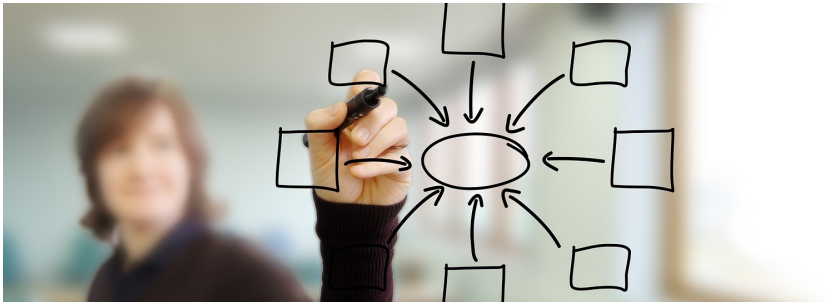
FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

DEPARTMENT
INFORMATIK
DIDAKTIK DER INFORMATIK

W-Seminare mit dem Leitfach Informatik



www.lehramt-informatik.de/w-seminare

Im wissenschaftspropädeutischen Seminar (W-Seminar) sollen Schülerinnen und Schüler einen Einblick in wissenschaftliches Arbeiten erhalten und grundlegende fachübergreifende Kompetenzen erwerben, um für ein universitäres Studium vorbereitet zu sein.

Sowohl für Lehrkräfte als auch für Schülerinnen und Schüler ist ein solches Seminar eine große Herausforderung: Es werden selbständige Arbeit und Recherche sowie das kritische Hinterfragen von Quellen und Ergebnissen gefordert. Insbesondere die Fachwissenschaft Informatik stellt die Schülerinnen und Schüler vor spezielle Anforderungen: Die verwendete Methodik zeigt Einflüsse von formal-strukturellen (Mathematik), experimentellen (Naturwissenschaften), konstruktiven (Ingenieurwissenschaften) und empirischen (Sozialwissenschaften) Disziplinen.

Diese Broschüre soll als Hilfestellung dienen, um Lehrkräfte bei der Gestaltung und Durchführung von W-Seminaren zu unterstützen.

In dieser Broschüre finden Sie daher…

...die Ergebnisse einer Auswertung über typische Schwierigkeiten, die Schülerinnen und Schüler mit W-Seminararbeiten in Informatik haben.

...Vorschläge zu Rahmen- mit dazugehörigen Seminararbeitsthemen.

Inhaltsverzeichnis

Weitere Information zur erfolgreichen Gestaltung eines W-Seminars in der Informatik, zum Dr. Hans-Riegel-Fachpreis sowie ständig aktualisierte und weitere Themenvorschläge finden Sie auf unserer Homepage unter htttps://www.lehramt-informatik.de/w-seminare

Wissenschaftler/-innen suchen Antworten!

Früh übt sich, wer Wissenschaftlerin oder Wissenschaftler werden will! In bayerischen Gymnasien bietet dafür das wissenschaftspropädeutische Seminar (W-Seminar) die Möglichkeit, wissenschaftliches Arbeiten zu erlernen und anzuwenden. W-Seminararbeiten im MINT-Bereich können für den Dr. Hans Riegel-Fachpreis eingereicht werden: Im Rahmen dieses Preises werden durch kooperierende Universitäten besonders gute Arbeiten ausgezeichnet.

Im Folgenden werden zentrale Ergebnisse der Auswertung der am Department Informatik der Friedrich-Alexander-Universität Erlangen-Nürnberg eingereichten Arbeiten präsentiert. Grundlage dieser Auswertung sind die 39 eingereichten Arbeiten aus den Jahren 2016 und 2017. Basierend auf der empirischen Analyse typischer Probleme werden Empfehlungen für die erfolgreiche Gestaltung einer W-Seminararbeit gegeben.

Klare Fragestellung

Wissenschaftliches Arbeiten ist durch ein systematisches Vorgehen gekennzeichnet: Zunächst wird meist eine Fragestellung oder These formuliert, die daraufhin mit der Methodik der jeweiligen Wissenschaft bearbeitet bzw. überprüft und dementsprechend akzeptiert, verworfen oder modifiziert wird. Wissenschaft ist daher stets erkenntnisorientiert: Es soll eine konkrete Frage beantwortet werden.

Dagegen fand sich in nur 10 % der untersuchten W-Seminararbeiten eine zentrale Fragestellung. Von den übrigen 90 % hatte lediglich die Hälfte eine klare Zielsetzung, die herausgestellt und in der Arbeit verfolgt wurde. Eine Fragestellung (bzw. zumindest eine Zielsetzung) motiviert die Arbeit, sorgt für eine sinnvolle Gliederung, hilft bei einer nachvollziehbaren Darstellung des Erkenntnisprozesses und bei der Begrenzung auf relevante und für die Beantwortung der Fragestellung wesentliche Informationen. Insgesamt kann eine sinnvolle Fragestellung dazu beitragen, die Qualität einer W-Seminararbeit deutlich zu steigern.

Quellcode und Diagramme

Beschränkung auf Dokumentation oder Bedienungsanleitung

In der Informatik ist die konkrete Implementierung in Hard- und Software

zum Zwecke der Simulation oder experimentellen Auswertung, Evaluation oder zum Testen häufig Bestandteil wissenschaftlicher Arbeit. Hier schließt sich die Frage an, welchen Umfang und in welcher Form dies Teil der Ausarbeitung werden sollte. Zunächst einmal gilt: Eine wissenschaftliche Arbeit ist weder Dokumentation des Programmcodes noch Bedienungsanleitung. Gleichzeitig ist sie keine kleinschrittige Dokumentation des Entwicklungsprozesses (so ist z. B. die schrittweise Installation des Betriebssystems auf einem Raspberry Pi inklusive eingegebener Konsolenbefehle kein Bestandteil einer wissenschaftlichen Arbeit). Andererseits ist es durchaus wichtig, relevante Details des „Versuchsaufbaus“ (z. B. die verwendete Hard- und Software) zu diskutieren sowie prozessbezogene Details (z. B. warum so gemessen wurde) zu beschreiben, um Transparenz, Reliabilität sowie Nachvollziehbarkeit zu gewährleisten.

In 64 % der analysierten Arbeiten machten Beschreibungen von Programmcodes oder Bedienungsanleitungen für die entwickelte Software jedoch einen Großteil der Arbeit aus. In W-Seminararbeiten sollte der Schwerpunkt jedoch auf der wissenschaftlichen Arbeit liegen. Solche Beschreibungen oder Bedienungsanleitungen können daher nur ein Beiprodukt darstellen.

Unnötiger Quellcode

Auch stellt sich die Frage, wie mit Quellcode umzugehen ist. Vereinzelte Codezeilen, etwa zur Erläuterung eines Beispiels, sind hier nicht gemeint; problematisch wird Quellcode jedoch, wenn lange Stücke eines Programmcodes im Fließtext auftauchen, da sie dort den Verlauf der Arbeit stören und in der Regel keinen Beitrag zum Nachvollziehen bzw. Verständnis leisten.

Etwa 40 % der untersuchten W-Seminararbeiten mit Implementierungsanteilen beinhalteten überflüssigen Quellcode im laufenden Text. Im Fließtext sollte Code jedoch nur aufgenommen werden, wenn er zur Verdeutlichung von zentralen Algorithmen oder Lösungen für zuvor aus theoretischer Perspektive thematisierte Problemstellen o. ä. dient. Ausführlicher Programmcode sollte sich hingegen idealerweise im Anhang der Arbeit finden, wo er bei Bedarf jederzeit nachgeschlagen werden kann.

Unnötige Diagramme

UML-Diagramme oder anderweitige Ergebnisse von Modellierungsarbeiten können einen Beitrag zum Verständnis bzw. der Nachvollziehbarkeit der Arbeit leisten. Das gelingt jedoch nur, wenn solche Darstellungen im Text aufgegriffen, erläutert, oder diskutiert werden.

In 23 % aller analysierten Arbeiten fanden sich jedoch UML– oder andere Diagramme, die entweder ganz für sich und ohne Erläuterungen, d. h. als reine Illustration standen, oder aber keinen Beitrag zur Nachvollziehbarkeit der Ausführungen leisteten.

Objektivität

Wissen unterscheidet sich von Glauben, Vermutung und Meinung. Aus diesem Grund sollten die Ergebnisse einer wissenschaftlichen Arbeit sich nicht auf die persönliche Meinung stützen: Die Argumentation muss objektiv, transparent und nachvollziehbar sein. In 23 % der untersuchten Arbeiten fanden sich persönliche Meinungen der Autoren, die dadurch die Gültigkeit der Aussagen minderten. Persönliche Meinungen sollten daher nur in einem klar von den Ergebnissen unterscheidbaren persönlichen Fazit o. Ä. vorkommen.

Fachliteratur

Mithilfe von Fachliteratur wird eine Arbeit im größeren Kontext verortet. Die Verwendung von passenden Quellen zeigt außerdem, dass sich mit dem Thema angemessen auseinandergesetzt wurde. Trotzdem verwendeten 49 % der untersuchten Arbeiten keine Fachliteratur, was dazu führte, dass solchen Arbeiten die Einbettung in einen theoretischen Kontext fehlte und wichtige Erkenntnisse aus dem Themenbereich der Arbeit keine Erwähnung fanden.

Welche Quellen sind also passend? Insbesondere Wikipedia oder Tutorials sind in der Regel nicht zitierfähig, während Bücher oder Artikel (die auch im Internet bei zuverlässigen Quellen gefunden werden können) oftmals einen besseren Überblick über ein Thema geben können. Hierbei sollte auf die Verwendung von zumindest einem repräsentativen Werk für das jeweilige Themengebiet geachtet werden.

Angabe von Quellen

In 15 % der untersuchten Arbeiten fanden sich fehlerhafte Zitationen. Diese Fehler reichten von falscher Angabe aufeinander folgender Quellenangaben über uneinheitlichen Stil bis hin zu Formatierungsfehlern. Obwohl es für Zitationen nicht das eine korrekte Format gibt, ist es am besten, sich auf ein bestimmtes Format festzulegen und dieses in der gesamten Arbeit konsistent zu verwenden (wie z. B. MLA, Cambridge oder APA). Immer im Hinterkopf sollte der Zweck von Quellenangaben bleiben: Durch diese soll der zugehörige Eintrag im Literaturverzeichnis leicht identifizier- und auffindbar sein.

Checkliste:

- ☐ Beinhaltet die Arbeit eine klare Fragestellung? Falls nicht: Ist zumindest eine Zielsetzung erkennbar und klar formuliert?
- ☐ Verfolgt die Arbeit die Klärung dieser Fragestellung bzw. Zielsetzung und ist das methodische Vorgehen hierfür beschrieben worden?
- ☐ Stellt die Dokumentation eines entwickelten Hard-/Softwaresystems bzw. eine Bedienungsanleitung höchstens ein Nebenprodukt der Arbeit dar und nimmt einen entsprechend geringen Anteil ein?
- ☐ Wird Quellcode (außer im Anhang) lediglich angemessen, d. h. beispielsweise zur Verdeutlichung von zentralen Algorithmen eingesetzt?
- ☐ Haben alle in der Arbeit (außer im Anhang) dargestellten Diagramme einen klaren Zweck bezüglich der Nachvollziehbarkeit der Ausführungen?
- ☐ Ist die Arbeit durchgängig nachvollziehbar und objektiv und kommt zur Begründung der zentralen Aussagen ohne unbelegte persönliche Meinung der Autorin oder des Autors aus?
- ☐ Stützt sich die Arbeit auf ein angemessenen Maß an Fachliteratur?
- ☐ Werden alle Quellen konsistent und ausreichend ausführlich zitiert?

Themenvorschläge für W-Seminare

„In Informatik habe ich einfach das Problem, dass ich keine geeigneten Themen für ein W-Seminar finde. Dieses Problem habe ich in meinem anderen Fach nicht.“

Die Konzeption und Themenfindung eines W-Seminars gestaltet sich oft schwierig. Deshalb bieten wir im Folgenden eine Auswahl an Rahmenthemen für W-Seminare an. Neben einer kurzen Motivation geben wir einen Überblick über das jeweilige Fachgebiet sowie Hinweise auf Literatur zum jeweiligen Rahmenthema. Um es Ihnen zu erleichtern, ein solches W-Seminar anzubieten, stellen wir außerdem einige Themen für W-Seminararbeiten (samt Literaturhinweisen) bereit. Abschließend beinhaltet jeder Abschnitt auch eine Übersicht über die Voraussetzungen, die die Schülerinnen und Schüler bei der Wahl des jeweiligen W-Seminars beachten sollten.

Auf den folgenden Seiten finden Sie zu jedem Rahmenthema jeweils fünf Themenvorschläge für Seminararbeiten von Schülerinnen und Schülern. **Eine vollständige Themenliste**, weitere Ideen und Anregungen finden Sie auf unserer Website https://www.lehramt-informatik.de/w-seminare.

Die hier angeführten Themenlisten sollen dabei nicht als erschöpfende Auflistungen verstanden werden, sondern eher als beispielhafte Vorschläge, die natürlich modifiziert, erweitert und ergänzt werden können und sollen. Um eine hohe Qualität bei Seminararbeiten zu ermöglichen, wurde bei den Themenvorschlägen versucht, folgende Kriterien zu erfüllen:

Das Thema muss einen klaren Eigenanteil ermöglichen und einfordern (z. B. Simulation, Implementierung, Evaluation, Modellierung, Vergleich, Umfrage).

Die Arbeit darf nicht nur deskriptiver Natur sein, ansonsten läuft sie Gefahr, eine reine Wissenswiedergabe zu werden. Eine solche wäre beispielsweise als Referatsthema durchaus akzeptabel, sollte aber nicht das zentrale Ziel einer wissenschaftsorientierten Arbeit darstellen.

Eine Verortung in der Fachwissenschaft muss bereits aus dem Thema hervorgehen, um sicherzustellen, dass die dazu entstehende Arbeit entsprechend kontextualisiert werden kann.

Durch eine angemessene Wahl und Formulierung der Seminararbeitsthemen kann typischen Problemen und Schwierigkeiten bereits im Vorfeld vorgebeugt werden.

Rahmenthema: **Datenanalyse und Big Data**

Big Data und die sich hierdurch bietenden Möglichkeiten der Datenanalyse haben einen immer größeren Einfluss auf unsere Gesellschaft und unser alltägliches Leben. Durch die Speicherung und Analyse großer Datenmengen kann oftmals ein großer Mehrwert für den Nutzer entstehen, wie zum Beispiel:

- Taxis können schon vorab zu stark frequentierten Orten gesendet werden.
- Google Flu Trends prognostiziert Grippewellen oftmals genauer und wesentlich schneller als herkömmliche Vorhersagen.
- Betrugsversuche mit Kreditkarten können wesentlich besser als traditionell verhindert werden.

Allerdings muss unterschieden werden zwischen für den Nutzer offensichtlichen Datenerfassungen und -auswertungen (wie z. B. SmartWatches) und für den Nutzer verborgenen (wie z. B. Sensorik von Smartphones). Für eine fundierte Meinungsbildung und einen mündigen Umgang mit diesen Möglichkeiten müssen daher beide Sichtweisen betrachtet werden.

In diesem Seminar sollen Potenziale, Grenzen und Risiken von großen und vielfältigen Datensammlungen betrachtet werden. Dabei soll ein tieferer Einblick hinter die Bedeutung der unter dem Buzzword *„Big Data“* zusammengefassten Entwicklungen gewonnen werden. Während im allgemeinen Sprachgebrauch unter *Big Data* lediglich ein „großer Haufen Daten“ verstanden wird, sind diese Datenmengen weiterhin – neben der Quantität – auch durch unterschiedliche Strukturierung sowie die immer schnellere Erzeugung und Verarbeitung gekennzeichnet. Dies stellt eine große Herausforderung für die Auswertung dar. Insgesamt hat sich das Vorgehen geändert: Anstatt konkrete Datensätze für spezielle Analysen zu erheben, gilt es aus einem riesigen und stetig wachsenden Datenpool (der unabhängig vom Analysezweck „einfach so“ erhoben wird) Informationen zu gewinnen. Der Begriff *Data Mining* beschreibt hierbei das Prinzip des „Schürfens“ nach wertvollen Informationen in einem solchen großen Datenberg (in Analogie zum Bergbau).

Literatur:

- Mayer-Schönberger, V. (2013). *Big Data: die Revolution, die unser Leben verändern wird*. München: Redline.
- Cleve, J. & Lämmel, U. (2016). *Data Mining*. Berlin: De Gruyter Oldenbourg.

Mögliche Themen für die Seminararbeiten

1. **Entwicklung und Auswertung eines Fitnesstrackers: Was finden wir über den Träger heraus?**
   Martini, M. (2015). Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz. In *Die digitale Lebenswelt gestalten* (S. 97-162). Baden-Baden: Nomos Verlagsgesellschaft.

2. **Für welche Anwendungen eignen sich SQL- bzw. NoSQL-Datenbanken besser? Wir vergleichen deren Performance.**
   Meier, A., Kaufmann, M. & Kaufmann, M. (2016). *SQL-& NoSQL-Datenbanken.* Berlin: Springer.

3. **Taxifahrten in New York: Welche Informationen ergeben sich aus der öffentlichen Datenbank? Methoden und Grenzen von Big-Data-Auswertungen am praktischen Beispiel.**
   Barnickel, N. & Klessmann, J. (2012). Open Data-Am Beispiel von Informationen des öffentlichen Sektors. In *Open Initiatives: Offenheit in der digitalen Welt und Wissenschaft* (S. 127-158). Saarbrücken: universaar.

4. **Simulation einer Smart City: Welche Daten können gewonnen werden und was finden wir über die Bewohner heraus?**
   Martini, M. (2015). Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz. In *Die digitale Lebenswelt gestalten* (S. 97-162). Baden-Baden: Nomos Verlagsgesellschaft.

5. **Predictive Policing: Was verraten uns die Daten der Polizei in Los Angeles (oder San Francisco) über Kriminalitätsschwerpunkte und deren zeitliche Abhängigkeit?**
   Rolfes, M. (2017). Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit. *Geoinformation & Visualisierung* (S. 51-76).

Voraussetzungen

Was **muss** ich mitbringen?

- Interesse am Fach und Neugier, neue Inhalte zu lernen
- Motivation, sich selbstständig in ein Fachgebiet einzuarbeiten um Erkenntnisse zu erlangen

Was muss ich **nicht** (zwingend) mitbringen?

- Programmierkenntnisse

Rahmenthema: **IT-Sicherheit**

Heutzutage umgeben uns IT-Systeme in immer mehr Lebensbereichen. Auch sicherheitskritische Aufgaben werden immer häufiger durch solche Systeme übernommen. Das gilt für die Gesellschaft als Ganzes (digitale Währungen, Verwaltung personenbezogener Daten oder Unternehmensgeheimnissen) genauso wie für das einzelne Individuum (Online-Banking, E-Mail-Kommunikation). Hier stellt sich die Frage der Sicherheit solcher Systeme:

- Ist mein WLAN wirklich „gesichert“?
- Wie sicher ist Online-Banking?
- Wie funktionieren Krypto-Währungen?

Das Feld der IT-Sicherheit umfasst Planungen, Maßnahmen und Kontrollen, mit deren Hilfe die Vertraulichkeit von Informationen sowie deren Integrität und Verfügbarkeit sichergestellt werden sollen. Damit ist jedoch nicht nur der reine Schutz von Informationen selbst gemeint, sondern auch von allen Systemen, deren Aufgabe es ist, Informationen zu verarbeiten, zu nutzen und zu speichern. Das Fachgebiet umfasst viele unterschiedliche Aspekte: Von der Funktionsweise von Krypto-Währungen wie Bitcoin über die Analyse von Kommunikationsdaten von Smartphones, bis hin zu sozialen Elementen wie Phishing.

Literatur:

- Mitnick, K., Vamosi, R. & Gößwein, E. (2018). *Die Kunst der Anonymität im Internet : so schützen Sie Ihre Identität und Ihre Daten*. Frechen: mitp.
- Eckert, C. (2013). *IT-Sicherheit: Konzepte-Verfahren-Protokolle*. Berlin: De Gruyter Oldenbourg.

Mögliche Themen für die Seminararbeiten

1. **Ein Spaziergang durch die Stadt: Empirische Untersuchung von IT-Sicherheit in der Umgebung.**
   Detken, K. O. & Eren, E. (2006). WLAN-Sicherheit–von WEP bis CCMP. *D* A* CH Security*, Klagenfurt (S. 187-201).
   Detken, K. O. & Eren, E. (2006). Bluetooth-Sicherheit–Schwachstellen und potenzielle Angriffe. *DACH Mobility* (S. 173-186).

2. **Wozu muss eine Taschenlampen-App eigentlich mein Adressbuch lesen? Analyse der Nutzerwahrnehmungen von Permissions bei der App-Installation.**
   Brummund, A. (2014). Smartphones und Apps: Datenschutzrechtliche Risiken und deren Begrenzung. In *GI-Jahrestagung* (S. 539-550).

3. **Wenn afrikanische Prinzen dir Geld schenken wollen: Eine experimentelle Überprüfung von Methoden zum Erkennen von Phishing-Angriffen.**
   Stockhardt, S., Reinheimer, B. & Volkamer, M. (2015). Über die Wirksamkeit von Anti -Phishing-Training. *Mensch und Computer 2015–Workshopband*.

4. **Morgen bin ich reich? Konzeption und Entwicklung einer eigenen Kryptowährung.**
   Buhl, H., Schweizer, A. & Urbach, N. (2007). Blockchain-Technologie als Schlüssel für die Zukunft?.

5. **Welche Meta-Daten werden von „Smart Home“ Produkten über Bewohner erfasst und inwiefern kann die Auswertung dieser Daten die Privatsphäre der Bewohner verletzen?**
   Lankau, R. (2015). Fragen Sie Alexa. Die Entmündigung des Individuums durch die Vermessung der Welt. In *Zur Aktualität der Kritischen Theorie für die Pädagogik* (S. 277-297). Wiesbaden: Springer.

Voraussetzungen

Was **muss** ich mitbringen?

- Interesse am Fach und Neugier, neue Inhalte zu lernen
- Motivation, sich selbstständig in ein Fachgebiet einzuarbeiten

Was muss ich **nicht** (zwingend) mitbringen?

- Programmierkenntnisse
- Vorkenntnisse im „Hacken“ von Computern und Smartphones

Rahmenthema: **Kryptographie**

„9 3 8 12 9 5 2 5 9 14 6 15“

Kannst du diesen Code knacken? Dann bist du hier genau richtig (aber auch sonst)! Verschlüsselte Kommunikation ist für unsere moderne Gesellschaft unabdingbar. Oder würdest du dich trauen deine Bankdaten beim Online-Banking unverschlüsselt zu senden? Seit 2016 sendet selbst WhatsApp alle Nachrichten „Ende-zu-Ende-verschlüsselt“. In diesem Kontext stellen sich viele Fragen:

- Können meine WhatsApp-Nachrichten mitgelesen werden?
- Was ist eine Krypto-Währung?
- Gibt es „unbrechbare“ Verschlüsselungsverfahren?
- Warum wird heute nicht grundsätzlich alles automatisch verschlüsselt?
- (Wie) Kann ein Verschlüsselungsschlüssel über einen unsicheren Kommunikationskanal sicher übertragen werden?

Die Idee von Verschlüsselung zum sicheren Nachrichtenaustausch ist dabei keineswegs neu: 1900 v. Chr. wurden bereits ägyptische Hieroglyphen verwendet, die auf Verschlüsselung von Nachrichten hinweisen, 50-60 v. Chr. verwendete Julius Cäsar die nach ihm benannte Cäsar-Chiffre, bei der jeder Buchstabe durch den Buchstaben drei Positionen später im Alphabet ersetzt wurde, und während des 2. Weltkrieges wurde die deutsche Enigma-Maschine lange für nicht entschlüsselbar gehalten. All solche sogenannten symmetrischen Verschlüsselungsverfahren haben das Problem, dass neben dem verschlüsselten Text auch der Schlüssel selbst mit übertragen werden muss. Um heutzutage einen sicheren Schlüsselaustausch über eine unsichere Verbindung zu ermöglichen, werden zunehmend asymmetrische Verfahren eingesetzt. Als Gegenstück zur Verschlüsselung beschäftigt sich die Kryptoanalyse mit dem „Brechen“ solcher Verfahren.

Literatur:

- Beutelspacher, A. (2005). *Kryptologie: eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen.* Wiesbaden: Vieweg.
- Stallings, W. (2014). *Cryptography and network security*: principles and practice. Boston: Pearson.

Mögliche Themen für die Seminararbeiten

1. **Entwicklung eines eigenen Verschlüsselungsverfahrens und Vergleich mit existierenden Verfahren.**
   Miller, M. (2013). *Symmetrische Verschlüsselungsverfahren: Design, Entwicklung und Kryptoanalyse klassischer und moderner Chiffren*. Wiesbaden: Vieweg.
   Beutelspacher, A., Neumann, H. & Schwarzpaul, T. (2010). *Kryptografie in Theorie und Praxis Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld.* Wiesbaden: Vieweg.

2. **Konzeption und Entwicklung eines eigenen Protokolls zur sicheren Kommunikation am Beispiel „Stein, Schere, Papier“ zwischen drei Spielern.**
   Beutelspacher, A., Schwenk, J. & Wolfenstetter. (2015). *Moderne Verfahren der Kryptographie: von RSA zu Zero-Knowledge*. Wiesbaden: Springer.

3. **Wie gut ist mein Facebook-Passwort? Eine Analyse von Strategien zum „Knacken“ von Passwörtern und experimenteller Vergleich von Passwörtern und -stärken.**
   Florencio, D. & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (S. 657-666). ACM.

4. **Brainwallets: Eine Sicherheitsanalyse.**
   Vasek, M., Bonneau, J., Ryan Castellucci, C. K. & Moore, T. (2016). The Bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets. *Financial Cryptography and Data Security, Lecture Notes in Computer Science.* Springer.

5. **Entwicklung einer eigenen Codierung und Vergleich mit existierenden Systemen (Barcode, QR-Code).**
   Witt, K. U. (2005). *Algebraische Grundlagen der Informatik: Strukturen, Zahlen, Verschlüsselung, Codierung*. Wiesbaden: Vieweg.

Voraussetzungen

Was **muss** ich mitbringen?

- Interesse am Fach und Neugier, neue Inhalte zu lernen
- Keine Abneigung gegenüber der Mathematik

Was muss ich **nicht** (zwingend) mitbringen?

- Programmierkenntnisse
- Vorkenntnisse im Knacken von Passwörtern, „Hacken“, o. ä.

Rahmenthema: **Human Computer Interaction**

Grafische Benutzeroberflächen sind der erste Kontaktpunkt mit Informatiksystemen. Wie wichtig ein gutes und durchdachtes Design ist, zeigte beispielsweise der Reaktorunfall im Kernkraftwerk Three Mile Island in den USA 1979. Dieser Unfall konnte laut Ermittlungen zumindest teilweise auf die unintuitive grafische Benutzeroberfläche zurückgeführt werden.

Seitdem hat sich viel getan und die die Interaktion mit Informatiksystemen hat sich stetig weiterentwickelt. Seit 2007 hat mit der zunehmenden Verbreitung von Smartphones die Touchbedienung zur Interaktion von Mensch und Computer immer größere Bedeutung. Gleichzeitig steht heutzutage steht in vielen Haushalten bereits ein virtueller persönlicher Assistent („Smart Speaker“) wie Amazon Echo, Google Home oder der Homepod von Apple, mit denen wir via Spracheingabe kommunizieren. Die Interaktion mit Computern prägt unseren Alltag im „digitalen Zeitalter“ immer mehr, sodass sich spannende Fragen eröffnen:

- Kann ein Computer uns vorgaukeln, ein Mensch zu sein?
- Warum ändern Anwendungen regelmäßig ihre Icons? Warum werden Icons überhaupt re-designed?
- Wie bedienen wir Computer in 10 Jahren? Wie lange brauchen wir Maus und Tastatur noch?

Das Fachgebiet der Interaktion von Mensch und Computer („human-computer interaction“) beschäftigt sich mit der Verwendung und dem Design von Technologien an der Schnittstelle zwischen Anwendern und Maschinen. Besonders das Spannungsfeld aus Mensch, Maschine und Design ist dabei von großem Interesse für Forscher auf diesem Gebiet. Human-Computer-Interaction ist stark interdisziplinär ausgelegt: Das Fachgebiet ist zwischen der Informatik, Verhaltenswissenschaften, Design, Medienwissenschaften, Psychologie und anderen Fachgebieten angesiedelt.

Literatur:

- Shneiderman, B. (2010). *Designing the user interface: strategies for effective human-computer interaction*. Boston: Pearson.
- Heinecke, A. M. (2011). *Mensch-Computer-Interaktion: Basiswissen für Entwickler und Gestalter*. Berlin: Springer.

Mögliche Themen für die Seminararbeiten

1. **Aspekte der Gestaltung der Mensch-Maschine-Schnittstelle: Untersuchungen, die verschiedene Arten der Interaktion (Sprachsteuerung, Touch, Tastatur/Maus) miteinander vergleichen.**
   Sears, A. & Shneiderman, B. (1991). High precision touchscreens: design strategies and comparisons with a mouse. *International Journal of Man-Machine Studies*, *34*(4) (S. 593-613).
2. **Eine qualitative Analyse von Benutzeroberflächen: Warum werden manche Menüs intuitiver wahrgenommen als andere?**
   Müller, R. (2010). *Ermittlung intuitiver user interfaces zur Visualisierung einer Zeitreise* (Diplomarbeit, Koblenz, Universität Koblenz-Landau, Campus Koblenz).
3. **Ikonographie: Welche Icons vermitteln ihre Funktion durch ihr Design, welche nicht? Eine empirische Analyse.**
   Müller, R. (2010). *Ermittlung intuitiver user interfaces zur Visualisierung einer Zeitreise* (Diplomarbeit, Koblenz, Universität Koblenz-Landau, Campus Koblenz).
4. **Wie kann die Immersion in Virtual-Reality-Anwendungen gesteigert werden? Eine qualitative Untersuchung.**
   Dörner, R., Broll, W., Grimm, P. & Jung, B. (Hsg.). (2013). *Virtual und augmented reality (VR/AR): Grundlagen und Methoden der Virtuellen und Augmentierten Realität*. Berlin: Springer.
5. **Empirische Analyse von ausgewählten Science-Fiction-Filmen: Wie werden Computer in futuristischen Filmen bedient?**
   Sears, A. & Shneiderman, B. (1991). High precision touchscreens: design strategies and comparisons with a mouse. *International Journal of Man-Machine Studies*, *34*(4) (S. 593-613).

Voraussetzungen

Was **muss** ich mitbringen?

- Interesse am Fach und Neugier, neue Inhalte zu lernen
- Interesse daran, die Interaktion zwischen Mensch und Maschine zu hinterfragen und zu erforschen

Was muss ich **nicht** (zwingend) mitbringen?

- Programmierkenntnisse
- Vorkenntnisse im Grafikdesign

Rahmenthema: **Mein digitaler Fußabdruck**

Laut einer Studie von 2013 können aus digitalen Aufzeichnungen, wie *likes* auf Facebook, individuelle Eigenschaften und Einstellungen von Menschen abgeleitet werden. In der Studie konnten ausgehend von den Facebook-Profilen von Nutzern sehr persönliche Dinge mit hoher Wahrscheinlichkeit vorhergesagt werden – etwa Religion, Sexualität und Drogengebrauch. Forscher sind der Meinung, dass das Erstellen solcher Persönlichkeitsprofile auch aus allen möglichen anderen alltäglich anfallenden Daten denkbar ist[1]. Allerdings sind solche Auswertungen nicht nur auf bewusst hinterlassene Informationen (wie *likes* aus Facebook) beschränkt, sondern können beispielsweise auch auf Daten, die andauernd und im Hintergrund erfasst werden, wie GPS-Daten des Smartphones oder besuchte Websites im Internet, basieren. Diese Tatsache wirft gewisse Fragen auf:

- Welche Spuren – bewusst oder unbewusst – hinterlasse ich in der digitalen Welt?
- (Wie) Kann ich meine Privatsphäre und Anonymität wahren?
- Wie speichere ich eigene Daten dauerhaft und sicher?

Mit solchen und anderen Fragestellungen setzt sich dieses Seminar auseinander. Dabei werden zentrale Themen aus diesem Bereich wie Datenschutz und Datensicherheit thematisiert. Das Ziel ist dabei, Daten vor Manipulation und Missbrauch (wie z. B. unerlaubtem Zugriff, Verbreitung, Verfälschung) zu schützen. Für diesen Schutz sind verschiedene Aspekte zentral, etwa die physische Sicherheit der Daten (d. h. Vermeidung unerlaubtem Zugangs zu unseren Datenspeichern) und technische Maßnahmen (wie geeignete Backups, Verschlüsselung von Kommunikation oder Firewalls) gewährleistet werden. Solche und andere Konzepte tragen auch zu der für viele Menschen zunehmend schwerer werdenden Herausforderung bei, im Zeitalter der Vernetzung und der digitalen Spuren Persönlichkeitsrecht und Privatsphäre zu wahren.

Literatur:

- Petrlic, R. & Sorge, C. (2017). *Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*. Wiesbaden: Vieweg.
- Lenhard, T. (2017). *Datensicherheit : Technische und organisatorische Schutzmaßnahmen gegen Datenverlust und Computerkriminalität*. Wiesbaden: Vieweg.

1 https://netzpolitik.org/2013/du-bist-was-du-magst-aus-facebook-likes-lassen-sich-religion-sexualitat-und-drogengebrauch-vorhersagen/

Mögliche Themen für die Seminararbeiten

1. **Wie kann mich eine Website identifizieren und welche Analyseverfahren werden dazu eingesetzt? Eine empirische Analyse.**
   Pieronczyk, T. (2012). Device Fingerprinting mit dem Web-Browser. *Innovative Internet Technologies and Mobile Communications (IITM), and Aerospace Networks (AN)*, *23*.

2. **Wie wichtig ist Jugendlichen Privatsphäre im Internet?**
   Schaar, P. (2007). *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft*. München: Bertelsmann.
   Pfitzmann, A. & Steinbrecher, S. (2003). Digitale Glaubwürdigkeit und Privatsphäre in einer vernetzten Gesellschaft. *Klumpp, Dieter/Kubicek, Herbert/Rossnagel, Alexander: Next Generation Information Society*.

3. **Wie viel Prozent einer Website sind eigentlich Werbung? Eine empirische Auswertung.**
   Weiss, S. (2010). *Werbung im Web: der Stellenwert der klassischen Online-Werbung in der Werbekommunikation* (Dissertation, Münster (Westfalen), 2010).

4. **Welche Daten in meinem Netzwerk werden unverschlüsselt übertragen?**
   Alexander, M. (2006). *Netzwerke und Netzwerksicherheit : das Lehrbuch*. Heidelberg: Hüthig.

5. **Welche Backupstrategien werden im Alltag und im Unternehmen genutzt?**
   Wald, E. (2002). *Backup & disaster recovery*. Bonn: Mitp.

Voraussetzungen

Was **muss** ich mitbringen?

- Interesse am Fach und Neugier, neue Inhalte zu lernen

Was muss ich **nicht** (zwingend) mitbringen?

- Programmierkenntnisse
- Vorkenntnisse im „Hacken“

Rahmenthema: **Mustererkennung**

Am 1.8.2017 startete am Bahnhof „Südkreuz“ in Berlin ein Testlauf für Videoüberwachung mit automatischer Bewegungsmuster- und Gesichtserkennung. Die Kameras sollen dabei herrenloses Gepäck, das längere Zeit nicht bewegt wird, sowie typische Verhaltensmuster von Taschendieben und Menschen, die beispielsweise auf einer Fahndungsliste stehen, erkennen.[1]

Diese Technologie basiert auf der automatischen Erkennung von gewissen Mustern. Allgemein ist Mustererkennung heute sehr präsent und findet sogar schon auf unseren Smartphones statt, wenn diese selbstständig die Gesichter unserer Freunde auf Fotos erkennen und den korrekten Namen zuordnen. Damit eröffnet Mustererkennung einige spannende Fragestellungen:

- Was sind die Muster auf die ein solches System reagiert?
- Wie erkennt unser Gehirn Gesichter? Und wie funktioniert das am Computer?
- Was hat die Komprimierung von Bildern, Musik und Text mit Mustererkennung zu tun?

Typische Anwendungsbeispiele sind Gesichts- und Bewegungserkennung, Texterkennung oder Spracherkennung. Als Mustererkennung im Allgemeinen bezeichnet man die Identifikation von Regelmäßigkeiten, Gesetzmäßigkeiten oder sonstigen Ähnlichkeiten in einer Datenmenge. In der Informatik können wir durch das Erkennen solcher Muster Vorhersagen treffen, Regeln aufstellen und allgemeinere Probleme lösen.

Literatur:

- Theodoridis, S. & Koutroumbas, K. (1999). *Pattern recognition*. Amsterdam: Elsevier.
- Murty, M. N. & Devi, V. S. (2015). *Introduction to pattern recognition and machine learning*. New Jersey: IISc Press.

1 https://netzpolitik.org/2017/ortstermin-am-suedkreuz-die-automatische-gesichtserkennung-beginnt/

Mögliche Themen für die Seminararbeiten

1. **Komprimierung: Analytischer Vergleich verschiedener Verfahren und Konzeption und Implementierung eines eigenen Kompressionsalgorithmus.**
   Schulz, R. H. (2013). *Codierungstheorie: Eine Einführung.* Berlin: Springer.

2. **Woran erkenne ich manipulierte und „gephotoshoppte" Bilder? Eine experimentelle Untersuchung.**
   Büllesbach, A. (2008). *Digitale Bildmanipulation und Ethik. Aktuelle Tendenzen im Fotojournalismus*. Köln: Herbert von Halem-Verlag.

3. **OCR: Implementierung eines Programms zur Erkennung von Schriftzeichen in Bildern.**
   Vorbach, P. (2014). Analysen und Heuristiken zur Verbesserung von OCR-Ergebnissen bei Frakturtexten.
   Wu, V., Manmatha, R. & Riseman, E. M. (1997). Finding text in images. In *ACM DL'97*(S. 3-12).

4. **Wie erkennt Instagram Gesichter? Konzeption und Implementierung eines eines eigenen Gesichtserkennungsverfahrens.**
   Kopf, S. & Oertel, A. (2005). Gesichtserkennung in Bildern und Videos mit Hilfe von Eigenfaces.
   Hjelmås, E. & Low, B. K. (2001). Face detection: A survey. *Computer vision and image understanding*, 83(3) (S. 236-274).

5. **Einer aus 80 Millionen: Wie leicht ist mein Browser identifizierbar? Eine Auswertung.**
   Mulazzani, M., Reschl, P., Huber, M., Leithner, M., Schrittwieser, S., Weippl, E. & Wien, F. C. (2013). Fast and reliable browser identification with javascript engine fingerprinting. In *Web 2.0 Workshop on Security and Privacy*.

Voraussetzungen

Was **muss** ich mitbringen?

- Grundlegende Programmierkenntnisse
- Hohes Maß an Eigeninitiative und Eigenverantwortung

Was muss ich **nicht** (zwingend) mitbringen?

- Erfahrung mit Bilderverarbeitungssoftware

Notizen

Impressum

Herausgeber:
Professur für Didaktik der Informatik
Friedrich-Alexander-Universität Erlangen-Nürnberg
Martensstraße 3
91058 Erlangen

Redaktion und Gestaltung:
Sven Jatzlau, Tilman Michaeli

Auflage:
500 Stück

www.lehramt-informatik.de/w-seminare