specification.

Black, P.E., Software Write Block, *Testing Support Tools Validation – Part B – Test and Code Review Report*, NISTIR 7207-B

This NIST Internal Report consists of two parts. Part A covers the planning, design, and specification of testing and reviewing the Software write block (SWB) support tools. Part B, which is a companion document, covers the test and code review support report. Part A gives a test plan, test design specification, and test case specification for validation of the disk drive software write block testing support tools. The test plan defines the scope, including specific items and features to be validated, the methodology or approach for validating the SWB test support tools, and some technical background. The test design specification gives requirements for validating SWB tools. These requirements yield assertions. Each assertion leads to one or more code reviews or test cases consisting of preconditions, values, and method(s) for gaining confidence that the SWB test support tools correctly assess those assertions, a test procedure and the expected results. The test case specification gives details of test and review procedures for setting up the test, performing the test, and assessing the results. Appendices include a code review checklist and source code for validation programs. Part B reports the results of reviewing the source code of the SWB test tools and testing them against Part A of the companion NIST Internal Report entitled Software Write Block Testing Support Tools validation – Test Plan, Test Design Specification, and Test Case Specification.

Blanz, V., Grother, P., Phillips, P. J., Vetter, T., *Face Recognition Based on Frontal Views Generated from Non-Frontal Images*, IEEE Conference on Computer Vision and Pattern Recognition 2005, to be published

This paper presents a method for face recognition across large changes in viewpoint. Our method is based on a Morphable Model of 3D faces that represents face-specific information extracted from a dataset of 3D scans. For non-frontal face recognition in 2D still images, the Morphable Model can be incorporated in two different approaches: In the first, it serves as a preprocessing step by estimating the 3D shape of novel faces from the non-frontal input images, and generating frontal views of the reconstructed faces at a standard illumination using 3D computer graphics. The transformed images are then fed into state of-the-art face recognition systems that are optimized for frontal views. This method was shown to be extremely effective in the Face Recognition Vendor Test FRVT 2002. In the process of estimating the 3D shape of a face from an image, a set of model coefficients are estimated. In the second method, face recognition is performed directly from these coefficients. In this paper we explain the algorithm used to preprocess the images in FRVT 2002, present additional FRVT 2002 results, and compare these results to recognition from the model coefficients.

Bowdrey, M.D., Jones, J.A., Knill, E., Laflamme, R., *Compiling Gate Networks on an Ising Quantum Computer*, Physical Review A and http://arxiv.org/quant-ph, January 12, 2005

Here we describe a simple mechanical procedure for compiling a quantum gate network into the natural gates (pulses and delays) for an Ising quantum computer.

Brewer, T.L., Editor, *Computer Security Division 2004 Annual Report*, NISTIR 7219, to be published

This report covers the work conducted within the National Institute of Standards and Technology's Computer Security Division during Fiscal Year 2004. It discusses all projects and programs within the Division, staff highlights, and publications. For many years, the Computer Security Division (CSD) has made great contributions to help secure the nation's sensitive information and information systems. CSD's work has paralleled the evolution of information technology, initially focused principally on mainframe computers, to now encompass today's wide gamut of information technology devices. CSD's important responsibilities were re-affirmed by Congress with passage of the Federal Information Security Management Act of 2002 (FIMSA) and the Cyber Security Research and Development Act of 2002. Beyond the role to serve the Federal agencies under FISMA, CSD standards and guidelines are often voluntarily used by U.S. industry, global industry, and foreign governments as sources of information and direction for securing information systems. CSD's research also contributes to securing the nation's critical infrastructure systems. Moreover, the Division has an active role in both national and international standards organizations in promoting the interests of security and U.S. industry.

Bullock, S.S., Carteret, H.A., *Quantum Interferometer Circuits for Multi-Partite Entanglement*, Quantum Information and Computation, to be published

The concurrence of a pure quantum state of qubits is the component of the state vector on its spin-flip. In two qubits, it is equivalent to all other measures of entanglement, in particular a one-to-one function of the entropy of either partial trace. In the multi-partite case, any even-qubit state with a nonzero concurrence is not local but rather entangled. Here, we present quantum interferometer circuits which measure the entanglement (concurrence) of their quantum data registers. Computing the concurrence requires a sequence of such interferometers, and they function properly on mixed as well as pure even-qubit data-states.

Bullock, S.S., O'Leary, D.P., Brennen, G.K., *Asymptotically Optimal Quantum Circuits for d-level Systems*, Physical Review Letters and http://www.arxiv.org/, to be published

As a qubit is a two-level system whose state space is spanned by   and , so a qudit is a -level system whose state space is spanned by ,…, . Quantum computation has stimulated much recent interest in algorithms factoring unitary evolutions of an -qubit state space into component two-particle unitary evolutions. In the absence of symmetry, Shende, Markov, and Bullock use Sard’s theorem to prove that at least   two-qubit unitary evolutions are required, while Vartiainen, Moettoenen, and Salomaa (VMS) use the   matrix factorization and Gray codes in an optimal order construction involving two-particle evolutions. In this work, we note that Sard’s theorem demands   two-qudit unitary evolutions to construct a generic (symmetry-less) -qudit evolution. However, the VMS result applied to virtual qubits only recovers optimal order in the case that is a power of two. We further construct a decomposition for   multi-level quantum logics, proving a sharp asymptotic of   two-qudit gates and thus closing the complexity question for all -level systems (finite). Gray codes are not required.

Cowley, P., Nowell, L., Scholtz, J., *Glass Box: An Instrumented Infrastructure for Supporting Human Interaction with Information*, Hawaii International Conference on System Science (HICSS 38), January 3, 2005

In this paper, we discuss the challenges involved in developing an infrastructure to support a new generation of analytic tools for information analysts. The infrastructure provides data for establishing context about what the analyst is doing with the analytic tools, supports an integration environment to allow suites of tools to work together, and supports evaluation of the analytic tools. We discuss the functionality of the Glass Box, the challenges of evaluating adaptive systems including the capture of data for evaluation metrics, and lessons learned from our experiences to date.

Dabrowski, C., Mills, K.L., Quirolgico, S., *A Model-Based Analysis of First-Generation Service Discovery Systems*, NIST SP 500-260, to be published

Future commercial software systems will be based on distributed service-oriented architectures in which applications are composed dynamically from remote components. A key part of service-oriented computing is the ability for clients to discover remote services that fulfill specific requirements. Since the mid-1990s, various commercial and public domain designs for service discovery systems have been proposed that enable clients and services to rendezvous in a distributed system. The report characterizes such designs as first-generation service discovery systems, based on the belief that experience with these systems will lead to future, improved designs.

Using three widely used service discovery systems as a basis, this publication first presents a high level overview of the operation of service discovery protocols. A detailed generic model of first-generation service discovery systems, written in UML, follows this. The UML model provides an in-depth analysis of the alternative service discovery designs available today, including the major functional components that comprise these designs, the behaviors of these components, and the information they exchange. The report verifies the generality of the model by mapping its component element to corresponding elements of existent and emerging service discovery systems. This report also identifies issues that designers should attempt to resolve in the next generation of service discovery systems.

The analysis is then extended to provide designers of future service discovery systems with a means to evaluate designs. First, the report proposes a set of service goals that service discovery systems should strive to satisfy to ensure a desirable level of quality of service. These goals provide a basis to define metrics, for evaluation the behavior and measuring performance of system designs and implementations. Second, the report identifies potential performance issues that may arise during operation of service discovery systems. Identifying performance issues can alert designers and implementers to the potential for unexpected behavior when service discovery technology is deployed at large scale. The report presents possible solutions to performance problems that extend well-known optimization algorithms for distributed systems and present new algorithms tailored to service discovery environments.

The contributions in this report will help to improve the quality of the next generation of service discovery systems on which the service-oriented architectures of tomorrow appear likely to depend. Further, should an industry standards group choose to develop a unified specification for service discovery, the model should provide helpful input to the process.

Davis, R.A., Dunsmuir, W.T.M., Streett, S.B., *Maximum Likelihood Estimation for an Observation Driven Model for Poisson Counts*, Methodology and Computing in Applied Probability, accepted for publication

This paper is concerned with an observation driven model for time series of counts whose conditional distribution given past observations follows a Poisson distribution. This class of models is capable of modeling a wide range of dependence structures and is readily estimated using an approximation to the likelihood function. Recursive formulae for carrying out maximum likelihood estimation are provided and the technical components required for establishing a central limit theorem of the maximum likelihood estimates are given in a special case.

DerSimonian, R., Kacker, R., *Random-Effects Model for Meta-analysis of Clinical Trials: An Update*, Controlled Clinical Trials, to be published

The random-effects model is a useful approach for meta-analysis of clinical studies. It explicitly accounts for the heterogeneity of studies through a statistical parameter representing the inter-study variation. We discuss several iterative and non-iterative alternative methods for estimating the inter-study variance and hence the overall population treatment effect. We show that the leading methods for estimating the inter-study variance are special cases of a general method-of-moments estimate of the inter-study variance. The general method suggests two new two-step methods. The iterative estimate is statistically optimal and it can be easily calculated on a spreadsheet program, such as Microsoft Excel, available on the desktop of most researchers. The two-step methods are useful when a non-iterative estimate is desired.

Donnelly, D., Rust, B., *The Fast Fourier Transform for Experimentalists, Part I: Concepts*, Computing in Science and Engineering, to be published

The discrete Fourier transform (DFT) is a widely used tool for the analysis of measured time series data. The Cooley-Tukey fast Fourier transform (FFT) algorithm gives an extremely fast and efficient implementation of the DFT. This is the first of a series of three articles which will describe the use of the FFT for experimental practitioners. This installment gives fundamental definitions and tells how to use the FFT to estimate power and amplitude spectra of a measured time series. It discusses the use of zero padding, the problem of aliasing, the relationship of the inverse DFT to Fourier series expansions, and the use of tapering windows to reduce the sidelobes on the peaks in an estimated spectrum.

Dray, J.F., Guthery, S., Schwarzhoff, T., *Interfaces for Personal Identity Verification*, NIST SP 800-73, http://csrc.nist.gov/publications/nistpubs/index.html, April 11, 2005

FIPS 201, Personal Identity Verification for Federal Employees and Contractors, specifies that the identity credentials must be stored on a smart card. Special Publication 800-73 contains technical specifications for smart card interfaces used to retrieve and use identity credentials. These specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying PIV data model, communication interface, and application programming interface (API). SP 800-73 enumerates requirements where the standards include options and branches and also constrains implementers' interpretation of the standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications. Specifications include the PIV data model, API, and card interface requirements necessary to comply with the mandated use cases for interoperability across deployments or agencies. Interoperability is defined as the use of PIV identity credentials such that client APIs, compliant card applications and compliant integrated circuit cards can be used interchangeably by information processing systems across Federal agencies. SP 800-73 does not address the back-end processes that must be performed to attain full identity assertion. The document describes two realizations of the client-application programming and card command interfaces for personal identity verification: the transitional interfaces and the end-point interfaces. Transitional interfaces may be used by agencies with an existing identity card program as an optional step in evolving to the end-point interfaces. End-point interfaces are used by agencies without an existing identity card program and by agencies that elect to evolve to the end-point interface in one step rather than two. SP 800-73 is divided into three parts as follows: Part 1, providing the specification for that which is common to both the transitional and end-point interfaces and guidance on strategies for migrating from the transitional interfaces to the end-point interfaces; Part 2, describing the subsets of GSC-ISv2.1 that comprise the transitional interfaces to the PIV data model; and Part 3, describing in detail the end-point interfaces to the PIV data model.

Filliben, J.J., *Statistical Approaches in the NIST World Trade Center Analysis*, Proceedings of the 9th International Conference on Structural Safety and Reliability, Rome, Italy, June 19-23, 2005

The Federal Building and Fire Safety Investigation of the World Trade Center Disaster is currently essentially completed. The pre-collapse progression was extremely complicated, with structural, thermal, dynamic and stochastic interdependencies across time and space. Four pre-collapse stages (a simplification of reality) will be discussed: aircraft impact, fire spread, thermal propagation through insulation, and structural deformation. Engineering issues and the statistical methodologies to address them will be discussed. A major challenge in the statistical analysis of the World Trade Center was the relatively meager amount of data – little physical evidence remained that could shed light on important events occurring in the core of the WTC buildings. In this regard, the study was simultaneously assisted – and complicated – by reliance on computational engineering virtual data – primarily in the form of NIST FDS (Fire Dynamics Simulator) and phase-specific FEA (Finite Element Analysis) computational models. As analyses progress from component to subassembly to global models, such computational models require characterization and validation – it will be shown how experiment design played an important role in this regard. Various other statistical analysis techniques (e.g., complex demodulation for assessing post-impact building oscillation frequency and – indirectly – building damage) will also be discussed. This paper will emphasize the methodologies employed. Conclusions and recommendations resulting from the Federal Building and Fire Safety Investigation of the World Trade Center Disaster are presented in the investigation final report, due to be released in draft form in the Spring of 2005.

Fong, E., *Conformance Testing of the Government Smart Card*, NISTIR 7210, http://xw2k.sdct.itl.nist.gov/smartcard, February 15, 2005

A conformance Test suite helps to ensure consistency between a specification and the behavior of a product. This paper presents the conformance testing methodology for the Government Smart Card Interoperability Specification. It starts with some basic terminology in the area of testing and discusses a methodology on how to design conformance test. The test strategy used for the design of this conformance test suite uses the extended Markup Language (XML), which is a declarative, implementation-neutral markup language. Finally, the paper explores the benefits and limitations with the conformance testing approach for the Government Smart Card Interoperability Specification.

Fong, J., *The Role of Engineering Statistics in a Reference Benchmark Approach to Verification and Validation of Multi-Physics Simulations of High-Consequence Engineering Systems*, Proceedings of the Stanford Mechanics Symposium on "Applied Mechanics and Multi-Physics Simulations of High-Consequence Engineering Systems" in honor of Professor Charles R. Steele, Stanford University, Stanford, California, April 18, 2005

Three basic tools in engineering statistics are considered: (A) Error Analysis, (B) Experimental Design, and (C) Uncertainty Analysis. It is argued that engineers who use mathematical, statistical, or computational models to simulate "high-consequence" systems for design, manufacturing, construction, maintenance, and retrofitting, need (A), (B), and (C) to ensure the correctness of those models by verification and validation (V&V). To support this argument, we examine a novel approach to V&V by extending three ideas in metrological science to numerical simulations: (I-1) expression of uncertainty as defined in ISO 1993 Guide to the Expression of Uncertainty in Measurement, (I-2) design of experiments, and (I-3) reference benchmarks for calibration and interpretation of key comparison and inter-laboratory studies. To illustrate the role of engineering statistics in this new approach, we provide four specific examples: (a) the uncertainty analysis of a length measurement process using standard 50 mm gauge blocks, (b) the verification of 12 simulations of the deformation of a cantilever beam, (c) the verification and validation of 15 simulations of the unconstrained cylindrical bending of 1.0-mm-thick aluminum sheet, and (d) the calculation of a mean time to failure due to fire for a uniformly loaded 100-column single-floor steel grillage.

Gallagher, L.J., Offutt, A.J., Cincotta, A.V., *Integration Testing of Object-Oriented Components Using Finite State Machines*, Software Testing, Verification, and Reliability (STVR) International Journal, to be published

In object-oriented terms, one of the goals of integration testing is to ensure that messages from objects in one class or component are sent and received in the proper order and have the intended effect on the state of external objects that receive the messages. This research extends an existing single-class testing technique to integration testing of multiple classes. The previous method models the behavior of a single class as a finite state machine, transforms that representation into a data flow graph that explicitly identifies the definitions and uses of each state variable of the class, and then applies conventional data flow testing to produce test case specifications that can be used to test the class. This paper extends those ideas to inter-class testing by developing flow graphs and tests for an arbitrary number of classes and components. It introduces flexible representations for message sending and receiving among objects and allows concurrency among any or all classes and components. Data flow graphs are stored in a relational database, and database queries are used to gather def-use information. This approach is conceptually simple, mathematically precise, quite powerful, and general enough to be used for traditional data flow analysis. This testing approach relies on finite state machines, database modeling and processing techniques, and algorithms for analysis and traversal of directed graphs. The paper presents empirical results of the approach applied to an automotive system.

Garris,.M.D., Wilson, C.L., *NIST Biometric Evaluations and Developments*, NISTIR 7204 (February 9, 2005) http://www.itl.nist.gov/iaui/894.03/pact/pact.html and Photonics for Port and Harbor Security Conference Proceedings, Defense & Security Symposium, Orlando, Florida, March 2005

This paper presents an R&D framework used by the National Institute of Standards and Technology (NIST) for biometric technology testing and evaluation. The focus of this paper is on fingerprint-based verification and identification. Since 9-11 the NIST Image Group has been mandated by congress to run a program for biometric technology assessment and biometric systems certification. Four essential areas of activity are discussed: 1.) developing test datasets, 2.) conducting performance assessment; 3.) technology development; and 4.) standards participation. A description of activities and accomplishments are provided for each of these areas. In the process, methods of performance testing are described and results from specific biometric technology evaluations are presented. This framework is anticipated to have broad applicability to other technology and application domains.

Gentile, C., *Sensor Location through Linear Programming with Triangle Inequality Constraints*, IEEE International Conference on Communications, Seoul, Korea, May 16-20, 2005

Interest in dense sensor networks due to falling price and reduced size has motivated research in sensor location in recent years. While many algorithms can be found in literature, no benchmark exists and most papers fail to compare their results to other competing algorithms. To our knowledge, the algorithm that achieves the best performance in sensor location uses semi-definite relaxation of a quadratic program to solve the sensor location. We propose solving the same program, however without relaxing the constraints, but rather transforming them into linear triangle inequality constraints. Our linear program ensures a tighter solution to the problem. We benchmark ours against the competing algorithm, and provide extensive experimentation to substantiate the robustness of our algorithm even in the presence of high levels of noise.

Gilsinn, D.E., *Discrete Fourier Series Approximation to Periodic Solutions of Autonomous Delay Differential Equations*, Proceedings of IDETC/CIE 2005: ASME 2005 International Design Engineering Technical Conference & Computers & Information in Engineering Conference, Long Beach, California, September 24-28, 2005

This paper describes the algorithmic details involved in developing high order Fourier series representations for periodic solutions to autonomous delay differential equations. Although, the final approximate Fourier coefficients are computed by way of a nonlinear minimization algorithm, the steps to set up the objective function are shown to involve a sequence of matrix-vector operations. By proper coordination these operations can be made very efficient so that high order approximations can easily be obtained. An example of the calculations is shown for a Van der Pol equation with unit delay.

Griffith, D., Sriram, K., Golmie, N., *Protection Switching for Optical Bursts Using Segmentation and Deflection Routing*, IEEE Communications Letters 2005, to be published

Burst segmentation in OBS networks can significantly reduce the amount of data that is lost due to contention events by dropping or deflecting only the portion of a burst that overlaps another contending burst. In this letter, we demonstrate how segmentation combined with deflection routing can be used to reduce the amount of data that is lost when network elements fail. By enabling an OBS switch to deflect the tail-end segments of bursts that are in transmission as soon as it becomes aware of a downstream link failure, the retransmission of lost data can be reduced.

Gurski, K.F., McFadden, G.B., Miksis, M.J., *The Effect of Contact Lines on the Rayleigh Instability with Anisotropic Surface Energy*, SIAM Journal on Applied Mathematics, to be published

We determine the linear stability of a rod or wire on a substrate subject to capillary forces arising from an anisotropic surface energy for a range of contact angles between $-\pi/2$ and $\pi/2$. The Unperturbed rod is assumed to have infinite length with a uniform cross-section given by a portion of the two-dimensional equilibrium shape. We examine the effect of surface perturbations on the total energy. The stability of the equilibrium interface is reduced to determining the eigenvalues of a coupled system of ordinary differential equations. This system is solved both asymptotically and numerically for several types of anisotropic surface energies. We find that, in general, the presence of the substrate has a stabilizing effect as compared to a free rod.

Harman, D., *Text Retrieval Conference and Message Understanding Conference*, Encyclopedia of Language and Linguistics, to be published

The Text REtrieval Conferences (TRECs) and the Message Understanding Conferences (MUCs) are two critical evaluation efforts in natural language understanding that in large part have shaped the research in those areas during the 1990s. The TREC work concentrated on research in information retrieval, starting with the basic retrieval task of finding documents in response to a question, but then branching into multiple variations on this central theme. The MUC tests have targeted information extraction, in particular how to find and aggregate specific information on entities such as persons, locations, and organizations, and the relationships between such entries.

Harman, D., *The History of IDF and its Influences on IR and Other Fields*, Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones, to be published

The surprisingly simple IDF measure developed in 1972 by Karen Sparck Jones has continued to dominate the term weighting metrics used in information retrieval, despite several efforts to develop more complex measures of term distribution. It has been incorporated in (probably) all information retrieval systems and used in languages other than English. This chapter presents the origins of the IDF measure and how it evolved into the measure that is used today.

Harman, D., *The Importance of Focused Evaluations: A Case Study of TREC and DUC*, Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones, to be published

Evaluation has always been an important part of scientific research, and in information retrieval, this evaluation has mostly been done using test collections. In 1992, a new test collection was built at the National Institute of Standards and Technology (NIST), and a focused evaluation (the Text REtrieval Conference or TREC) was started to use the collection. Results from nearly 12 years of this focused evaluation show significant technology transfer across systems, leading to major improvements in system performance. Focused evaluations also create the ability to target specific problems in language technology, such as retrieval across languages, and to design tasks for evaluation such that issues can be studied concurrently by multiple groups. This chapter will discuss some of the tasks that have been examined in TREC, including critical factors in the design of those evaluations. Additionally a second focused evaluation, the Document Understanding Conference (DUC), which evaluates text summarization, will be discussed.

Harman, D., Voorhees, E.M., *TREC: An Overview*, Annual Review of Information Science and Technology, Volume 40, to be published

The Text REtrieval Conference (TREC) is a workshop series designed to build the infrastructure necessary for large-scale evaluation of text retrieval technology. Participants in the workshops (over 100 groups in the latest TREC) have been drawn from the academic, commercial, and government sectors, and have included representatives from more than 20 different countries. These collective efforts have accomplished a great deal: a variety of large test collections have been built for both traditional "ad hoc" retrieval and related tasks such as cross-language retrieval, speech retrieval, and question answering; retrieval effectiveness has approximately doubled; and many commercial retrieval systems now contain technology first developed in TREC. This chapter chronicles the first twelve years of TREC, with extensive references to the experiments that have been done during those years.

Hash, J., Bowen, P., Johnson, A., Smith, C.D., Steinberg, D.I., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act*, NIST SP 800-66, http://csrc.nist.gov/publications, March 28, 2005

This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule and does not supplement, replace, or supersede the HIPAA Security Rule itself.

Hash, J., *Integrating IT Security into the Capital Planning and Investment Control Process*, ITL Bulletin, http://csrc.nist.gov/publications, January 2005

To assist federal agencies with effectively integrating security into the capital planning and investment control (CPIC) process, NIST has released Special Publication (SP) 800-65, Integrating IT Security into the Capital Planning and Investment Control Process. It provides tips and pointers in addition to a sample methodology, which can be used to address prioritization of security requirements in support of agency business units. The publication describes risk factors that should be considered in addressing security investments and links the current Office of Management and Budget (OMB) guidance in this area to the current Federal Information Security Management Act (FISMA) including the Plan of Action and Milestones (POA&M) process which all agencies are required to implement. NIST Special Publication 800-65 describes in detail the underpinning methodology which can be easily applied to address security requirement integration and prioritization into an agency's capital planning and investment planning process using well understood concepts related to the current FISMA framework and existing NIST standards and guidance. This ITL Bulletin summarizes the special publication.

Hash, J., *Integrating IT Security into the Capital Planning and Investment Control Process*, NIST SP 800-65, http://csrc.nist.gov/publications, January 27, 2005

Traditionally, information technology (IT) security and capital planning and investment control (CPIC) processes have been performed independently by security and capital planning practitioners. However, the Federal Information Security Management Act (FISMA) of 2002 and other existing federal regulations charge agencies with integrating the two activities. In addition, with increased competition for limited federal budgets and resources, agencies must ensure that available funding is applied towards the agencies' highest priority IT security investments. Applying funding towards high-priority security investments supports the objective of maintaining appropriate security controls, both at the enterprise-wide and system level, commensurate with levels of risk and data sensitivity. This special publication (SP) introduces common criteria against which agencies can prioritize security activities to ensure that corrective actions identified in the annual FISMA reporting process are incorporated into the capital planning process to deliver maximum security in a cost-effective manner.

Hewett,T.T., Scholtz, J.C., *A Questionnaire to Assess the Difficulty of Open Source Analysis Taskings*, 2005 International Conference on Intelligence Analysis, to be published

Our goal is to produce metrics for assessing the impact of software tools and environments produced for the intelligence community. To this end we are developing a task difficulty questionnaire to attempt to identify and assess the impact of task characteristics that make some open source analytic taskings harder than. In this paper we present the most recent version of the questionnaire and invite comments and suggestions for improvement.

Hewett,T.T., Scholtz, J.C., *Developing a Difficulty Metric for Open Source Analytic Tasks*, 2005 International Conference on Intelligence Analysis, to be published

Our goal is to produce metrics for assessing the impact of software tools and environments produced for the intelligence community. To this end we need to understand the variables that make some analytic tasks harder than others and to determine which data need to be captured to meaningfully assess the effects of these variables on process and effectiveness. In this paper we describe the initial stages of development of a task difficulty questionnaire and report some feedback on the questionnaire collected from professional intelligence analysts in the context of their work. We discuss some additional steps needed to further clarify and refine the task difficulty questionnaire and explore the implications for possible task difficulty metrics.

Hornikova, A., Guthrie, W.F., *A Survey of Key Comparisons*, Proceedings of the Measurement Science Conference 2005, Anaheim, California, January 17, 2005

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Metrology Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately 120 Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a large set of completed comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons has now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Hornikova, A., Guthrie, W.F., *Troubleshooting Key Comparisons*, Proceedings of Joint Statistical Meetings 2004, Toronto, Canada, December 2004

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Measurement Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately sixty Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a rich set of real comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons has now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Huang, I-F., Hwang, I-S., Shie, H-J., *Guaranteed Quality of Recovery in WDM Mesh Networks*, IEEE Proceedings Communications Research Publication, 2005, to be published

This study proposes a mechanism of guaranteed quality of recovery (GQoR) for Wavelength Division Multiplexing (WDM) mesh networks. Four GQoR levels are used to support customized services, and each of them is mapped to the adaptive recovery methodology. Once a failure occurs, the control system activates the recovery mechanism in compliance with the GQoR level. If the protection procedure fails as well, the proposed algorithm will then execute the restoration mechanism. Consequently, the recovery success rate is increased. This paper examines the shared segment recovery methods to establish backup path; therefore, it is well suited for large-scale networks and also increases the bandwidth utilization of the networks. Furthermore, a node deals only with its own routing information by employing the distributed control, so the fault recovery procedure can be speeded up. Simulation results reveal that the proposed method has greater performance of lower blocking probability and mean hop number than other methods previously reported in the literature.

Hwang, I-S., Huang, I-F., Chien, C-D., Su, D., *Efficient Path-Segment Protection Utilizing Logical-ring Approach in WDM Mesh Networks*, Institute of Electronics, Information and Communication Engineers (IEICE) Transactions on Information & Systems, 2006, to be published

This work proposes a distributed fault protection mechanism called the Dynamic-Shared Segment Protection (DSSP) algorithm for WDM (Wavelength Division Multiplexing) mesh networks. The study explores the shared protection scheme in the network with constraints of Shared Risk Link Group (SRLG) and Shared Bandwidth Assignment (SBA). The objects are to assure high probability of path protection and efficient use of network resources. The proposed approach exploits the segment protection mode, which accommodates the characteristics of both path-based and link-based protections, for providing finer service granularities, to satisfy the versatile requirements of critical applications in foreseeable future. The protection paths are pre-calculated from the logical-rings, which are dynamically created from mesh networks. Accordingly, the DSSP algorithm is able to select the suitable logical-rings to be protection paths quickly once a working path is assigned. To show that DSSP can improve performance efficiency, simulations are conducted using four networks (NSFNET, USANET, Mesh 6x6, Mesh 9x9) for a comparative study of the proposed DSSP versus ordinary shared protection schemes and SLSP (Short Leap Shared Protection). Simulation results reveal that the proposed DSSP method results in much lower blocking probability and has higher network utilization. Consequently, it is very useful for application to a real-time WDM network, which changes status dynamically.

Irvine, J.M., Fenimore C.P., Cannon D., Roberts, J., Israel, S A., Simon, L., Watts, C., Miller, J.D.; Avilés, A. I., Tighe, P.F., Behrens, R.J., *Factors Affecting Development of a Motion Imagery Quality Metric*, Proceedings Visual Information Processing Conference (SPIE Defense and Security Symposium 2005), Orlando, Florida, March 29-30, 2005

The motion imagery community would benefit from the availability of standard measures for assessing image interpretability. The National Imagery Interpretability Rating Scale (NIIRS) has served as a community standard for still imagery, but no comparable scale exists for motion imagery. Several considerations unique to motion imagery indicate that the standard methodology employed in the past for NIIRS development may not be applicable or, at a minimum, require modifications. Traditional methods for NIIRS development rely on a close linkage between perceived image quality, as captured by specific image interpretation tasks, and the sensor parameters associated with image acquisition. The dynamic nature of motion imagery suggests that this type of linkage may not exist or may be modulated by other factors. An initial study was conducted to understand the effects target motion, camera motion, and scene complexity have on perceived image interpretability for motion imagery. This paper summarizes the findings from this evaluation. In addition, several issues emerged that require further investigation: The effect of frame rate on the perceived interpretability of motion imagery§ Interactions between color and target motion, which could affect perceived interpretability§ The relationships among resolution, viewing geometry, and image interpretability§ The ability of an analyst to satisfy specific image exploitation tasks relative to different types of motion imagery clips. Plans are being developed to address each of these issues through direct evaluations. This paper discusses each of these concerns, presents the plans for evaluations, and explores the implications for development of a motion imagery quality metric.

Irvine, J.M., Fenimore, C.P., Cannon, D., Roberts, J., Israel, S.A., Simon, L., Watts, C., Miller, J.D., Avilés, A.I., Tighe, P.F., Behrens, R.J., *Feasibility Study for the Development of a Motion Imagery Quality Metric*, Proceedings of Applied Imagery Pattern Recognition Workshop 2004, Washington, D.C., October 13-15, 2004

The motion imagery community would benefit from the availability of standard measures for assessing image interpretability. The National Imagery Interpretability Rating Scale (NIIRS) has served as a community standard for still imagery, but no comparable scale exists for motion imagery. Several considerations unique to motion imagery indicate that the standard methodology employed in the past for NIIRS development may not be applicable or, at a minimum, require modifications. Traditional methods for NIIRS development rely on a close linkage between perceived image quality, as captured by specific image interpretation tasks, and the sensor parameters associated with image acquisition. The dynamic nature of motion imagery suggests that this type of linkage may not exist or may be modulated by other factors. An initial study was conducted to understand the effects of specific factors on perceived image interpretability for motion imagery. These factors are: Target motion: Other studies indicate that moving targets exhibit greater salience that can enhance target detection and recognition; Camera motion: The parallax effect and changing viewing geometry assist the analyst, particularly when viewing partially occluded targets; Scene complexity: It has been hypothesized that both target and camera motion exhibit greater effects on perceived interpretability when the scenes are more complex. In this evaluation, a number of experienced imagery analysts provided ratings and comparisons of a number of motion imagery clips and images derived from these clips. The image set was well characterized in terms of target motion, camera motion, and scene complexity, as well as ground sampled distance. Analysis of the data from this evaluation provides insight into the magnitude of these effects on perceived image interpretability. This paper describes the evaluation, presents the results, and explores the implications for development of a "NIIRS-like" scale for motion imagery.

Jansen, W., Ayers, R., *Guidelines on PDA Forensics*, Recommendations of the National Institute of Standards and Technology, NIST SP 800-72, http://csrc.nist.gov/publications, November 15, 2004

Forensic specialists periodically encounter unusual devices and new technologies normally not envisaged as having immediate relevance from a digital forensics perspective. The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with Personal Digital Assistants (PDAs), and to prepare forensic specialists to deal with new situations when they are encountered. This guide provides an in-depth look into PDAs and explains associated technologies and their impact on the procedures for forensic specialists. It covers the characteristics of three families of devices: Pocket PC, Palm OS, and Linux based PDAs and the relevance of various operating systems associated.

Kacker, R.N., Datla, R.U., Parr, A.C., *Response to Comments by Franco Pavese on Kacker et al*., Metrologia 41 (2004) 340-352, Metrologia, Volume 42, Number 1, February 2005

This is response to comments on our published papers submitted by Dr. Franco Pavese of the NMI of Italy.

Kearsley, A.J., *Projections Onto Order Simplexes and Isotonic Regression*, NIST Journal of Research, to be published

Isotonic regression is the problem of fitting data to order constraints. This problem can be solved numerically in an efficient way by successive projections onto order simplex constraints. An algorithm for solving the isotonic regression using successive projections onto order simplex constraints was originally suggested and analyzed by Grotzinger and Witzgall. This algorithm has been employed repeatedly in a wide variety of applications. In this paper we briefly discuss the isotonic regression problem and its solution by the Grotzinger-Witzgall method. We demonstrate that this algorithm can be appropriately modified to run on a parallel computer with substantial speed-up. Finally we illustrate how it can be used to pre-process mass spectral data for automatic high throughput analysis.

Kelsey, J., Schneier, B., *Second Primages on n-bit Hash Functions for Much Less than 2n Work*, Proceedings of Eurocrypt 2005, published by Springer in the Lecture Notes in Computer Science, to be published

We expand a previous result of Dean[Dea99] to provide a second preimage attack on all n-bit iterated hash functions with Damgard-Merkle strengthening and n-bit intermediate states, allowing a second preimage to be found for a 2k-message-block message with about k x 2n/2+1 + 2n-k+1 work. Using RIPE-MD160 as an example, our attack can find a second preimage for a 260 byte message in about 2106 work, rather than the previously expected 2160 work. We also provide slightly cheaper ways to find multicollisions than the method of Joux[Jou04]. Both of these results are based on expandable messages--patterns for producing messages of varying length, which all collide on the intermediate hash result immediately after processing the message. We provide an algorithm for finding expandable messages for any n-bit hash function built using the Damgard-Merkle construction, which requires only a small multiple of the work done to find a single collision in the hash function.

Knill, E.H., *Quantum Computing with Very Noisy Devices*, Nature 434, 39-44 (03 March 2005) and http://arxiv.org/quant-ph

There are quantum algorithms that can efficiently simulate quantum physics, factor large numbers and estimate integrals. As a result, quantum computers can solve otherwise intractable computational problems. One of the main problems of experimental quantum computing is to preserve fragile quantum states in the presence of errors. It is known that if the needed elementary operations (gates) can be implemented with error probabilities below a threshold, then it is possible to efficiently quantum compute arbitrarily accurately. Here we give evidence that for independent errors, the theoretical threshold is well above 3% a significant improvement over earlier calculations. However, the resources required at such high error probabilities are excessive. Fortunately, they decrease rapidly with decreasing error probabilities. If we had quantum resources comparable to the considerable resources available in today's digital computers, we could implement non-trivial quantum algorithms at error probabilities as high as 1% per gate.

Kuhn, D.R., Walsh, T.J., Fries, S., *Security Considerations for Voice Over IP Systems*, Recommendations of the National Institute of Standards and Technology, NIST SP 800-58, http://csrc.nist.gov/publications, January 15, 2005

Voice over Internet Protocol (VOIP) refers to the transmission of speech across data-style networks. This form of transmission is conceptually superior to conventional circuit switched communication in many ways. However, a plethora of security issues are associated with still-evolving VOIP technology. This publication introduces VOIP, its security challenges, and potential countermeasures for VOIP vulnerabilities.

Leigh, S.D., *Book Review of Statistics for the Quality Control Chemistry Laboratory*, by Eamonn Mullins, Analytical and Bioanalytical Chemistry, to be published

Book Review

Lennon, E.B., Editor, *2004 Information Technology Laboratory (ITL) Technical Accomplishments*, NISTIR 7169, http://www.itl.nist.gov/itl-publications.html, February 7, 2005

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY 2004. Following the Director's Foreword and the ITL overview, the report describes technical projects in ITL research areas, followed by cross-cutting focus areas, industry and international interactions, publications, conferences, and staff recognition.

Lyon, G.E., Mink, A., Van Dyck, R.E., *Toward an Architectural Framework to Improve Accountability in the Use of Electronic Records*, NISTIR 7157, to be published

Sensitive electronic record systems (ERSs) raise questions about their proper use. Insider-threat involves hidden, unknown and unanticipated activities that constitute unacceptable use of an ERS, even while operating within individual access privileges. Insider-threat detection and control is an ERS monitoring and management challenge of the first order. A flexible preliminary framework can encourage discussion and comparison among various monitoring elements for the insider-threat. Responding to a lack of such a framework, one is sketched here: It employs two perspectives of an ERS user -- structural and intentional. The structural view is short term, whereas the intentional view seeks to discover general content topics of interest to a user, and to follow these over time. Discussion includes details of a possible architecture that uses untrained classification methods to amplify the concern set beyond that specifically defined at the onset of monitoring. The general framework may expedite development of common guidelines and methodologies to monitor insider threats. Although developed for medical services (e.g., an E-Health RS), the framework likely has applicability in other similar database areas such as security and intelligence archiving.

Micheals, R.J., Boult, T.E., *Is the Urn Well-Mixed? Uncovering False Cofactor Homogeneity Assumption in Evaluation*, NISTIR 7156, October 27, 2004

Measuring system performance is conceptually straightforward; it is the interpretation of the results and their use as predictors of future performance that are the exceptional challenges in system evaluation and the experimentation in general. Good experimental design is critical in evaluation, but there have been very few techniques that a scientist may use to check their design for either overlooked associations or weak assumptions. For biometric and vision system evaluation, the complexity of the systems make a thorough exploration of the problem space impossible. This lack of verifiability in experimental design is a serious issue. In this paper, we present a new evaluation methodology that aids the researcher in discovering false assumptions about the homogeneity of cofactors – when the data is not "well mixed." The new methodology is then applied in the context of a biometric system evaluation.

Mills, K., *Network for Pervasive Computing*, NIST SP 500-259, to be published

Information technology is undergoing a paradigm shift from desktop computing, where isolated workstations connect to shared servers across a network, to pervasive computing, where myriad portable, embedded, and networked information appliances continuously reconfigure themselves individually and collectively to support the information requirements of mobile workers and work teams. This shift will not occur overnight, nor will it be achieved without solving a range of new technical and social problems. Still, this inexorable change should yield many economic opportunities for the global information technology industry, and for the increasing swath of businesses that depend on information. The potential value of pervasive computing motivated the NIST Information Technology Laboratory (ITL) to establish a five-year program of research to help the information technology industry identify and solve some looming technical roadblocks that seemed likely to slow development and acceptance of the new paradigm. The ITL Pervasive Computing program addressed three general areas: human-computer interaction, programming models, and networking. This special publication provides a compendium of technical papers published by NIST researchers who investigated networking for pervasive computing.

Mills, K., Tan, C., *Performance Characterization of Decentralized Algorithms for Replica Selection in Distributed Object Systems*, Proceedings of the International Workshop on Software Performance 2005, to be published

Designers of distributed software systems often rely on server replicas for increased robustness, scalability, and performance. Replicated server architectures require some technique to select a target replica for each client transaction. In this paper, we survey key concepts related to replica selection and we use simulation to characterize performance (response time, server latency, selection error, probability of server overload) for four common replica-selection algorithms (random, greedy, partitioned, weighted) when applied in a decentralized form to client queries in a distributed object system deployed on a local network. We introduce two new replica-selection algorithms (balanced and balanced-partitioned) that give improved performance over the more common algorithms. We find the weighted algorithm performs best among the common algorithms and the balanced algorithm performs best among all those we considered. Our findings should help designers of distributed object systems to make informed decisions when choosing among available replica-selection algorithms.

Montavont, N., Montavont, J., Noel, T., *Enhanced Schemes for L2 Handover in IEEE 802.11 Networks and their Evaluations*, Proceedings PIMRC 2005, 16th IEEE International Symposium on Personal, Indoor & Mobile Radio Communications, 9/05, Berlin, DE, to be published

Given the relatively limited coverage area of 802.11 access points, stations moving inside WLAN are often required to perform a handover. The time needed for a STA to switch from one AP to another is too long for real-time applications to continue operating seamlessly, even if no layer 3 handover is to occur ulteriorly. Many solutions have been proposed for improving the layer 2 handover latency, but we have observed a lack of performance analysis and comparison of the different algorithms. In this article we present two new schemes that aim to enhance L2 handover mechanisms. The main characteristic of these new methods is to reduce the discovery time. We then provide an evaluation of four algorithms in order to analyze and compare solutions in six different scenarios.

Morse, E., Steves, M.P., Scholtz, J.C., *Metrics and Methodologies for Evaluating Technologies for Intelligence Analysts*, 2005 International Conference on Intelligence Analysis, to be published

In this paper we discuss the evaluation methodologies and metrics we have developed for ARDA's Novel Intelligence for Massive Data (NIMD) program. We discuss the challenges of developing methods and metrics in a situation where software components that were to be tested were in very early stages of development and where investigators who might be on the leading edge with respect to their technology were novices with respect to evaluation. Additionally, we discuss how our process of evaluation design is evolving as we gain experience with metrics and measures that are obtainable, yet have some value as indicators of future software performance in the field.

Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Chang, J., Hofman, K., Marques, J., Min, J., Worek, W., *Overview of the Face Recognition Grand Challenge*, NISTIR 7195 and IEEE Computer Society International Conference on Computer Vision and Pattern Recognition 2005, to be published

Over the last couple of years, face recognition researchers have been developing new techniques, such as recognition from three-dimensional and high resolution imagery. These developments are being fueled by advances in computer vision techniques, computer design, sensor design, and interest in fielding face recognition systems. These techniques hold the promise of reducing the error rate in face recognition systems by an order of magnitude over FRVT 2002 results. The Face Recognition Grand Challenge (FRGC) is designed to achieve this performance goal by making available to researchers a data corpus of 50,000 images and a challenge problem containing six experiments. The data consists of 3D scans and high resolution still imagery. The imagery is taken under controlled and uncontrolled conditions. This paper describes the data corpus and challenge problems, and presents baseline performance and preliminary results on natural statistics of facial imagery.

Phillips, P.J., *Privacy Operating Characteristic for Privacy Protection in Surveillance Applications*, Conference on Audio- and Video-Based Biometric Person Authentication 2005, to be published

With the mass deploy of cameras, concern has risen about protecting a person's privacy as he goes about his daily life. Many of the cameras are installed to perform surveillance tasks that do not require the identity of a person. In the context of surveillance applications, we examine the trade-off better privacy and security. The trade-off is accomplished by looking at quantitative measures of privacy and surveillance performance. To provide privacy protection we examine the effect on surveillance performance of a parametric family of privacy function.

A privacy function degrades images to make identification more difficult. By varying the parameter, different levels of privacy protection are provided. We introduce the privacy operating characteristic (POC) to quantitatively show the resulting trade-off between privacy and security. From a POC, policy makers can select the appropriate operating point for a surveillance systems with regard to privacy.

Podio, F.L., *International Biometric Standards - Addressing the Customer Needs for Personal Authentication*, ISO Focus, November 1, 2004

Authentication is the provision of assurance of the claimed identity of an entity. Biometrics is defined as the automated recognition of individuals based on their behavioral and biological characteristics. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. Biological characteristics include hand and facial features, fingerprints, and iris patterns. In addition to supporting national security and preventing ID fraud, they are starting to play a crucial role in enterprise-wide network security infrastructures, the protection of buildings from unauthorized individuals, employee IDs, secure electronic banking and financial transactions, retail sales, law enforcement and health and social services. Mobile devices, colleges, and amusement parks are already benefiting from these technologies. In the last few years, national security priorities have emphasized the need for biometrics in employee identification documents, passports and other high secure applications. These activities are inherently global in scope. These needs for biometric technologies have encouraged international biometric standardization. ISO/IEC JTC 1 established Subcommittee 37 – Biometrics in June 2002 in response to these users' immediate needs, and to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of biometric standards. Twenty-seven member countries are involved in this endeavor. The article describes the current activities of this Subcommittee, its program of work, and the interrelationship with other standards bodies and outside organizations. It emphasizes also early adoption of international biometric standards developed under SC 37 by large organizations such as the International Civil Aviation Organization and the International Labor Organization of the UN.

Quirolgico, S., Assis, P., Westerinen, A., Baskey, M., Stokes, E., *Toward a Formal Common Information Model Ontology*, Ontologies for Networked Systems (ONS04), to be published

Self-managing systems will be highly dependent upon information acquired from disparate applications, devices, components and subsystems. To be effectively managed, such information will need to conform to a common model. One standard that provides a common model for describing disparate computer and network information is the Common Information Model (CIM). Although CIM defines the models necessary for inferring properties about distributed systems, its specification as a semi-formal ontology limits its ability to support some important requirements of a self-managing distributed system including knowledge interoperability and aggregation, as well as reasoning. To facilitate the interoperability and aggregation of CIM-based knowledge, as well reasoning over such knowledge, there is a need to model, represent and share CIM as a formal ontology. In this paper, we propose a framework for constructing a formal CIM ontology based on previous research that identified mappings from UML to ontology language constructs.

Radack, S.M., Editor, *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, ITL Bulletin, http://csrc.nist.gov/publications, March 2005

Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, was approved by Carlos M. Guitierrez, the U.S. Secretary of Commerce, on February 25, 2005. The standard specifies a system based on the use of smart cards, which will be issued by all federal government departments and agencies to their employees and contractors who require access to federal facilities and information systems. Homeland Security Presidential Directive (HSPD) 12, issued by President Bush on August 27, 2004, directed the development of the standard for a government-wide identification system that would enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. NIST developed the standard, working in conjunction with private industry and with other federal agencies, including the Office of Management and Budget the Office of Science and Technology Policy, and the Departments of Defense, State, Justice and Homeland Security. FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that issue smart cards as identification credentials and that use the cards to authenticate an individual's identity. Information about the standard, how it was developed, and related publications is available on NIST's web site.

Roginsky, A.L., *Targeted Search: Reducing the Time and Cost for Searching for Objects in Multi-Server Networks*, 24th IEEE International Performance, Computing, and Communications Conference, Phoenix, Arizona, April 7-9, 2005

In many applications – including P2P file sharing, content distribution networks, and grid computing – a single object will be searched for in multiple servers. In this paper, we find the provably optimal search method for such applications and develop analytical models for search time and cost. A client node searching for objects maintains statistics on where (in which servers) it has previously found objects. Using these statistics to target future searches to “popular” servers is provably optimal. For object location and request distributions that are non-uniform, which has been shown to be the case in P2P file sharing networks, this method of targeted searching is found to be more cost-effective (i.e., use less server resources) than broadcast-based searching. Our targeted search method is implemented in a prototype Gnutella servent called Ditella. Ditella can improve the scalability of file sharing in P2P networks and reduce the amount of traffic in the Internet by reducing file search query traffic.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., Lee, A., *Recommended Security Controls for Federal Information Systems*, NIST SP 800-53, http://csrc.nist.gov/publications, February 28, 2005

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by: (i) facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems; (ii) providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems; (iii) promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and (iv) creating a foundation for the development of assessment methods and procedures for determining security control effectiveness. The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies until the publication of FIPS 200, Minimum Security Controls for Federal Information Systems (projected for publication December 2005).

Ross, R.S., Toth, P.R., *Understanding the NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government*, ITL Bulletin, http://csrc.nist.gov/publications, November 2004

This ITL Bulletin summarizes an article entitled "Understanding the New FISMA Required NIST Standards and Guidelines,” by Ron S. Ross, Ph.D.

Rouil, R., Chevrollier, N., Golmie, N., *Unsupervised Anomaly Detection System Using Next-Generation Router Architecture*, MILCOM 05, to be published

Unlike many intrusion detection systems that rely mostly on labeled training data, we propose a novel technique for anomaly detection based on unsupervised learning and we apply it to counter denial-of-service attacks. Initial simulation results suggest that significant improvements can be obtained. We then discuss an implementation of our anomaly detection system in the ForCES router architecture and evaluate it using attack traffic.

Scholtz, J.C., Antonishek, B., Young, J., *Implementation of a Situation Awareness Assessment Tool for Evaluation of Human Robot Interfaces*, IEEE Transactions on System, Man, and Cybernetics, Part A, to be published

In this paper we outline a methodology for evaluating the situation awareness (SA) provided by a supervisory interface for an autonomous on-road vehicle. Our goal is to be able to use the evaluations to compare interface designs with respect to how well each facilitates the users' acquisition of situation awareness. We used Endsely's Situation Awareness Global Assessment Technique (SAGAT) [8] and developed scenarios and assessment questions appropriate for supervisors of autonomous on-road driving vehicles. We describe the results of two experiments used to refine our SA assessment implementation. In a third experiment we applied the refined implementation to a graphical user interface we developed to test the sensitivity of our SAGAT implementation. We discuss the results of this experiment and implications for applying the SAGAT methodology to supervisory user interfaces for autonomous vehicles.

Scholtz, J.C., Antonishek, B., Young, J.D., *Evaluation of Human-Robot Interaction in the NIST Reference Search and Rescue Test Arenas*, Performance Metrics for Intelligent Systems 2004 Workshop Proceedings, PerMIS '04, August 24, 2004

We describe data collections that we have conducted during Urban Search and Rescue (USAR) competitions within the NIST Reference Test Arenas. We also discuss our analyses of this data and present guidelines based on these studies. We also describe future plans for augmenting USAR competitions to specifically compare different methods of human-robot interaction (HRI).

Scholtz, J.C., Morse, E., Hewett, T.T., *An Analysis of Qualitative and Quantitative Data from Professional Intelligence Analysts*, 2005 International Conference on Intelligence Analysis, to be published

Our goal is to produce metrics for measuring the effectiveness of software tools and environments produced for the intelligence community. To this end we need to understand the analytic process and to determine which data need to be captured to meaningfully measure process and effectiveness. In this paper we compare data from observational studies of professional intelligence analysts with data collected from an instrumented environment. We discuss some findings and their implications for possible metrics and for additional data needed to compute potential measures.

Scholtz, J.C., *The Effect of Situation Awareness Acquisition in Determining the Ratio of Operators to Semi-Autonomous Driving Vehicles*, The International Society for Optical Engineering, to be published

We used a technical readiness level assessment to obtain intervention time and the time to acquire situation awareness for different classifications of interventions. We analyzed this data to determine if it is feasible for one operator to control multiple robots of this type in similar environments. We conclude that in both terrains analyzed (an arid terrain and a wooded terrain) it would be feasible for one operator to control two robots. While it is also possible for an operator to work on another task and control a robot as well, there is an issue of providing situation awareness about the robot. There are also constraints on the tasks that could be effectively accomplished.

Slattery, O.T., *Drive Compatibility Test (Phase 2) for DVD-R (General) and DVD+R Discs, Including DVD Creation Plan*, NIST SP 500-258, http://www.itl.nist.gov/div895/docs/NIST-SP500-258.pdf, October 19, 2004

Phase 2 test procedure is designed to test the compatibility of DVD drives with DVD writable media including DVD-R (for general) and DVD+R. The test plan includes detailed instructions on how to create and test the recordable media and how to determine the result from each test. Following implementation of Phase 1 (NIST Special Publication 500-254), the National Institute of Standards and Technology (NIST), the Optical Technology Storage Association (OSTA) and the DVD Association (DVDA) expanded the scope of testing in Phase 2. Phase 2 includes testing of DVD recordable drives and also includes a procedure to create test media.

Slutsker, J., Thornton, K., Roytburd, A.L., Warren, A., McFadden, G.B., Voorhees, P.W., *Phase-Field Modeling of Solidification Under Stress*, Acta Materialia, to be published

A phase-field model that includes the stress field during non-isothermal phase transformation of a single-component system has been developed. The model has been applied to the solidification and melting of confined spherical volumes, where sharp interface solutions can be obtained and compared with the results of the phase-field simulations. Numerical solutions for a spherically-symmetric geometry have been obtained. The analysis of these equilibrium states for the phase-field model allows us to estimate the value of interface energy in the model, which can then compared to the analogous calculation of the energy of planar liquid-solid interface. It is also demonstrated that the modeling of the liquid as a coherent solid with zero shear modulus is realistic by comparison of the long-range stress fields in phase-field calculations with those calculated using sharp interface models of either a coherent or relaxed liquid-solid interface. The model can be applied to simulate the process of “writing” to electronic media that exploits an amorphous-to-crystalline phase change for recording information.

Somma, R., Barnum, H., Knill, E.H., Ortiz, G., Viola, L., *Generalized Entanglement and Quantum Phase Transitions*, International Journal of Modern Physics B, to be published

Quantum phase transitions in matter are characterized by structural changes in some correlation functions of the system, thus ultimately entanglement. In this work, we study the second order quantum phase transitions present in models of relevance to condensed-matter physics by exploiting the notion of generalized entanglement [Barnum et al., Phys. Rev. A 68, 032308 (2003)]. In particular, we focus on the illustrative case of a one-dimensional Ising model in the presence of a transverse magnetic field. Our approach leads to useful tools for distinguishing between the ordered and disordered phases in the case of broken symmetry quantum phase transitions. Possible extensions to the study of other kinds of phase transitions as well as of the inherent relation between generalized entanglement and computational efficiency are also discussed.

Souppaya, M.M., Wack, J., Kent, K., *Security Configuration Checklists Program for IT Products: Guidance For Checklists Users and Developers*, NIST SP 800-70, to be published

The National Institute of Standards and Technology (NIST) has produced Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular security level (or baseline). It could also include templates or automated scripts and other procedures. Typically, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations such as consortia, academia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems. This publication is intended for users and developers of IT product security configuration checklists. For checklist users, this document gives an overview of the NIST Checklist Program, explains how to retrieve checklists from NIST’s repository, and provides general information about threat discussions and baseline technical security practices for associated operational environments. For checklist developers, the document sets forth the policies, procedures, and general requirements for participation in the NIST Checklist Program.

Souryal, M.R., Larsson, E.G., Peric, B.M., Vojcic, B.R., *Soft-Decision Metrics for Turbo-Coded FH M-FSK Ad Hoc Packet Radio Networks*, 2005 IEEE Vehicular Technology Conference (VTC 2005/Spring), May 30, 2005

This paper addresses turbo-coded non-coherent FH M-FSK ad hoc networks with a Poisson distribution of interferers where multiple access interference can be modeled as symmetric a-stable (SaS) noise and a is inversely proportional to the path loss exponent. The Bayesian Gaussian metric does not perform well in non-Gaussian (a?2) noise environments and therefore an optimum metric for Cauchy (a=1) noise and a generalized likelihood ratio (GLR) Gaussian metric requiring less side information (amplitude, dispersion) are presented. The robustness of the metrics is evaluated in different SaS noise environments and for mismatched values of the interference dispersion and channel amplitude in an interference-dominated network with no fading or independent Rayleigh fading. Both the Cauchy and GLR Gaussian metric exhibit significant performance gain over the Bayesian Gaussian metric, while the GLR Gaussian metric does so without the knowledge of the dispersion or amplitude. The Cauchy metric is more sensitive to the knowledge of the amplitude than the dispersion, but generally maintains better performance than the GLR Gaussian metric for a wide range of mismatched values of these parameters. Additionally, in an environment consisting of non-negligible Gaussian thermal noise along with multiple access interference, increasing the thermal noise level degrades the performance of the GLR Gaussian and Cauchy metric while for the observed levels both maintain better performance than the Bayesian Gaussian metric.

Souryal, M.R., Larsson, E.G., Peric, B.M., Vojcic, B.R., *Soft-Decision Metrics for Coded Orthogonal Signaling in Symmetric Alpha-Stable Noise*, Proceedings of the 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), March 18, 2005

This paper derives new soft decision metrics for coded orthogonal signaling in symmetric a-stable noise, which has been used to model impulsive noise. In addition to the optimum metrics for Gaussian (a = 2) noise and Cauchy (a = 1) noise, a class of generalized likelihood ratio (GLR) metrics with lower side information requirements is derived. Through numerical results for a turbo code example, the Cauchy decoder is found to be robust for a wide range of a, and GLR metrics are found which provide performance gains relative to the Gaussian metric, but with lower complexity and less a priori information.

Stanford, V., Rochet, C., Michel, M., Garofolo, J., *Beyond Close Talk - Issues in Distant Speech Acquisition, Conditioning Classification, and Recognition*, Included in NIST SP 500-257, Proceedings of the ICASSP 2004 Meeting Recognition Workshop, http://www.itl.nist.gov/iad/IADpapers/2004/ICASSP2004Workshop.pdf, October 14, 2004

Properly designed reference data and performance metrics can offer crucial aid to developers of advanced statistical recognition technologies. We focus here on audio data acquisition from close-talk, nearfield, and farfield sensors, and upon its processing, and its metrology. Our intention is to support the research community as it develops state of the art data acquisition and multimodal processing algorithms by supplying standard reference data, metrics, and sharable infrastructure.

Theofanos, M.F., Scholtz, J., *A Diner's Guide to Evaluating a Framework for Ubiquitous Computing Applications*, Human Computer Interaction International Conference 2005, July 27, 2005

There is a clear need for evaluation methodologies specifically suited to ubiquitous computing applications. Here we investigate a user evaluation framework we proposed earlier which draws upon traditional desktop methods, but carefully adapts them based on our experiences with ubiquitous architectures. We test and clarify the criteria in our methodology by examining the utility and applicability of the framework to an existing commercial ubiquitous application for restaurant ordering at the tableside. We analyzed its functionality by discussing design principles with its software developers, and interviewed wait staff as well as restaurant managers to understand its impacts on the workflow and business processes. We conclude that the proposed framework does contain appropriate metrics to assess whether good design principles were achieved and if the designed system will produce the desired user experience.

Toman, B., *Linear Statistical Models With Type B Uncertainty: A Bayesian View of Annex H.3 and H.5 of the Guide to the Expression of Uncertainty in Measurement*, Metrologia, to be published

Annex H.3 of the Guide to the Expression of Uncertainty in Measurement presents an example of calibration of a thermometer using a linear regression model. Annex H.5 of the same publication presents a class of statistical models and analysis techniques which are commonly called the Analysis of Variance (ANOVA). These models are useful for accounting for the effects of factors which cause the measurand in an experiment to change over time or over experimental conditions. Both Annex H.3 and H.5 present procedures which assume that the observations are not subject to type B uncertainties. A natural question then is: Can these models be used in the presence of type B uncertainties? This article answers the question in the affirmative and provides a natural interpretation of the results. The example data from the two Annexes are used for an illustration.

Ulery, B., Hicklin, A., Watson, C., Indovina, M., Kwong, K., *Slap Fingerprint Segmentation Evaluation 2004 Analysis Report*, NISTIR 7209, http://fingerprint.nist.gov/slapseg04/index.html, March 9, 2005

The Slap Fingerprint Segmentation Evaluation 2004 (Slap Seg04) was conducted to assess the accuracy of algorithms used to segment slap fingerprint images into individual fingerprint images. Segmenters from ten different organizations were evaluated on data from seven government sources, according to several distinct measures of accuracy. The source of data, the segmentation software used, and the decision criteria used were each found to have a significant impact on accuracy. Depending on the data source, the best segmenters produced at least 3 matchable fingers, with finger positions correctly identified, from 93% to over 99% of the slaps. The source of data is a much better predictor of success than whether the images were collected on livescan devices or paper. Most segmenters performed well, but there were significant differences among segmenters on poor quality data.

Walsh, T.J., Kuhn, D.R., *Securing Voice Over Internet Protocol Networks*, ITL Bulletin,
http://csrc.nist.gov/publications, October 2004

Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today's computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.

Walsh, T.J., Kuhn, R.D., *Securing Voice Over IP Networks*, IEEE Computer Security and Privacy, to be published

Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today's computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.

Wang, C.M., Iyer, H.K., *Detection of Influential Observation in the Determination of the Weighted-Mean KCRV*, Metrologia, to be published

Since the signing of the Mutual Recognition Arrangement, National Metrology Institutes (NMI) have carried out many key comparisons in a wide range of metrological areas to establish the equivalence of their measurement standards. The determination of a key comparison reference value (KCRV) and its associated uncertainty are the central tasks in the evaluation of key comparison data. One of the most popular ways to estimate the KCRV is to use a weighted mean of each NMI's reporting values, with weights inversely proportional to the variances of the NMI's reporting value. One potential problem with the use of the weighted mean is its reliance on the weights that may vary greatly across NMIs. Consequently, some of the NMIs can be influential in the determination of the weighted-mean KCRV. Thus it is of interest to identify the influential NMIs based on some simple and well-defined criteria. In this paper, we present several easy-to-use criteria for detecting influential data in the calculation of the weighted-mean KCRV.

Wang, C.M., Iyer, H.K., *On Higher Order Corrections for Propagating Uncertainties*, Metrologia, to be published

The ISO Guide to the Expression of Uncertainty in Measurement (GUM) recommends the use of a first-order Taylor series expansion for propagating errors and uncertainties. The GUM also suggests the use of a second-order Taylor series approximation for calculating uncertainties when the first-order approximation alone is not adequate. In this paper we derive the formulas for evaluating measurement uncertainty based on a second-order Taylor series approximation. We provide a computer program that uses symbolic derivatives to calculate the second-order approximations of the uncertainty in measurement results.

Wang, C.M., Iyer, H.K., *Propagation of Uncertainties in Measurement Using Generalized Inference*, Metrologia, Volume 42, Number 2, 145-153, April 2005

The ISO Guide to the Expression of Uncertainty in Measurement (GUM) recommends the use of a first-order Taylor series expansion for propagating errors and uncertainties. The GUM also endorses the use of 'other analytical or numerical methods' when the conditions for using the Taylor expansion do not apply. In this paper we propose an alternative approach for evaluating measurement uncertainty based on the principle of generalized inference. The proposed approach can be applied to measurement models having any number of input quantities and a vector-valued measurand. We use several examples from the GUM to illustrate the implementation of the proposed approach for the calculation of uncertainties in measurement results.

Wang, Q., Ressler, S., *A Tool Kit to Generate 3D Animated CAESAR Bodies*, 2005 SAE Digital Human Modeling For Design and Engineering Symposium, Iowa City, Iowa, June 14, 2005

The Civilian American and European Surface Anthropometry Resource (CAESAR) database provides a comprehensive source for body measurement in numerous industries such as apparel, aerospace, and automobile. Generating animated CAESAR body sequences from still surface and landmark data will stimulate research and design in these areas. A tool kit has been developed to convert CAESAR bodies to models compliant with the Humanoid Animation specification (H-Anim). It will be helpful to set up a realistic motion capable humanoid library for application environment that can be reused in a wide variety of ergonomic applications. The process consists of preprocessing the mesh, building a skeleton structure, creating segments of the body, assigning weights for vertices, and integrating motion capture data. Publicly available software is adopted for mesh compression and hole filling. C programs were developed to implement the translation from CAESAR body data to H-Anim. The technical issues involved in the process are discussed, and experimental results are shown in the paper.

Wang, Q., Saunders, B., *Web-Based 3D Visualization in a Digital Library of Mathematical Functions*, NISTIR 7159 and Conference Proceedings of the WEB3D 2005 Symposium, University of Wales, United Kingdom, March 29, 2005

The National Institute of Standards and Technology (NIST) is developing a digital library of mathematical functions to replace the widely used National Bureau of Standards Handbook of Mathematical Functions published in 1964 [1]. The NIST Digital Library of Mathematical Functions (DLMF) will provide a wide range of information about high-level functions for scientific, technical and educational users in the mathematical and physical sciences. Clear, concise 3D visualizations that allow users to examine poles, zeros, branch cuts and other key features of complicated functions will be an integral part of the DLMF. Specially designed controls will enable users to move a cutting plane through the function surface, select the surface color mapping, choose the axis style, or transform the surface plot into a density plot. To date, Virtual Reality Modeling Language and Extensible 3D (VRML/X3D) standards have been used to implement these capabilities in more than one hundred 3D visualizations for the DLMF. We discuss the development of these visualizations, focusing on the design and implementation of the VRML code, and show several examples.

Watson, C., Wilson, C., *Effect of Image Size and Compression on One-to-One Fingerprint Matching*, NISTIR 7201, http://www.itl.nist.gov/iaui/894.03/pact/pact.html, February 9, 2005

NIST has conducted testing of one-to-one fingerprint matching systems to evaluate the effect of image size and compression on the accuracy of the one-to-one matching process. Images from three live-scan fingerprint scanners collected by the Departments of State and Homeland Security were used as test samples. Image sizes from 368 pixels by 368 pixels down to 180 pixels by 180 pixels were tested and compression ratios from no compression up to 30 to 1 were tested. Three commercial fingerprint-matching systems were used in the test. The results of the study show that image cropping quickly degrade matcher performance. Compression degrades matcher performance more slowly and may, for compression ratios of 15 to 1, increase performance. Image sizes below 320 by 320 should not be used. Image compression in the range up 20 to 1 produces minimal effects on fingerprint matching accuracy.

White, D., Tebbutt, J., *A Perl-Based Framework For Distributed Processing*, Open Source Developers' Conference 2004, Melbourne, Australia, December 1, 2004

The National Software Reference Library (NSRL) of the U.S. National Institute of Standards and Technology (NIST) collects software from various sources and publishes file profiles computed from this software (such as MD5 and SHA-1 hashes) as a Reference Data Set (RDS) of information. The RDS can be used in the forensic examination of file systems, for example, to speed the process of identifying unknown or suspicious files. This paper describes the cross-platform, public domain, Linux/Apache/MySQL/Perl (LAMP) framework with which we produce the RDS from acquired software. The framework is easily deployed (it has been packaged on a Knoppix-based live CD) and allows for the distributed processing of large numbers of files in a loose, heterogeneous computing cluster. We go on to suggest that the framework is sufficiently general in its implementation to be suitable for application to classes of problems quite beyond our original scope.

Wilson, C., Grother, P., Chandramouli, R., *Biometric Data Specification for Personal Identity Verification*, NIST SP 800-76, to be published

The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201) was developed to establish standards for identity credentials. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It specifies technical acquisition and formatting requirements for the biometric credentials of the PIV system, including the PIV Card1 itself. It enumerates required procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is universal interoperability. For the preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint Transaction Sets.

Wu, J.C., Wilson, C.L., *Nonparametric Analysis of Fingerprint Data*, NISTIR 7168 and Pattern Recognition, to be published

This paper demonstrates that, for large-scale tests, the match and non-match similarity scores have no specific underlying distribution function. The forms of these distribution functions require a nonparametric approach for the analysis of the fingerprint similarity scores. In this paper, we present an analysis of the discrete distribution functions of the match and non-match similarity scores of the fingerprint data that clarifies the widely varying form of these distribution functions. This analysis demonstrates that a precise Receiver Operating Characteristic (ROC) curve based on the True Accept Rate (TAR) of the match similarity scores and the False Accept Rate (FAR) of the non-match similarity scores can be constructed without any assumption regarding operating thresholds or the form of the distribution functions. The area under such a ROC curve, assuming normality, is equivalent to the Mann-Whitney statistic directly formed from the match and non-match similarity scores. In addition, the Z statistic computed using the areas under ROC curves along with their variances is applied to test the significance of the difference between two ROC curves. Four examples than from NIST's extensive testing of commercial fingerprint systems are provided. The nonparametric approach presented in this article can also be employed in the analysis of other biometric data.

Yanik, L., Torre, E.D., Donahue, M.J., Cardelli, E., *Micromagnetic Eddy Currents in Conducting Cylinders*, Journal of Applied Physics, to be published

The inclusion of eddy currents into micromagnetic programs is important for the proper analysis of dynamic effects in conducting magnetic media. This paper introduces a limited numerical implementation for eddy current calculations and discusses some interesting analytic cases in the simplified geometry. It is designed to provide some benchmarks for more complex program.

Zhang, N.F., *Statistical Process Control in Biochemical and Hematological Quality Control Data*, Proceedings of the American Statistical Association, to be published

Daily quality control (QC) measurements of common biochemical and hematological quantities were recorded during several months while methods and analyzers showed no signs of malfunctioning. Usually it is assumed that QC data may be described as i.i.d. In this case an X chart and/or an EWMA chart are the proper control charts to use. When autocorrelation is presented, the traditional control charts may be inefficient. An alternative control chart, the EWMAST chart proposed in Zhang (1998) has been developed for stationary process data. The EWMA and the EWMAST chart were applied to each of the 11 QC data series. In 6 of the 11 series, significant process autocorrelations were demonstrated. The results show that the conventional EWMA chart may give false alarms in the presence of autocorrelation while the EWMAST chart gave few false alarms.

Zhang, N.F., Winkel, P., *The Effect of Recalibration and Reagent Lot Changes on the Performance of QC Control Charts*, Clinical Chemistry, to be published

Daily QC measurements of biochemical quantities were recorded during four to five months while methods and analyzer showed no signs of malfunctioning. The time series of QC values were divided into subseries according to reagents or electrolyte diluent lot and (within diluent subseries) disposable electrode used. ANOVA was used to examine if the mean level changed significantly between subseries. All time series, as well as reagents and diluent subseries were examined for autocorrelation. The X-chart and the EWMAST (in autocorrelated series) or EWMA chart were applied to each time series and each reagents and diluent subseries and the number of values falling outside the 3 SD control limits were noted. Results: The mean levels changed significantly due to diluent lot changes, replacement of disposable electrodes and recalibrations following reagents lot changes. These changes caused spurious autocorrelation as evidenced by the ACF plot. In 42% of all reagents subseries a significant autocorrelation could also be demonstrated; however, 5.64% and 29.1% of all time series values fell outside the control limits of the X-charts and the EWMA or EWMAST charts respectively. These percentages were reduced to 0.44 and 0.7 when separate control charts were calculated following recalibrations and changes of diluent lot. Conclusions: The mean level may change due to recalibrations and change of electrode diluent lot that causes an excessive number of false alarms unless new control charts are calculated subsequent to these events.

Ziring, N., Wack, J., *Specification for the Extensible Configuration Checklists Definition Format (XCCDF)*, NISTIR 7188, http://checklists.nist.gov, January 14, 2005

This document specifies the data model and XML representation for the Extensible Configuration Checklist Description Format. An XCCDF document is a structured collection of security configuration rules for some set of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.