

Vorlesungsverzeichnis

M.Sc. Computer Science for Digital Media

Sommer 2025

Stand 23.09.2025

M.Sc. Computer Science for Digital Media	3
Modeling	3
Distributed and Secure Systems	5
Intelligent Information Systems	6
Graphical and Interactive Systems	8
Electives	8
Project	16
Specialization	28

M.Sc. Computer Science for Digital Media

Faculty Welcome for Master's Students Computer Science for Digital Media

Tuesday, April 1, 2025, 10 a.m., Bauhausstraße 11, room A

Project fair

Tuesday, April 1, 2025, 5 p.m., Steubenstraße 6, Maurice-Halbwachs-Auditorium

Modeling

301017 Exam: Mathematics for data science

B. Rüffer, M. Schönlein

Prüfung

Mi, Einzel, 09:00 - 17:00, Final examination - oral exam (organized by chair) --> please contact the responsible, 30.07.2025 - 30.07.2025

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 oral exam

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe

301017 Mathematics for data science

B. Rüffer, M. Schönlein

Veranst. SWS: 4

Vorlesung

Do, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Fr, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods

from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 oral exam

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe

417130003 Discrete Optimization

A. Jakoby

Veranst. SWS: 4

Vorlesung

Do, wöch., 11:00 - 12:30, Bauhausstraße 11 - R 015, Lecture , ab 03.04.2025

Di, wöch., 15:15 - 16:45, Bauhausstraße 11 - R 015, lab class, ab 08.04.2025

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkomentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination

Distributed and Secure Systems**419140050 Introduction to Modern Cryptography****S. Lucks, N. Lang, J. Leuther**

Veranst. SWS: 3

Vorlesung

Fr, wöch., 11:00 - 12:30, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lab class 04Apr25: 1st Lecture, ab 04.04.2025

Mo, wöch., 13:30 - 15:00, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lecture, ab 07.04.2025

Mo, Einzel, 11:00 - 13:30, Bauhausstraße 11 - N 004, schriftliche Prüfung/ written exam, 29.09.2025 - 29.09.2025

Beschreibung

Früher galt die Kryptographie als Werkzeug für Militärs, Geheimdienste und Diplomaten. Aus dieser Zeit stammt auch noch die berühmte Enigma-Chiffriermaschine.

Heute entwickelt sich die Kryptographie buchstäblich zu einer Schlüsseltechnologie für sichere Kommunikation und Mediennutzung. Von der Öffentlichkeit kaum bemerkt hat die Kryptographie schon längst Einzug gehalten in alltäglich genutzte Geräte wie Geldautomaten und Mobiltelefone.

Der Entwurf kryptographischer Komponenten ist schwierig, und in der Praxis trifft man oft auf erhebliche Entwurfsfehler.

(Dies kommentiert der IT-Sicherheitsexperte Bruce Schneier mit drastischen Worten: "Milliarden von Dollar werden für Computersicherheit ausgegeben, und das Meiste davon wird für unsichere Produkte verschwendet.")

Nicht nur der Entwurf kryptographischer Komponenten ist schwierig, auch der Einsatz von "an sich guten" Komponenten für sichere IT-systeme ist fehlerträchtig und erfordert ein genaues Verständnis der jeweiligen Bedingungen, unter denen eine kryptographische Komponente als "sicher" gelten kann.

Die Vorlesung gibt einen Einblick in Denkweise und Methodik der Mediensicherheit und der modernen Kryptographie und die Anwendung der Kryptographie, um Sicherheitsprobleme zu lösen.

engl. Beschreibung/ Kurzkomentar**Bemerkung**

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Für Studierende, die in ihrem früheren Bachelor-Studium keine Einführung in die Kryptographie besucht haben, ist die Veranstaltung ihrerseits Zulassungsvoraussetzung für fortgeschrittene Kryptographie-Vorlesungen.

Voraussetzungen

Regelmäßige Bearbeitung der Übungsaufgaben und Teilnahme an den Übungen, Klausur.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungsaufgaben, Klausur

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther

Veranst. SWS: 4

Vorlesung

Fr, wöch., 15:15 - 16:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lab class 04.04.25: 1st Lecture, ab 04.04.2025
Di, wöch., 09:15 - 10:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lecture, ab 08.04.2025

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzten Hashfunktionen wie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Struktur von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichten Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidaten drehen. Basierend auf den Erkenntnissen und Kandidaten des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einführung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung

Intelligent Information Systems

420160000 Introduction to Natural Language Processing

B. Stein, M. Wolska, N. Mirzakhmedova, M. Wiegmann

Veranst. SWS: 3

Vorlesung

Do, wöch., 15:15 - 16:45, Bauhausstraße 11 - N 004, Lecture, ab 03.04.2025
Do, wöch., 17:00 - 18:30, Bauhausstraße 11 - N 004, Lab class, ab 03.04.2025
Do, Einzel, 15:15 - 18:30, Marienstraße 13 C - Hörsaal C, 10.04.2025 - 10.04.2025
Do, Einzel, 09:00 - 11:00, Marienstraße 13 C - Hörsaal A, schriftliche Prüfung/ written exam, 24.07.2025 - 24.07.2025
Do, Einzel, 09:00 - 11:00, Coudraystraße 13 B - Hörsaal 3, schriftliche Prüfung/ written exam, 24.07.2025 - 24.07.2025

Beschreibung

This course gives an overview of basic techniques of working with language data. We will introduce basic linguistic notions, issues involved in building and working with language corpora, current standard techniques for preparing

text for analysis, and methods of computational processing of a subset of language phenomena. By the end of the course students will

- (1) have an understanding of key word-level, syntactic, semantic, and discourse phenomena,
- (2) be aware of issues involved in building text corpora,
- (3) be familiar with typical language processing tasks addressed in the NLP community and methods of addressing them, and
- (4) will be able to perform tasks that are part of a standard NLP pipeline.

Leistungsnachweis

Klausur

4336010 Image Analysis and Object Recognition

V. Rodehorst, M. Kaisheva

Veranst. SWS: 4

Vorlesung

Di, wöch., 15:15 - 16:45, Marienstraße 13 C - Hörsaal A, Lecture, ab 08.04.2025

Do, wöch., 11:00 - 12:30, Marienstraße 13 C - Hörsaal A, Lab class, ab 17.04.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal B, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal C, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal D, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Beschreibung

Bildanalyse und Objekterkennung

Die Vorlesung gibt eine Einführung in die Grundlagen der Mustererkennung und Bildanalyse. Behandelt werden unter anderem die Bildverbesserung, lokale und morphologische Operatoren, Kantenerkennung, Bilddarstellung im Frequenzraum, Fourier-Transformation, Hough-Transformation, Segmentierung, Skelettierung, Objektklassifizierung und maschinelles Lernen zur visuellen Objekterkennung.

engl. Beschreibung/ Kurzkomentar

Image analysis and object recognition

The lecture gives an introduction to the basic concepts of pattern recognition and image analysis. It covers topics as image enhancement, local and morphological operators, edge detection, image representation in frequency domain, Fourier transform, Hough transform, segmentation, thinning, object categorization and machine learning for visual object recognition.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungen sowie des Miniprojekts und Klausur

Graphical and Interactive Systems

4556227 Usability Engineering & Testing

J. Ehlers

Veranst. SWS: 4

Vorlesung

Di, wöch., 13:30 - 15:00, Bauhausstraße 11 - N 004, Lecture / lab class online , ab 08.04.2025

Di, Einzel, 15:30 - 17:30, Steubenstraße 6, Haus F - Hörsaal K20, schriftliche Prüfung/ written exam, 22.07.2025 - 22.07.2025

Beschreibung

Usability indicates the "absence of frustration". But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesizing. We will also discuss procedures for quantitative data analysis and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

engl. Beschreibung/ Kurzkomentar

Usability indicates the "absence of frustration". But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesizing. We will also discuss procedures for quantitative data analysis and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

Leistungsnachweis

Empirical exercises (tutorial) and written exam

Electives

4336010 Image Analysis and Object Recognition

V. Rodehorst, M. Kaisheva

Veranst. SWS: 4

Vorlesung

Di, wöch., 15:15 - 16:45, Marienstraße 13 C - Hörsaal A, Lecture, ab 08.04.2025

Do, wöch., 11:00 - 12:30, Marienstraße 13 C - Hörsaal A, Lab class, ab 17.04.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal B, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal C, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Di, Einzel, 10:00 - 12:30, Marienstraße 13 C - Hörsaal D, schriftliche Prüfung/ written exam, 29.07.2025 - 29.07.2025

Beschreibung

Bildanalyse und Objekterkennung

Die Vorlesung gibt eine Einführung in die Grundlagen der Mustererkennung und Bildanalyse. Behandelt werden unter anderem die Bildverbesserung, lokale und morphologische Operatoren, Kantenerkennung, Bilddarstellung im Frequenzraum, Fourier-Transformation, Hough-Transformation, Segmentierung, Skelettierung, Objektklassifizierung und maschinelles Lernen zur visuellen Objekterkennung.

engl. Beschreibung/ Kurzkomentar

Image analysis and object recognition

The lecture gives an introduction to the basic concepts of pattern recognition and image analysis. It covers topics as image enhancement, local and morphological operators, edge detection, image representation in frequency domain, Fourier transform, Hough transform, segmentation, thinning, object categorization and machine learning for visual object recognition.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungen sowie des Miniprojekts und Klausur

4555262 Visualisierung

B. Fröhlich, D. Kiesel, I. López García, G. Rendle

Veranst. SWS: 4

Vorlesung

Do, wöch., 13:30 - 15:00, Bauhausstraße 11 - R 015, Lecture / Lab class , ab 03.04.2025

Fr, wöch., 13:30 - 15:00, Bauhausstraße 11 - Pool G, Lab class, ab 04.04.2025

Mo, wöch., 09:15 - 10:45, Bauhausstraße 11 - Pool G, Lab class, ab 07.04.2025

Fr, Einzel, 10:00 - 12:00, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Prüfung / exam, 26.09.2025 - 26.09.2025

Fr, Einzel, 10:00 - 12:00, Karl-Haußknecht-Straße 7 - Seminarraum (IT-AP) 001, Prüfung / exam, 26.09.2025 - 26.09.2025

Beschreibung

Im ersten Teil der Veranstaltung werden die wichtigsten Verfahren und Techniken aus dem Bereich der Informationsvisualisierung für folgende Datentypen vorgestellt: multi-dimensionale und hierarchische Daten, Graphen, Zeitreihen und mengenbasierte Daten. Der zweite Teil beschäftigt sich mit verschiedenen Ansätzen und Algorithmen zur Visualisierung volumetrischer und vektorieller Simulations- und Messdaten. Die Veranstaltung wird englischsprachig angeboten.

In den Übungen werden eine Auswahl der in den Vorlesungen vorgestellten Visualisierungsansätze umgesetzt, getestet und evaluiert. Die abschließende Übungsaufgabe ermöglicht es Ihnen, ein eigenes Visualisierungsprojekt zu entwerfen, implementieren, evaluieren und präsentieren.

Voraussetzungen

Programmierkenntnisse sowie gute Kenntnisse von Algorithmen und Datenstrukturen sind erforderlich, z.B. nachgewiesen durch den erfolgreichen Abschluss der entsprechenden Lehrveranstaltungen des Bachelor-Studiengangs Medieninformatik.

In den Laborveranstaltungen werden JavaScript- und grundlegende GLSL-Programmierung eingesetzt. Grundkenntnisse der Computergrafik sind hilfreich, z.B. erworben durch die Vorlesung Computergrafik im Bachelor-Studiengang Medieninformatik.

Leistungsnachweis

Vorlesungsbegleitende, bewertete Übungen, mündliche oder schriftliche Prüfung und ein abschließendes Projekt.

301017 Exam: Mathematics for data science

B. Rüffer, M. Schönlein

Prüfung

Mi, Einzel, 09:00 - 17:00, Final examination - oral exam (organized by chair) --> please contact the responsible, 30.07.2025 - 30.07.2025

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 oral exam

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe

301017 Mathematics for data science

B. Rüffer, M. Schönlein

Veranst. SWS: 4

Vorlesung

Do, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Fr, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis**1 oral exam**

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe**417130003 Discrete Optimization****A. Jakoby**

Veranst. SWS: 4

Vorlesung

Do, wöch., 11:00 - 12:30, Bauhausstraße 11 - R 015, Lecture , ab 03.04.2025

Di, wöch., 15:15 - 16:45, Bauhausstraße 11 - R 015, lab class, ab 08.04.2025

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkomentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination

419140050 Introduction to Modern Cryptography**S. Lucks, N. Lang, J. Leuther**

Veranst. SWS: 3

Vorlesung

Fr, wöch., 11:00 - 12:30, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lab class 04Apr25: 1st Lecture, ab 04.04.2025

Mo, wöch., 13:30 - 15:00, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lecture, ab 07.04.2025

Mo, Einzel, 11:00 - 13:30, Bauhausstraße 11 - N 004, schriftliche Prüfung/ written exam, 29.09.2025 - 29.09.2025

Beschreibung

Früher galt die Kryptographie als Werkzeug für Militärs, Geheimdienste und Diplomaten. Aus dieser Zeit stammt auch noch die berühmte Enigma-Chiffriermaschine.

Heute entwickelt sich die Kryptographie buchstäblich zu einer Schlüsseltechnologie für sichere Kommunikation und Mediennutzung. Von der Öffentlichkeit kaum bemerkt hat die Kryptographie schon längst Einzug gehalten in alltäglich genutzte Geräte wie Geldautomaten und Mobiltelefone.

Der Entwurf kryptographischer Komponenten ist schwierig, und in der Praxis trifft man oft auf erhebliche Entwurfsfehler.

(Dies kommentiert der IT-Sicherheitsexperte Bruce Schneier mit drastischen Worten: "Milliarden von Dollar werden für Computersicherheit ausgegeben, und das Meiste davon wird für unsichere Produkte verschwendet.")

Nicht nur der Entwurf kryptographischer Komponenten ist schwierig, auch der Einsatz von "an sich guten" Komponenten für sichere IT-systeme ist fehlerträchtig und erfordert ein genaues Verständnis der jeweiligen Bedingungen, unter denen eine kryptographische Komponente als "sicher" gelten kann.

Die Vorlesung gibt einen Einblick in Denkweise und Methodik der Mediensicherheit und der modernen Kryptographie und die Anwendung der Kryptographie, um Sicherheitsprobleme zu lösen.

engl. Beschreibung/ Kurzkomentar

Bemerkung

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Für Studierende, die in ihrem früheren Bachelor-Studium keine Einführung in die Kryptographie besucht haben, ist die Veranstaltung ihrerseits Zulassungsvoraussetzung für fortgeschrittene Kryptographie-Vorlesungen.

Voraussetzungen

Regelmäßige Bearbeitung der Übungsaufgaben und Teilnahme an den Übungen, Klausur.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungsaufgaben, Klausur

420160000 Introduction to Natural Language Processing

B. Stein, M. Wolska, N. Mirzakhmedova, M. Wiegmann

Veranst. SWS: 3

Vorlesung

Do, wöch., 15:15 - 16:45, Bauhausstraße 11 - N 004, Lecture, ab 03.04.2025

Do, wöch., 17:00 - 18:30, Bauhausstraße 11 - N 004, Lab class, ab 03.04.2025

Do, Einzel, 15:15 - 18:30, Marienstraße 13 C - Hörsaal C, 10.04.2025 - 10.04.2025

Do, Einzel, 09:00 - 11:00, Marienstraße 13 C - Hörsaal A, schriftliche Prüfung/ written exam, 24.07.2025 - 24.07.2025

Do, Einzel, 09:00 - 11:00, Coudraystraße 13 B - Hörsaal 3, schriftliche Prüfung/ written exam, 24.07.2025 - 24.07.2025

Beschreibung

This course gives an overview of basic techniques of working with language data. We will introduce basic linguistic notions, issues involved in building and working with language corpora, current standard techniques for preparing

text for analysis, and methods of computational processing of a subset of language phenomena. By the end of the course students will

- (1) have an understanding of key word-level, syntactic, semantic, and discourse phenomena,
- (2) be aware of issues involved in building text corpora,
- (3) be familiar with typical language processing tasks addressed in the NLP community and methods of addressing them, and
- (4) will be able to perform tasks that are part of a standard NLP pipeline.

Leistungsnachweis

Klausur

424150030 Advanced Topics in Software Engineering

J. Ringert

Veranst. SWS: 2

Seminar

Fr, wöch., 15:15 - 16:45

Beschreibung

This module is a seminar worth 3 ECTS.

The module focuses on a systematic literature review:

- finding a topic from Software Engineering,
- defining research questions for a literature review, and
- reviewing Software Engineering literature to answer your research questions.

Your mark will be determined by:

- intermediate submissions of your progress,
- presentations of your findings during the semester, and
- a final seminar paper and presentation (submitted at the end of the semester).

Leistungsnachweis

Presentations during the semester

Final seminar paper

425160000 Current Topics in Cryptography: Secure Channels

S. Lucks, N. Lang, J. Leuther

Veranst. SWS: 2

Seminar

Di, Einzel, 17:00 - 18:30, InfoSec Lab, B11, Raum K016, 08.04.2025 - 08.04.2025

Beschreibung

Ein sicherer Kanal (secure channel) zwischen zwei oder mehreren Teilnehmern gewährleistet die Vertraulichkeit 1 und Integrität der übertragenen Daten. Ein Übertragungskanal zwischen zwei Entitäten kann beispielsweise durch die Verwendung von "Authenticated Encryption Modes", die sowohl Daten verschlüsseln als auch authentifizieren, sicher gemacht werden. In diesem Seminar werden Sie selbstständig ein ausgewähltes wissenschaftliches Thema aus dem Bereich der Kryptographie bearbeiten. Das Thema wird in Absprache mit den Betreuern ausgewählt. Auch selbst vorgeschlagene Themen oder Gebiet Ihrer Wahl (im Rahmen des Seminar-Themas) sind gerne gesehen. Es

wird Präsenztermine für den Kick-off, die Zwischenpräsentation und die Abschlusspräsentation geben. Dazwischen können bei Bedarf flexibel Termine für Fragen und Antworten vereinbart werden.

Bemerkung

Terminabsprache über Moodle-Kurs

Voraussetzungen

Introduction to Modern Cryptography (or equivalent)

Leistungsnachweis

Eigenständige Bearbeitung eines Themas, mündliche Präsentation zu einem Thema, Teilnahme an Diskussion zu den präsentierten Themen

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther

Veranst. SWS: 4

Vorlesung

Fr, wöch., 15:15 - 16:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lab class 04.04.25: 1st Lecture, ab 04.04.2025

Di, wöch., 09:15 - 10:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lecture, ab 08.04.2025

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzten Hashfunktionen wie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Struktur von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichten Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidaten drehen. Basierend auf den Erkenntnissen und Kandidaten des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einführung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung

4526501 Academic English Part One

G. Atkinson

Veranst. SWS: 2

Kurs

Mi, wöch., 15:15 - 16:45, Consultations, R.N212, B11 (indiv.appointments)

Mi, wöch., 17:00 - 18:30, Bauhausstraße 11 - R 015, Academic English Part I+II (alternating)

Beschreibung

This is the first part of a two-part course which aims to improve your ability to express yourself clearly in written English and to develop a suitably coherent academic writing style. Part One concentrates mainly on structure in writing academic articles, essays and reports. We begin by examining the structure of individual paragraphs and move on to extended texts of various types (e.g. process essays, cause/effect, comparison/contrast, etc.). Particular attention is paid to connectives, i.e. transitional phrases and constructions which help you link ideas and paragraphs in a logical, systematic way.

Bemerkung

You are advised to take Part One first, although it is possible to take both parts in reverse order or concurrently (i.e. in the same semester). You may only do the latter on the authority of the course leader (Atkinson).

Voraussetzungen

Registration (compulsory)

All students must register. First time participants are required to present a B2 English Level certificate along with their email registration. All students, **including those who have already taken Academic English Part Two and those who need to repeat Academic English Part One**, must register by contacting Howard Atkinson at: howard.atkinson@uni-weimar.de.

You will be informed by email when registration opens and when the deadline is. Please do not attempt to register until you have received this Email. Registration Emails should be given the subject heading: AE I Registration.

Leistungsnachweis

continuous assessment

4526502 Academic English Part Two

G. Atkinson

Veranst. SWS: 2

Kurs

Mi, wöch., 15:15 - 16:45, Consultations, R.N212, B11 (indiv.appointments)

Mi, wöch., 17:00 - 18:30, Bauhausstraße 11 - R 015, Academic English Part I+II alternating

Beschreibung

Part Two of the Academic English course concentrates on improving and refining aspects of academic writing style. It includes sections on clause and sentence structure, punctuation rules and how to incorporate quotations, statistics and footnotes into academic texts.

Bemerkung

You are advised to take Part One first, although it is possible to take both parts in reverse order or concurrently (i.e. in the same semester). You may only do the latter on the authority of the course leader (Atkinson).

Voraussetzungen

Registration (compulsory)

All students must register. First time participants are required to present a B2 English Level certificate along with their email registration. All students, **including those who have already taken Academic English Part One and those who need to repeat Academic English Part Two**, must register by contacting Howard Atkinson at: howard.atkinson@uni-weimar.de.

You will be informed by email when registration opens and when the deadline is. Please do not attempt to register until you have received this Email. Registration Emails should be given the subject heading: AE II Registration.

Leistungsnachweis

continuous assessment

4556227 Usability Engineering & Testing

J. Ehlers

Veranst. SWS: 4

Vorlesung

Di, wöch., 13:30 - 15:00, Bauhausstraße 11 - N 004, Lecture / lab class online , ab 08.04.2025

Di, Einzel, 15:30 - 17:30, Steubenstraße 6, Haus F - Hörsaal K20, schriftliche Prüfung/ written exam, 22.07.2025 - 22.07.2025

Beschreibung

Usability indicates the "absence of frustration". But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesizing. We will also discuss procedures for quantitative data analysis and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

engl. Beschreibung/ Kurzkomentar

Usability indicates the "absence of frustration". But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesizing. We will also discuss procedures for quantitative data analysis and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

Leistungsnachweis

Empirical exercises (tutorial) and written exam

Project

425110000 Agent-based AI for Illumulus

B. Stein, T. Gollub, S. Ruth

Veranst. SWS: 10

Projekt

Beschreibung

What makes a story a good story? In the project, we want to develop multi-modal story quality metrics which allow for the implementation of an agent-based feedback loop into Illumulus, our story generation AI.

Goals: Develop next version of Illumulus featuring :

- The state-of-the-art models for text and image generation.
- Automated story and image quality assessment
- Agent-based feedback loop
- Adherence to context information (about the user and the event).
- A conversational interface for the user interaction.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Projektbericht, Abschlusspräsentation

425110002 Human Cognition & AI

M. Jakesch, N. Navajas Fernández
Projekt

Veranst. SWS: 10

Beschreibung

As AI technologies models increasingly shape industries, communication, and decision-making, understanding their impact has never been more urgent. Participants will work on timely research questions across key areas related to the societal impact of AI, including bias and fairness, misinformation and disinformation, ethical and economical consequences, as well as regulatory frameworks. The specific research questions will be presented at the project fair.

After initial engagement with the relevant literature and tools, participants will conduct hands-on empirical research, including data analysis, AI prototypes, and surveys or experiments. The format offers students the opportunity to develop their skills in their area of interest, to get to know the lab's research, and (evtl.) work towards their first publication.

The project concludes with writing sessions, and the expected output will be a draft of an investigative report or scientific paper. Participants' results will contribute to an ongoing global conversation about how society can navigate the development of AI technologies in a way that enable their benefits while minimizing risks.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Students must have successfully completed one of the following courses:

- Methods of Social Data Analysis
- Natural Language Processing
- Machine Learning

Time commitment: 2x8h/week for 12ECTS and 3x8h/week for 18 ECTS; students taking more than 32ECTS (adjusted for other part-time work) this term are not eligible.

If you do not clearly fulfill the requirements but believe that you would make a strong project participant, please reach out to the instructor.

Leistungsnachweis

Research paper and presentation

425110003 Bobby Tables - How to Implement an Insecure System

S. Lucks, N. Lang, J. Leuther
Projekt

Veranst. SWS: 10

Beschreibung

Um zu verstehen, wie man ein sicheres System erstellt, fangen wir damit an, absichtlich ein unsicheres System zu bauen. Inspiriert von OWASP's Juice Shop (<https://help.owasp-juice.shop/>) ist unser Ziel, eine Plattform zu entwickeln, welche verschiedene Sicherheitslücken aufweist, um als Übungen für Penetrationstests und andere Angriffe genutzt werden können. Ausgehend vom Konzept des berühmten XKCD-Comics „Exploits of a Mom“ (<https://xkcd.com/327/>) möchten wir eine Plattform in einem Schulumfeld gestalten.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

At least one of the following:

- very good programming skills
- passed Webtechnologie
- passed Software Engineering
- passed Einführung in die Programmierung

Leistungsnachweis

Zwischenpräsentationen, Abschlusspräsentation, Abschlussbericht

425110004 Building Language Models

B. Stein, M. Wiegmann
Projekt

Veranst. SWS: 10

Beschreibung

There are many moving parts when using language models for text generation: the model technology (n-gram, RNN, Transformers) and its parameters, the data used to fit the model, and various sampling and decoding strategies. It is difficult to understand how each of these parts influences the generation performance. In this project, we want to build a configurable system where we can easily exchange parts and observe how this change influences the generation.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Projektbericht, Abschlusspräsentation

425110005 Digital Twin for a Building Exposed to Wind Hazards

C. Koch, M. Artus, G. Morgenthal, A. Athanasiou
Projekt

Veranst. SWS: 10

Beschreibung

The project starts with the collection of design information pertaining to the case study - a wind sensitive building in Weimar. Subsequently, climatic data for the city of Weimar is gathered. Guidance is provided to students in the design and development of the sensor system. The students are responsible for programming the sensors and integrating the collected sensor data into the system. Data engineering processes are employed to interpret sensor measurements and update system parameters. Ultimately, the students develop a virtual twin that visualizes the building's observed performance.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Project report and short oral presentation.

425110007 Digital Ventures Lab

M. Jakesch
Projekt

Veranst. SWS: 10

Beschreibung

In this project, students develop an innovative product idea and work on the planning, development, and market entry of digital products. The hands-on format is aimed at highly motivated students in HCI and computer science who have an interest in product development and entrepreneurship.

At the beginning of the course, students use methods such as Design Thinking to identify problem areas and develop innovative product ideas. In the second phase, the teams collect data to refine their product idea through interviews with potential users, and explore the market environment through research.

In the third phase, students work on developing a prototype or Minimum Viable Product (MVP) to test the product's core functionalities and assess its technical feasibility. The goal of the project is to create an initially validated product and business concept, which prepares the team for startup programs like the Neudeli Fellowship or EXIST.

The project includes structural and methodical guidance but requires a high level of motivation and independence of participants. In addition to technical and business competencies, participants develop their leadership skills as well as communication and teamwork abilities

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Personal initiative: Interest in entrepreneurship, startups, product development, innovation.

Significant time commitment: Minimum 2x8h/week for 12ECTS and 3x8h/week for 18 ECTS; students taking more than 32ECTS (adjusted for other part-time work) this term are not eligible.

Please send your CV, a statement of interest, and an explanation of your time commitment to the instructor prior to enrollment

Leistungsnachweis

Minimum viable product and business plan

425110008 Distributed Wireless Sensor Systems and Digital Twins

J. Ringert, B. Burse, M. Artus
Projekt

Veranst. SWS: 10

Beschreibung

We will develop low-cost distributed sensor nodes and apply them in a case study setting. The measures sensor data will be stored and made available for different analysis scenarios, e.g., exploring augmented building information models (BIMs).

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Digital Engineering students must have completed their foundations

Leistungsnachweis

Projektbericht und Ergebnisse in Form von Software

425110009 Embodied Conversational Agents in Social Virtual Reality

B. Fröhlich, E. Schott, T. Zöppig
Projekt

Veranst. SWS: 10

Beschreibung

The growing capabilities of large language models and text-to-speech technology are expanding the use of conversational agents. In virtual environments, these agents can be represented as animated avatars, leading to more lively and engaging VR experiences, e.g. when using them as guides in virtual museums. However, communication with these agents in VR relies entirely on speech, as traditional text input is no longer an option. In this project, we aim to extend previous work of our research group to multi-user settings (i.e. social virtual reality), making interactions more natural and intuitive while integrating multiple agents into virtual worlds. The key challenge is to ensure smooth communication between multiple VR users and multiple AI agents without overwhelming or confusing conversations. We will investigate how users can initiate interactions with agents without explicit selection of a specific agent and how they can receive additional information in an intuitive way. To explore these aspects, you will build on our existing integrations of OpenAI's language models and animated avatars in Unity3D. You will investigate different modalities such as pointing, looking, and speaking to select agents and experiment with ways to playfully engage VR users in immersive experiences. During this project, you will learn to design multi-user virtual reality applications and deepen your understanding of virtual reality development. Furthermore, you will explore advanced multi-modal interaction concepts, gain practical experience using OpenAI's API and enhance your proficiency with Unity3D and C#. Prior experience with C#, Unity3D, and multi-user VR is strongly advised. Additionally, familiarity with rigging and character animations will be beneficial. Equipment for VR development will be provided.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Solid software programming / scripting experience (e.g. C#, C++, Python). Experience in Unity is very helpful. Experience with rigging and character animations could be beneficial. Successful completion of the Virtual Reality course is recommended.

425110010 Hot Topics in Computer Vision: Realistic Relighting of Point Clouds

V. Rodehorst, J. Eick, A. Frolov, M. Kaisheva, D. Tschirschwitz
Projekt

Veranst. SWS: 10

Beschreibung

Die Teilnehmer werden an ein aktuelles forschungs- oder industrierelevantes Thema herangeführt. Es ist nicht beabsichtigt einen festgelegten Bereich in voller Breite zu explorieren. Stattdessen werden die Teilnehmer mit der vollen Komplexität eines begrenzten Themas konfrontiert und die Eigeninitiative gefördert. Es ermöglicht einen Einblick in die Forschungs- und Entwicklungsprojekte des Fachgebiets.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Vorlesungen „Photogrammetric Computer Vision“ oder „Image Analysis and Object Recognition“ wünschenswert. Gute Programmierkenntnisse (z.B. C/C++, MATLAB/Octave, Python, OpenCL/CUDA)

Leistungsnachweis

Aktive Mitarbeit, Einführungsvortrag, Abschlusspräsentation, Dokumentation

425110011 Logic, Argumentation, and LLMs

B. Stein, K. Heinrich, M. Kanadan
Projekt

Veranst. SWS: 10

Beschreibung

Large language models (LLMs) have remarkable language capabilities that open up new possibilities for logical reasoning and argumentation. This project explores reasoning and argumentation abilities of LLMs using various approaches, including Walton's argument schemes and knowledge bases.

Goals: Development of an argumentation agent that is able to:

- detect and analyze argument structures, and
- identify inconsistencies and weak points in an argumentation.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Projektbericht, Abschlusspräsentation

425110012 Manipulierte Flüsse**A. Jakoby, R. Adejoh**
Projekt

Veranst. SWS: 10

Beschreibung

... folgt.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Vorträge, Programme, Projektbericht, Abschlusspräsentation

425110013 Out of Bounds | Bauhaus Gamesfabrik**C. Wüthrich, W. Kissel, G. Pandolfo**
Projekt

Veranst. SWS: 10

Beschreibung

Herzlich willkommen bei Out of Bounds | Bauhaus Gamesfabrik, einem spannenden interdisziplinären Projekt, das die Fakultäten Kunst & Gestaltung und Medien an unserer Universität zusammenbringt. In diesem innovativen Projekt arbeiten Studierende unterschiedlicher Fachrichtungen in interdisziplinären Gruppen zusammen, um die dynamische Welt der Spieleentwicklung zu erkunden. An der Schnittstelle von Kunst und Technologie dient Out of Bounds | Bauhaus Gamesfabrik als Spielwiese für Kreativität und Innovation. Studierende der Fakultät Kunst & Gestaltung bringen ihre Expertise in visueller Ästhetik, Erzählkunst und Konzeption ein, während diejenigen der Fakultät Medien ihre Fähigkeiten in Programmierung, Animation und interaktiven Medien einbringen. In diesem gemeinschaftlichen Unterfangen werden interdisziplinäre Gruppen gebildet, die einen reichen Ideen- und Perspektivenaustausch fördern. Inspiriert vom Pioniergeist der Bauhaus-Bewegung, wo Kunst und Technologie zusammenkamen, um das moderne Design zu prägen, begeben sich unsere Studierenden auf eine Reise, um immersive und fesselnde Spielerlebnisse zu gestalten. Im Laufe des Projekts vertiefen sich die Studierenden in verschiedene Aspekte der Spieleentwicklung, von der Ideenfindung und Prototypenerstellung bis hin zur Produktion und Präsentation. Unter der Anleitung eines erfahrenen Mentors beider Fakultäten lernen sie, die Komplexität interdisziplinärer Teamarbeit zu bewältigen und ihre einzigartigen Stärken zu nutzen, um Herausforderungen zu meistern und ihre kreative Vision zu verwirklichen. Out of Bounds | Bauhaus Gamesfabrik ist mehr als nur ein Kurs; es ist eine transformative Erfahrung, die Studierenden ermöglicht, die Grenzen des traditionellen Spieldesigns zu überschreiten. Indem sie die Zusammenarbeit fördern und den Geist des Experimentierens annehmen, sind unsere Studierenden bereit, die nächste Generation visionärer Spieleentwickler zu werden und die Zukunft interaktiver Unterhaltung mitzugestalten. Begleiten Sie uns auf dieser aufregenden Reise, auf der digitale Träume Wirklichkeit werden, und lassen Sie uns gemeinsam die Zukunft des Spielens an der Schnittstelle von Kunst und Technologie gestalten.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Studierende der Medieninformatik sollten Programmierkenntnisse mitbringen. Studierende der Medienwissenschaft ein grundlegendes Interesse für Storytelling / Game Design

Leistungsnachweis

Abschlusspräsentation, fertiges Spiel.

425110014 Red Pill II – Verstecke die Matrix

A. Jakoby, R. Adejoh
Projekt

Veranst. SWS: 10

Beschreibung

... folgt.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Vorträge, Programme, Projektbericht, Abschlusspräsentation

425110015 ReVRse: Semantic Editing Tools for Immersive Recordings

B. Fröhlich, K. Brehm, A. Lammert, T. Zöppig
Projekt

Veranst. SWS: 10

Beschreibung

Immersive recordings capture events and interactions in virtual environments and allow users to explore them both temporally and spatially in virtual reality. Unlike 2D video and even 360 degree video, immersive recordings capture spatiotemporal data of a 3D virtual environment. Such recordings can be viewed from multiple perspectives and even interacted with during playback in VR. This unique capability makes immersive recordings a powerful tool, e.g. for psychotherapy. Recordings of reenactments of meaningful social interactions in VR could be collaboratively reviewed, analysed and modified according to therapeutic goals. In this project, you will extend an existing recording system to capture semantic data, such as actions like 'picking up and moving a bottle'. This will involve designing a suitable data structure to capture and store semantic data. By incorporating this data, the system can be programmed to maintain logical consistency when changes are made to the recordings. For example, if an action such as grasping the bottle is removed, the playback will automatically be updated to keep the bottle stationary. You will also investigate interaction techniques for allowing users to modify recorded interactions in virtual reality. This includes experimenting with playful approaches to engage users, such as developing a miniature 'dollhouse' version of the immersive environment. In this miniature, users can manipulate recorded actions by interacting with action figures or dolls that represent recorded characters. During the project, you will learn to design virtual reality applications and implement these applications using Unity3D and C#. For participants with experience in C++ programming, the extension of the underlying C++ plug-ins for Unity3D is also a potential task.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Solid software programming / scripting experience (C#, C++, Python o.Ä.). Experience in Unity is very helpful. Successful completion of the Virtual Reality course is recommended.

425110016 Schwamm drüber - Using Sponges for Security

S. Lucks, N. Lang, J. Leuther
Projekt

Veranst. SWS: 10

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

- Introduction to Modern Cryptography (or equivalent)
- Interest in scientific work

Leistungsnachweis

Zwischenpräsentationen, Abschlusspräsentation, Abschlussbericht

425110017 Software Engineering for Autonomous Vehicles 2

J. Ringert, .. Soaibuzzaman
Projekt

Veranst. SWS: 10

Beschreibung

We will develop software to control autonomous vehicles. The physical vehicle will be equipped with a range of sensors, e.g., LiDAR, cameras, gyroscopes, and distance sensors. We will use industry strength software platforms like the Robot Operating System (ROS2).

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Digital Engineering students must have completed their foundations.

Leistungsnachweis

Projektbericht und Ergebnisse in Form von Software

425110018 Textwasserzeichen

A. Jakoby, R. Adejoh
Projekt

Veranst. SWS: 10

Beschreibung

... folgt.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Vorträge, Programme, Projektbericht, Abschlusspräsentation

425110020 Urban Togetherness: Cross-Medium Artifact Design for Urban Community Engagement

E. Hornecker, M. Osipova

Veranst. SWS: 10

Projekt

Mi, Einzel, 15:00 - 18:00, Karl-Haußknecht-Straße 7 - Seminarraum (IT-AP) 001, 28.05.2025 - 28.05.2025

Beschreibung

Urban communities are drivers for positive urban change and comfort of living: neighbours organise dinners together, green communities push forward sustainable initiatives, students co-organise exhibitions etc. In the post-pandemic world, however, such things became rarer and more complex to ignite due to the trend of distancing and remote problem-solving.

This project invites you to explore, how technology can be imbedded in the urban space to play a role of a community "champion": inviting people to interact, spend time together and bring to life the spirit of Urban Togetherness.

Within this project you work with one of the Weimar communities and design a solution fitting their main challenges. You are free to explore and experiment with how the solution can look like and function through physical prototyping. The resulting prototypes will be presented at the Summaery 2025.

You will learn more about Urban Technology and Community Engagement through research through design approach. Physical prototyping skills are desired but learnable within the project. Interest in academic research is a desired pre-requisite as well, since the first phase is dedicated to exploring the literature.

The project's phase runs till the end of September (presence in Weimar is mandatory, break for exams is scheduled and personal vacations are possible with a prior notice and discussion) with an annotated portfolio report due the 1.10.2025. Expected workload during semester time is approximately 2 working days per week for 12 ECTS and 3 working days for 18 ECTS. The research results could turn into a MuC Student Research Competition submission or form the base for your thesis research.

All students need to email Margarita with CV to check whether you qualify for the project. Feel free to reach out for more details or with questions or clarifications to be sure that this project is a good fit for you. margarita.osipova@uni-weimar.de <mailto:margarita.osipova@uni-weimar.de>

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Students from HCI Masters and CS4DM and Bachelor (Medien)Informatik: have successfully completed at least one of the following courses by HCI chair: "HCI Research Methods", "Ubiquitous Computing", "HCI Introduction".

We further expect general interest in physical prototyping, desire to be creative, ability to contribute to conceptual work and willingness to work in a team.

To avoid issues after the project selection algorithm, we require interested students to write an email to Margarita to confirm eligibility for participation in the project.

Students from non-Computing programs (Master Media Architecture, Product-Design (BA/MA), Media Arts/Design (BA/MA) : Creativity, practical experience with physical construction (e.g. 3D-printing, laser-cutting, woodwork etc.), ideally some prior experience with electronics and Arduino.

Interested students from these non-Computing programs must apply and contact Margarita via email. Please apply until the end of the 31.03.2025 by E-Mail to margarita.osipova@uni-weimar.de <<mailto:margarita.osipova@uni-weimar.de>>

weimar.de> (please include a description of your prior experience in relevant areas, with examples of prior work if applicable) !

425110021 VRinSync

B. Fröhlich, E. Hornecker, J. Ehlers, L. Klass, A. Lammert, L. Simon Verant. SWS: 10
Projekt

Beschreibung

Collaborative activities such as dancing, singing, and movement games, which are based on synchronized interpersonal interaction have the potential to evoke feelings of togetherness and strengthen social bonds. Engaging in such activities with friends and family living far away from each other continues to be difficult, even in Virtual Reality (VR). One of the main difficulties for synchronised activities in VR is latency effects, which disrupt the experience of synchronous movement and often result in a poor user experience. Instead of togetherness, people feel disconnected and "out of sync". The phenomenon of falling into the same rhythm over time while interacting with another person has been extensively investigated and is referred to as "entrainment". This process typically occurs unconsciously, leading to coordinated movements that enhance feelings of sympathy, intimacy, and closeness. Social Virtual Reality (SVR) enables users to engage in shared activities, and thus being closer to real-life encounters but current VR environments and applications do not adequately support collaborative activities that rely on temporal synchronization. In this project, we will utilise different prototyping and development approaches to investigate what kind of interaction techniques can be applied to enhance entrainment in VR and how the feeling of shared synchronous experiences can be increased. For this purpose, we would like to investigate whether the effect of entrainment applies for SVR the same way as it does in reality and want to identify components that inhibit or promote entrainment in such designs e.g. how different feedback and environmental modalities can support perceived synchrony within movement based interactions. Step by step, we will identify difficulties during social interactions in latency affected environments and develop concepts to foster a shared sense of synchrony, which will then be implemented in Unity. To evaluate the implemented methods, we will employ qualitative methods alongside eye-tracking measurements e.g. to identify attention shifts or breaks in presence. This course is ideal for students who enjoy working individually and in multidisciplinary teams, who can identify challenges and problems, and take initiative in developing innovative solutions. We encourage students to participate that have a high interest in working from theory, coming up with speculative concepts, and learning how to realise those concepts as an artefact.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Interest in interaction design and different types of prototyping.

Or

Solid programming / scripting experience (C#, C++, Python o.Ä.).

Experience in Unity and/or with VR recommended.

All participants should enjoy working in an interdisciplinary group, want to be creative, build prototypes, and be able to converse in English.

425110032 Pupillenbasierte Kognometrie zur Nutzerauthentifizierung

J. Ehlers Verant. SWS: 10
Projekt

Beschreibung

Cognometrics can be defined as a class of authentication techniques that build on cognitive or motor abilities of the human user. The current project aims to investigate user interfaces that employ pupil-related data for the purpose of distinguishing individual users. Students should first familiarize themselves with the literature on cognitive pupillometry. In the following project stage, the task is to design two interface prototypes that utilize pupil dynamics for access authentication. Pupillary data are then to be collected in a laboratory study. In the concluding phase of the project, a systematic analysis will be conducted utilizing machine learning methodologies to assess the viability and practicality of the outcome.

Bemerkung

Time and place will be announced at the project fair.

Voraussetzungen

Basic knowledge in machine learning, e.g. the course "Introduction to Machine Learning" should have been completed

Leistungsnachweis

- 1) Design two interface prototypes that utilize pupil dynamics for access authentication
- 2) Conduct a laboratory study to collect pupillary data
- 3) Apply machine learning techniques to evaluate the usability of the outcome
- 4) Document the results in an empirical report

425110033 Opinion dynamics: how are you influenced by others?

M. Schönlein
Projekt

Veranst. SWS: 10

Beschreibung

This project is concerned with various modelling techniques to describe the evolution of different opinions within an interacting group of individuals. A central part will be the modelling of the interaction among individuals. In this context, an essential part is the description of several mechanisms how the opinion of an individual is influenced by others. This is particularly important if the considered group of individuals is not homogenous. For instance, in the case that group contains extremist trying to make their idea to the leading opinion. The objectives are to devise and implement different modelling techniques to describe the evolution of opinions within groups. Starting from popular existing models, one goal of the project is to investigate new interaction mechanisms.

Bemerkung

Time and place will be announced at the project fair.

425110034 Statistical analysis in modern academia

M. Schönlein, S. Bock
Projekt

Veranst. SWS: 10

Beschreibung

The academic world increasingly faces challenges related to publication misconduct. Many ethically questionable practices are related to predatory journals and predatory publishers, as these do not implement and enforce sound quality control measures. A list of these "bad players", known as Beall's List [Bea], can help researchers to avoid publishing in outlets of questionable quality. The list is not free from criticism,

though, and it is curated by humans. This list may also not be complete. This project aims to use statistics and machine learning techniques to automatically separate the good from the bad journals. The objective of this project are to devise and implement algorithms that will identify and separate "good" and "bad" academic journals.

Bemerkung

Time and place will be announced at the project fair.

425110035 When Code Meets Fluid Flow

M. Schönlein, N. Gorban

Veranst. SWS: 10

Projekt

Beschreibung

This project explores fluid dynamics through interactive simulation. Using a particle-based numerical approach, students will model how fluids move around obstacles and respond to changes in boundary conditions. The simulation will be implemented in Python and visualized with animations. The project combines mathematics, physics, programming, and engineering insight in an accessible and creative way.

Bemerkung

Time and place will be announced at the project fair.

Specialization

301017 Exam: Mathematics for data science

B. Rüffer, M. Schönlein

Prüfung

Mi, Einzel, 09:00 - 17:00, Final examination - oral exam (organized by chair) --> please contact the responsible, 30.07.2025 - 30.07.2025

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 oral exam

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe**301017 Mathematics for data science****B. Rüffer, M. Schönlein**

Veranst. SWS: 4

Vorlesung

Do, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Fr, wöch., 13:30 - 15:00, Coudraystraße 13 B - Hörsaal 3

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

linear regression, logistic regression, dimension reduction, principle component analysis, linear discriminant analysis, multidimensional scaling, k-means clustering, support vector machines, kernel methods, neural networks, natural language processing

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis**1 oral exam**

"Mathematics for data science"

30 min (100%) / **SuSe** + WiSe

417130003 Discrete Optimization**A. Jakoby**

Veranst. SWS: 4

Vorlesung

Do, wöch., 11:00 - 12:30, Bauhausstraße 11 - R 015, Lecture , ab 03.04.2025

Di, wöch., 15:15 - 16:45, Bauhausstraße 11 - R 015, lab class, ab 08.04.2025

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkomentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther

Veranst. SWS: 4

Vorlesung

Fr, wöch., 15:15 - 16:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lab class 04.04.25: 1st Lecture, ab 04.04.2025
Di, wöch., 09:15 - 10:45, Karl-Haußknecht-Straße 7 - Hörsaal (IT-AP), Lecture, ab 08.04.2025

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzten Hashfunktionen wie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Struktur von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichten Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidaten drehen. Basierend auf den Erkenntnissen und Kandidaten des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einführung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung