



Vertragsprof. Dipl.-Ing. Dr.techn. Horst Bischof
Institut für Maschinelles Sehen und Darstellen
E-Mail: bischof@icg.tu-graz.ac.at
Tel: 0316 873 5014



Ao.Univ.-Prof. Dipl.-Ing. Dr.techn. Karl-Christian Posch
Institut für Angewandte Informationsverarbeitung und
Kommunikationstechnologie
E-Mail: Karl.Posch@iaik.tugraz.at
Tel: 0316 873 5517



Vertragsprof. Dipl.-Ing. Dr.techn. Franz Wotawa
Institut für Softwaretechnologie
E-Mail: wotawa@ist.tugraz.at
Tel: 0316 873 5724

Forschung an der Fakultät für Informatik *Research at the Computer Science Faculty*

Die Forschungsaktivitäten der jungen Fakultät für Informatik sind vielfältig und reichen von Projekten im Bereich der graphischen Datenverarbeitung und Multimedia hin zu Arbeiten im Bereich der Künstlichen Intelligenz und Neuronalen Netze. Exemplarisch werden drei angewandte Forschungsgebiete an der Fakultät näher vorgestellt (für eine Zusammenstellung aller Forschungsaktivitäten sei auf <http://www.informatik.tugraz.at> verwiesen).

Das erste Forschungsgebiet beschäftigt sich mit Anwendungen der Bildverarbeitung im medizinischen Bereich und wird von Horst Bischof vom Institut für Maschinelles Sehen und Darstellen betreut. Das zweite Projekt beschäftigt sich mit dem Einbruch in Smart Devices. Für weitere Auskünfte steht Karl-Christian Posch vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie zur Verfügung. Das dritte vorgestellte Forschungsgebiet beschäftigt sich mit Werkzeugen zur Verbesserung der Qualität in der Softwareentwicklung und wird von Franz Wotawa vom Institut für Softwaretechnologie betreut.

Angewandte Informatik in der Medizinischen Bildverarbeitung

Basierend auf dem Erfolg mit dem virtuellen Leberplanungssystem (siehe Abb.1), das heuer den Matrix Preis am Europäischen Radiologenkongress gewonnen hat, konnten das Institut für Maschinelles Sehen und Darstellen (ICG) im letzten halben Jahr drei neue medizinische Bildverarbeitungsprojekte starten. Das erste Projekt, das vom FWF finanziert wird, beschäftigt sich als Nachfolgeprojekt Leberplanungssystem mit dem Bereich der Beurteilung von medizinischen Daten. Die detaillierte Planung von Leberoperationen erfordert die Beurteilung der (Patho-)Anatomie und regionale Verteilung der

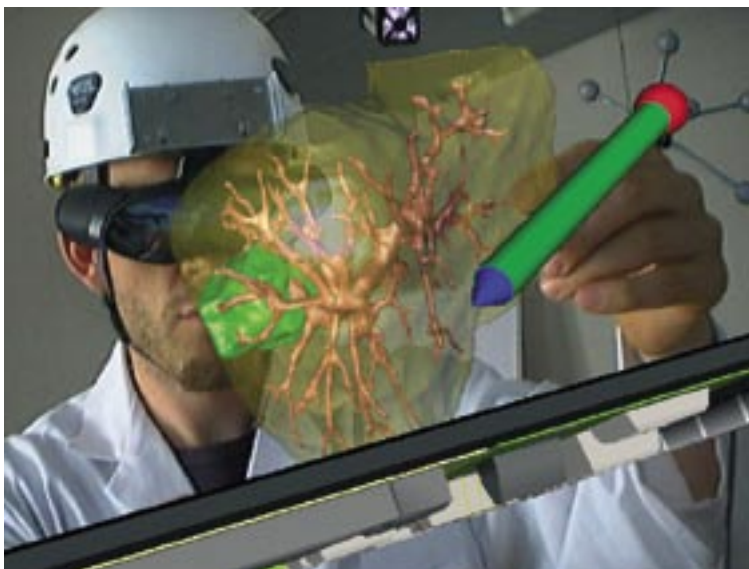


Abb. 1: Virtuelle Leberoperationsplanung mit dem Augmented Reality System am ICG.

hepatischen Funktionen. Das Ziel dieses Forschungsprojektes ist es, eine Methode zu entwickeln, die die zusätzliche Verwendung von Leberaufnahmen im virtuellen Leberoperationsplanungssystem,

ermöglicht. Im Vordergrund der Entwicklung stehen neben der Weiterentwicklung des Augmented Reality Systems neue Methoden zur Datenfusion. Ein zweites, ebenfalls vom FWF gefördertes Projekt, beschäftigt sich mit einer vollständig automatischen Methode zur Quantifizierung des Verlaufes der Rheumatoiden Arthritis basierend auf Röntgenaufnahmen. Diese Krankheit ist eine chronische Krankheit, die zu schmerzhaften Entzündungen der Gelenke führt. Die Folge sind schwere Gelenksschäden, die zu körperlicher Behinderung führen. Die Krankheit ist relativ häufig, sie ist für ca. 17 % aller Behinderungen von Personen die älter als 15 Jahre sind, verantwortlich. Der Schwerpunkt der Entwicklungen in diesem Bereich wird auf robusten Segmentierungsverfahren und der Reduktion von Trainingsdaten liegen. Dieses Projekt wird gemeinsam mit dem AKH Wien durchgeführt. Das dritte von der Firma Siemens (Bereiche PSE Graz und MED Erlangen) geförderte Projekt ist die Fusion von 3D Daten (CT) von Organen (insbesondere der Lunge) zum Thema. Im Rahmen dieses Projektes werden eine Reihe neuer Methoden für das noch weitgehend ungelöste Problem der nicht-rigidem Registrierung entwickelt. Durch diese Entwicklungen soll einerseits die Fusion von anatomischen und funktionalen Datenquellen sowie die Reduktion von Atmungsartefakten ermöglicht werden. In weiterer Folge können die Methoden zum besseren Verständnis der Physiologie der Atmung und Radiotherapieplanung herangezogen werden.

Links:

<http://liverplanner.icg.tu-graz.ac.at/>

<http://www.prip.tuwien.ac.at/Research/AAMIR/>

Über den routinemäßigen Einbruch in Smart Devices

Smart Devices stellen derzeit eine der interessantesten Herausforderungen aus sicherheitstechnischer Sicht dar. Darunter fallen nicht nur Chipkarten, sondern in zunehmenden Maße RFID-Tags (Radio Frequency Identification Chips oder auch Smart Wireless Devices genannt). Am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) arbeitet man im Rahmen von zwei Europäischen Projekten (IST innerhalb von FP6) und drei nationalen Projekten (FIT-IT und FWF) intensiv an diesem Thema. In einem international angesehenen Labor werden am IAIK Chipkarten einem Intensivtest hinsichtlich ihrer Resistenz gegenüber so genannten Seitenkanal-Attacken unterzogen. Bei diesen Attacken wird der Energieverbrauch oder auch das abgestrahlte elektromagnetische Feld während des Betriebs von Smart Devices herangezogen, um den im Chip gespeicherten geheimen kryptografischen Schlüssel zumeist unberechtigt zu ermitteln. Das in diesem Labor vorhandene Knowhow dient vor allem auch dazu, geeignete Gegenmaßnahmen beim Entwurf von Chipkarten und Smart Devices zu entwickeln. Das IAIK wurde nicht zuletzt auf Grund der Resultate in diesem Labor eingeladen, als Partner im „European Network of Excellence in Cryptological Research“ die Forschung im Bereich Hardware-Sicherheit maßgeblich mitzubestimmen. Das IAIK ist zudem wissenschaftlicher Leiter des europäischen IST-Projektes SCARD (Side Channel Analysis Resistant Design Flow), in welchem neue Entwurfsmethoden für den sicheren Entwurf von Smart Devices untersucht werden. Der wichtigste Industriepartner in diesem Projekt ist Infineon Technologies. RFID-Tags sind derzeit ein noch „heißeres“ Thema als Chipkarten.

Chipkarten sind bei vielen Anwendungen, wie etwa im Bankbereich relativ bekannt und werden akzeptiert. RFID-Tags hingegen stellen derzeit in Aussicht, nicht nur in jeder Geldbörse, sondern auf „allen möglichen Dingen“ des täglichen Gebrauchs als Strichcode-Ersatz aufzutreten. Damit besteht die Gefahr, bei sicherheitstechnisch nicht richtiger Verwendung die Besitzer von Gütern mit solchen RFID-Tags aufspüren und verfolgen zu können. Dies ist offensichtlich unerwünscht und verlangt nach geeigneten kryptografischen Methoden. Aus diesem Grund beschäftigt sich das IAIK (zusammen mit Philips Semiconductors und anderen Partnern) mit der Authentifizierung von RFID-Tags.

Links:

<http://www.iaik.tu-graz.ac.at/research/sca-lab/>
<http://www.iaik.tu-graz.ac.at/research/sca-lab/projects/scard.php>
<http://www.iaik.tu-graz.ac.at/research/vlsi%20design/art>

Qualitätssteigerung in der Software-Entwicklung

Neben Prozess- und Managementmethoden zur Steigerung der Qualität von Software spielt die Verwendung standardisierter Methoden zur Überprüfung der Funktionalität des fertigen Softwareprodukts eine wesentliche Rolle. Dieser Bereich wird durch das Testen und in zunehmendem Maß von der formalen Verifikation abgedeckt. Im Rahmen des 6. Forschungsprogramms wird am Institut für Softwaretechnologie (IST) das Projekt PROSYD durchgeführt, das zum Ziel hat, die Verwendung von Verifikationstechniken im Entwurf von elektronischen Systemen und der Programmierung weiter zu steigern. Dieses Projekt wird gemeinsam mit 7 Partnern unter anderem IBM und Infineon durchgeführt. PROSYD beschäftigt sich mit der Standardisierung einer Sprache zur Spezifikation von Bedingungen, die ein Programm beziehungsweise eine elektronische Schaltung erfüllen muss. Durch die Verwendung von Verifikationsmethoden kann sowohl die Produktivität als auch die Qualität des fertigen Produkts erhöht werden. Ein weiterer Aspekt von PROSYD ist die Automatisierung der Fehlersuche basierend auf den angegebenen Programmbedingungen. In diesem Bereich kann das IST bereits auf eine fundierte Basis verweisen. Im Rahmen zweier vom FWF geförderter Projekte beschäftigen sich drei Mitarbeiter bereits seit mehreren Jahren mit der automatischen Fehlersuche in Programmen. Im Rahmen des DEV-Projekts wird ein Werkzeug zur Fehlerlokalisierung in VHDL-Programmen, die zur Beschreibung von elektronischen Schaltungen verwendet werden, entwickelt. Dieses Werkzeug kann automatisch, ausgehend von Testfällen Fehler in Programmen lokalisieren. Das zweite Projekt (JADE-X) beschäftigt sich mit der Fehlerlokalisierung in objekt-orientierten Sprachen, wobei die Programmiersprache JAVA als Referenzsprache verwendet wird. In den Projekten konnten bereits sehr gute und erfolgversprechende Resultate erarbeitet werden. So ist es möglich, Fehler in größeren VHDL-Programmen mit mehreren tausend Zeilen innerhalb von wenigen Minuten zu lokalisieren. Dabei können im Durchschnitt 93 % des Programms als korrekt klassifiziert werden. Das heißt, ein Programmierer muss sich nur mehr 7 % des Programms ansehen, um den Fehler zu lokalisieren. Mit anderen Techniken ist ein Ausschluss von Programmzeilen bei den verwendeten Programmen nicht möglich.

Links:

<http://www.prosyd.org/>
<http://www.ist.tugraz.at/DEV/>

Research at the Computer Science Faculty

The computer science faculty carries out a large number of research projects which range from multimedia to artificial intelligence and neural networks. In this article three research topics in the area of applied computer science are introduced.

Medical Image Recognition

The Institute for Computer Graphics and Vision (ICG) has recently acquired three new medical imaging projects. Two of them are founded by the FWF and one is funded by Siemens (PSE and MED): The continuation of the award winning liver-planner project deals with the incorporation of functional data from the HIDAR-SPECT in the planning process. A new joint project with AKH-Vienna develops novel methods for quantitative evaluation of rheumatoid arthritis. The joint project with Siemens will investigate novel non-rigid registration methods for CT-data from lungs.

Security Issues of Smart Devices

The Institute for Applied Information Processing and Communications (IAIK) is researching security topics for smart cards, RFID tags, and smart wireless devices. Within two European Framework-6 IST projects and three nationally funded projects, IAIK looks at side-channel analysis, design methods for incorporating counter measures against side-channel attacks in the chip design process, and studies authentication for RFID tags. IAIK has gained international recognition with its side-channel analysis laboratory, is member of the „European Network of Excellence in Cryptological Research“, and leads an international IST project on side-channel analysis resistant chip design flow. IAIK's work on authentication for smart wireless devices is crucial in order to deploy these devices on a large scale without compromising data protection.

Quality Improvement in Software Engineering

The Institute for Software Technology (IST) has been carrying out three projects which deal with formal verification and fault localization. The objective of the EU funded project PROSYD is to introduce property-based verification for the design of electronic systems and software. Moreover, PROSYD aims in providing techniques for fault localization. In fault localization the IST has carried out 2 FWF funded research projects. The DEV Project aims at supporting and automating software debugging of VHDL programs which are used to describe hardware designs. During the project a debugging tool has been developed. The second project (JADE-X) aims in supporting the debugging process of object-oriented languages, e.g., Java. The first results of the projects are promising and indicate their usefulness. With the debugging tool fault localizing a fault in larger VHDL programs having several thousands lines of code in several minutes is possible. As a result the tool classifies only 7 percent of the code as fault candidates. This is a tremendous improvement when compared with other approaches where 100 percent of the code for the same programs remains to be fault candidates.