ACADEMIC GRADUATION MONITORING REPORT

2024

European Association for Biometrics (EAB)

version: 2025-09-19

Email: secretariat@eab.org

RESEARCH MONITOR CONTENT

PREFACE

The European Association for Biometrics (EAB) has composed this academic graduation monitoring report, which should provide information about academic theses that are completed in EAB member institutions. Such report should contain lists of entries of Bachelor-, Master- or PhD-theses and a short summary of each thesis. EAB is proud to provide an overview of the research going on in Europe. If you are member of EAB and you can contribute information about your graduated students. In order to facilitate the data collection, a webform, accessible to EAB members, has been added to the EAB website, in which author and contact information can be provided as well as a title, and abstract and an optional link to the report. The webform can be found here: https://eab.org/information/academic_report.html This report was composed by the EAB for its members. If you are not EAB member yet – please join and share the non-profit spirit of EAB. We are grateful for your continuous support of the EAB initiatives through your membership.

MONITOR
PHD-THESES

JANNIS PRIESNITZ - SECURE CONTACTLESS FINGERPRINT RECOGNITION

Full Title: Secure Contactless Fingerprint Recognition
Institution: Hochschule Darmstadt
Supervisor: Christoph Busch and Christian Rathgeb
URL: https://opus4.kobv.de/opus4-h-da/frontdoor/deliver/index/docId/536/file/Thesis_Jannis_Priesnitz__print.pdf
Contact email: christoph.busch@h-da.de

Abstract:
Fingerprints, i.e. ridge and valley patterns on the tip of a human finger, are one of the most important biometric characteristics due to their known uniqueness and persistence properties. Large-scale fingerprint recognition systems are not only used worldwide by law enforcement and forensic agencies, they are also deployed in the mobile market and in nationwide applications. In recent years, contactless fingerprint recognition has become a viable alternative to established contact-based methods. The contactless capturing process avoids distinct problems, e.g. signal of low contrast caused by dirt or humidity and left-over latent fingerprints on the capture surface. Moreover, contactless schemes provide a faster and more hygienic as well as a more convenient capturing process and hence have a higher user acceptance. However, contactless fingerprint recognition introduces new challenges. Environmental influences such as an uncontrolled background and varying illumination and an unconstrained finger positioning are especially a challenge for mobile recognition schemes. This Thesis contributes to an efficient and secure mobile contactless fingerprint recognition process. The work addresses various vital aspects along the contactless fingerprint recognition pipeline. The mobile, automatic capturing, segmentation and pre-processing of contactless fingerprint samples represents a central focus of this Thesis. Furthermore, contributions to the topics of quality assessment, feature extraction and presentation attack detection are conducted. To enable new research directions, such as training deep learning-based algorithms, a generator for synthetic mobile contactless fingerprint samples is also suggested. The results proposed in this Thesis show improvements on several components of the recognition method which contribute to an increased biometric performance, security and comfort level. Moreover, challenges and limitations are discussed.

JEREMY SPETH - REMOTE PHYSIOLOGICAL MEASUREMENT IN AN OPEN WORLD

Full Title: Remote Physiological Measurement in an Open World
Institution: University of Notre Dame
Supervisor: Adam Czajka and Patrick Flynn
URL:
https://curate.nd.edu/articles/thesis/Remote_Physiological_Measurement_in_an_Open_World/24884337?file=43780902
Contact email: aczajka@nd.edu

Abstract:
Many life-sustaining vital signs can be measured optically using a camera. Of particular interest is remote photoplethysmography (rPPG), a technique for non-contact blood volume pulse estimation from video. This presents a unique opportunity for monitoring health at a global scale using accessible consumer devices such as mobile phones. Yet, estimating these signals outside of controlled laboratory settings is still an unsolved and challenging problem. This dissertation proposes new data-driven methods to accurately estimate vital signs from video. We collected multiple video datasets of subjects moving and talking with simultaneous physiological ground truth to train and validate rPPG. After finding the immense promise of deep learning for remote vitals estimation, we reveal neural network's susceptibility to adversarial attacks and ``hallucination'' when anomalies occur. Next, we explore the unique property of camera-based systems to perform spatial measurements. By examining the pulse wave's time lags between different peripheral sites on the body (e.g. hands, face, arms, and legs), we show that rPPG can be used to estimate the pulse transit time. Given the challenges of collecting diverse video datasets with ground truth, we implemented a new non-contrastive unsupervised method for training artificial neural networks to learn rPPG from video without labels. We find that this framework is effective with very little video, enabling personalized and adaptive models for camera-based physiological measurement. Lastly, we show that the proposed framework is general enough for any type of band-limited periodic signal by applying it to remote respiration estimation.

MATEJ VITEK - LIGHT-WEIGHT DEEP MODELS FOR SCLERA RECOGNITION

Full Title: Light-weight deep models for sclera recognition
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Vitomir Štruc
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=158640&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
Sclera recognition is a subfield within biometric recognition technology that focuses on identifying individuals based on the vascular structures in the sclera, i.e. the white part of the eye. Most existing solutions for sclera recognition are based either on hand-crafted methods from the field of computer vision, which perform suboptimally, or on deep convolutional networks, which require powerful hardware to run efficiently. However, biometric systems are increasingly being deployed on smartphones, head-mounted displays, and edge devices, which require light-weight models, i.e. simple computational models capable of running well on weaker hardware. As such, in our thesis (i) we propose the novel method IPAD, which decreases the number of parameters and operations in a deep network, and using IPAD we develop a light-weight model for sclera segmentation, and (ii) we develop the light-weight GazeNet network, based on the SqueezeNet architecture and trained via multi-task learning, which we use as our sclera vessel feature extractor. The results of our extensive experimental analysis affirm the superiority of deep convolutional networks over classical hand-crafted methods. On the other hand, our analysis of the models developed with the IPAD method demonstrates that the networks commonly relied on in the literature can be significantly reduced in terms of their spatial and computational requirements, without a significant decrease in accuracy -- in fact, in certain cases, simplifying the models even enhances their accuracy. Even light-weight deep networks require a significant amount of training data to achieve high-quality performance. We note that, while iris datasets are plentiful, there is a considerable lack of sclera-focused datasets. Thus, as part of the aforementioned contributions, we introduce MOBIUS, the first publicly available mobile-camera-acquired dataset intended primarily for sclera segmentation, although it can be used for iris and periocular biometrics as well. Finally, since biometric systems have been shown to exhibit bias in various biometric fields, we (iii) propose a novel methodology for bias evaluation based on two novel metrics: FSD and CGD. Using the proposed methodology, we study the bias of contemporary sclera segmentation solutions and show that even in sclera biometrics a certain amount of demographic bias is present in existing solutions.

DAILÉ OSORIO-ROIG - PRIVACY PRESERVING WORKLOAD REDUCTION

Full Title: Privacy Preserving Workload Reduction in Biometric Systems
Institution: Hochschule Darmstadt
Supervisor: Christoph Busch and Christian Rathgeb
URL: https://opus4.kobv.de/opus4-h-da/frontdoor/index/index/docId/469
Contact email: christoph.busch@h-da.de

Abstract:
The development of large-scale biometric identification systems that provide privacy protection of the enrolled subjects is an ongoing concern. Most importantly, biometric technologies demand interoperability and deployment assuring maximum usability by including multi-modal biometric solutions. In the context of privacy protection, several Biometric Template Protection (BTP) schemes have been proposed in the past. However, these schemes appear to be unsuitable for indexing (Workload Reduction (WR)) in biometric identification systems. As a consequence, they have been utilised in biometric identification systems performing exhaustive searches (i. e. one-to-many search), which represent a time-consuming task and, hence, a high computational workload dominated by the number of comparisons. Additionally, novel privacy protection schemes have recently been developed in the literature. These approaches appear promising, but have not yet been evaluated in a detailed way, especially in terms of their privacy protection capabilities. Motivated by the acceleration of large-scale protected biometric database searches and the investigation for privacy enhancement, this thesis investigates in more detail indexing schemes operating on protected templates for different biometric characteristics, as well as some limitations in privacy protection. Extensive experimental evaluations demonstrate that novel BTP-agnostic and biometric characteristic (BC)-agnostic indexing schemes can successfully reduce the computational workload of a biometric system, while preserving biometric security and performance. Novel attacks have also been proposed in the context of privacy protection.

JAG MOHAN SINGH - 3D FACE MORPHING DETECTION

Full Title: Robust algorithms for 2D and 3D Face Morphing Attacks: Generation and Detection
Institution: Norwegian University of Science and Technology (NTNU)
Supervisor: Prof. Raghavendra Ramachandra
URL: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3130206
Contact email: raghavendra.ramachandra@ntnu.no

Abstract:
Biometric Authentication (Biometrics) is a powerful tool that authenticates individuals using digital means, which includes biological or behavioral characteristics. Biometrics harnesses biological features such as fingerprints, face, hand geometry, speech, iris, and fingerphoto. Face and finger modalities have generated the interest of biometric researchers thanks to their ease of use and high accuracy. Face biometric modality, in particular, is easy to use as it can be acquired passively. Furthermore, Face Recognition Systems (FRS) excel in real-world environments, thanks to the advancements in deep learning. However, it's important to know that FRS are not immune to attacks. They are vulnerable to various types of attacks, including presentation attacks and morphing attacks to a large extent and deepfakes to a smaller extent. This thesis focuses on Face Morphing Attacks (FMA), an active area of research in Biometrics. An FMA can be generated by linearly blending facial images in the color domain from two contributory data subjects. FMA has shown vulnerabilities in FRS when evaluated automatically by software or manually by human observers. Thus, FMA is a strong attack on FRS. Hence, detecting FMA is an actual problem from a security standpoint. Most FMA systems currently use full facial images from the two contributory data subjects. However, the part-based face morphing/compositing problem has received little attention, i.e., using facial parts from the two contributory data subjects to generate an FMA. Further, due to Generative Adversarial Networks (GANs), generating full photo-real synthetic faces or completing partial facial images is possible due to deep learning-based image synthesis advances. Thus, part-based facial morphing using the advances of deep learning could be a fruitful area of research. Motivated by the challenges arising from attacks toward FRS, the thesis focus is two-fold. The first is to increase the attack strength by generating higher quality attacks and the second is to advance the mitigation measures, a.k.a countermeasures for the generated attacks. We focus on Morphing Attacks, which include generation and detection, known as Morphing Attack Detection (MAD). Further, evaluating vulnerabilities imposed by part-based facial morphing could be a novel area of research and we have performed an extensive assessment of this nascent area. Currently, the critical problem is performing robust MAD in real-world environments, which have the challenges of facial pose, expression, illumination, image quality, print-scan variations and image capture distance. This brings us to building robust classifiers for the facial morphing problem. Morphing has been evaluated on face images, i.e., 2D image data. We generalize Morphing to 3D by performing first-of-its-kind 3D Morph operations on point clouds and present the results on both generation and detection. We generate a GAN-based facial composite of face images from face images of two contributory data subjects, with an extensive evaluation of different facial regions.

GIUSEPPE STRAGAPEDE - BIOMETRIC RECOGNITION BASED ON MOBILE HUMAN-COMPUTER INTERACTION

Full Title: Biometric Recognition based on Mobile Human-Computer Interaction
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Vera-Rodriguez and Ruben Tolosana
URL: https://repositorio.uam.es/handle/10486/715062
Contact email: ruben.vera@uam.es

Abstract:
The rapid digitalization of society is creating unprecedented Human-Computer Interaction (HCI) scenarios. Mobile devices such as smartphones and wearables have high computing and connectivity capabilities, and they are provided with several sensors that are able to acquire a vast and diverse amount of information pertaining to the users, for purposes such as security (biometric verification systems), health and fitness (activity trackers), user profiling (social media and e-commerce), among others. From one perspective, many studies have highlighted the disadvantages of passwords and physiological biometric characteristic such as fingerprint or face, as they may be easy to be stolen, forged, and they cannot guarantee prolonged protection throughout the entire device usage. To this end, it can be shown that the touch gestures on the smartphone screen and the body movements captured by the background sensors are traits that provide enough discriminative power to be associated with users' identities, and therefore to be used for biometric recognition. On the flip side, the large availability of personal data generated on mobile devices has turned this technology into a potential source of major invasion of personal privacy. In fact, thanks to the recent advancements of Artificial Intelligence (AI), the automated processing of mobile user interaction data can easily reveal users' sensitive attributes, reducing the privacy and security of the users. In this scenario, this Thesis work aims at advancing behavioral biometrics for mobile transparent user authentication. This objective is pursued by considering different modalities (touch gestures, mobile sensor data patterns, and keystroke dynamics), state-of-the-art deep learning classifiers, metrics, and databases. At the same time, individuals' mobile behavioral biometric data used for authentication might enclose personal and sensitive information. This aspect is also explored for privacy quantification. This Dissertation comprises four different parts. Part I first concentrates on the problem statement and main contributions of the Thesis. The experimental chapters are then divided into two parts, Part II, and Part III. Lastly, Part IV concludes the Thesis. Part I presents the basics of biometric systems, together with an explanation of the theoretical framework and the practical applications of the current Thesis, an outline of the Dissertation, and a summary of the research contributions originated from this Thesis. Then, the most important aspects of related work are described, with a presentation of the databases used, and the metrics adopted in the experimental part of this Dissertation. The first experimental part (Part II) presents a comparative analysis of unimodal and multimodal behavioral biometric traits acquired while the subjects perform different activities on the phone such as typing, scrolling, drawing a number, and tapping on the screen, considering the touchscreen and the simultaneous background sensor data (accelerometer, gravity sensor, gyroscope, linear accelerometer, and magnetometer). The experiments are performed over HuMIdb, one of the largest and most comprehensive freely available mobile user interaction databases to date. A separate Recurrent Neural Network (RNN) with triplet loss is implemented for each single modality, followed by the biometric fusion at score level, leading to Equal Error Rates (EER) ranging from 4% to 9% depending on the modality combination in a 3-second interval. Then, a new database, BehavePassDB, collected within this Thesis work, is presented and benchmarked with similar results in terms of recognition performance. BehavePassDB is structured into separate acquisition sessions and tasks to mimic the most common aspects of mobile Human-Computer Interaction (HCI), and it was acquired through a dedicated mobile app installed on the subjects devices, also including the case of different users on the same device for evaluation. An international ongoing competition, MobileB2C, was organized based on the novel database. In the second experimental part (Part III of this Dissertation), the focus of exploring mobile behavioral biometrics is narrowed down to Keystroke Dynamics (KD), which resulted to be the most discriminative trait among the ones considered in the earlier chapters. First, a novel Transformer architecture, TypeFormer, is proposed for mobile KD-based verification improving recent state-of-the-art keystroke verification systems based on

LSTM RNNs. Then, a novel experimental framework to benchmark keystroke for biometric verification is described, designed to quantify the recognition performance as well as the fairness of biometric systems. The framework is provided in the form of the Keystroke Verification Challenge at the 2023 IEEE International Conference on Big Data. To create the framework, we consider two of the largest public databases of keystroke dynamics up to date, the Aalto Desktop and Mobile Keystroke Databases, extracting datasets that guarantee a minimum amount of data per subject, age and gender annotations, absence of corrupted data, and that avoid too unbalanced subject distributions with respect to the considered demographic attributes. The framework is designed to represent the modern challenges of massive application usage, counting on over 185,000 subjects, and it considers tweet-long sequences of arbitrary text, in mobile and desktop scenarios.

MELZI PIETRO - SECURITY AND PRIVACY ENHANCEMENT IN BIOMETRIC AND EHEALTH SYSTEMS

Full Title: Security and privacy enhancement in biometric and ehealth systems: new machine learning approaches for ecg, face, and data synthesis
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Tolosana and Ruben Vera-Rodriguez
URL: https://repositorio.uam.es/handle/10486/715035
Contact email: ruben.tolosana@uam.es

Abstract:
Privacy, encompassing the right to protect personal freedom and private life, encounters challenges in our digitalized society due to technological advancements like Big Data, the Internet of Things, and Artificial Intelligence. The erosion of privacy is accelerated by the widespread collection of personal data, requiring novel approaches to mitigate privacy risks. Biometric technologies, such as face recognition, contribute to increasing privacy concerns as they process personal data, representing biological and behavioral characteristics of individuals. These biometric data enable the automatic extraction of distinguishing features across individuals and possess favorable properties for recognition, leading to their extensive use in security applications. Biometric recognition systems consist of various subsystems that capture biometric samples, process, and compare them to determine if individuals are recognized or not. Over the years, biometric data have seen growing use in civil and commercial applications, including healthcare. While beneficial, this progress underscores the importance of protecting individuals' privacy during the collection and use of biometric data. The General Data Protection Regulation (GDPR), introduced in 2016 in the European Union, outlines data protection principles, categorizing biometric data as sensitive and requiring explicit consent before collecting them. Storing unprotected biometric data raises privacy concerns, as potential leaks of the original data representations can compromise individuals' security. Attacks on biometric databases pose risks such as impersonation, unauthorized system access, and the extraction of personal attributes, including health conditions, emotions, and soft-biometric traits. To align with the GDPR and address privacy concerns, numerous Privacy-Enhancing Technologies (PETs) have been proposed in the literature to securely store biometric data in biometric recognition systems. While numerous PETs are designed to implement essential data protection principles, dedicated technologies must be considered in the context of biometric recognition. This Dissertation is motivated by the convergence of several factors. Firstly, the widespread use of biometric data across various applications has raised concerns about their potential misuse for unintended purposes. Secondly, technological advancements have led to the exploration of novel biometric characteristics for monitoring medical information and daily activities. Additionally, the application of Deep Learning technologies to biometric data, such as transformers and generative models, has further pushed the field forward with unexplored possibilities. Within this Dissertation, we address concerns related to privacy erosion, including the extraction of soft-biometric attributes, which have gained increased attention over the years. Finally, the impact of privacy regulations that resulted in the discontinuation of widely used public databases, reducing the availability of data for various biometric applications, is also a factor that motivates this Dissertation. With this Dissertation, we make a substantial contribution to enhancing multiple aspects of security and privacy within biometric technologies. It is organized into five parts, with a focus on the investigation of three interconnected research lines. Part I outlines the problem statement and highlights the contributions made throughout this Dissertation. Subsequently, the three central parts describe in detail the studies carried out to explore the different research lines. Part II delves into privacy quantification in scenarios involving Human-Computer Interfaces, with a particular focus on the emerging biometric characteristic of electrocardiograms (ECGs), examined in both security and eHealth applications. New Machine Learning (ML) approaches based on ECGs have been investigated for the applications of individual recognition and disease prediction. This research line has produced evidence regarding the amount of sensitive information contained in ECGs and significant advances in the mentioned applications. Part III conducts a literature review of PETs for biometric recognition systems, introducing a comprehensive framework to classify them and evaluate their properties. Additionally, this research line includes benchmarking of state-of-the-art technologies belonging to a specific category of PETs, i.e., cancelable biometrics. Our

benchmarking has been conducted by applying such technologies to the templates extracted from different biometric characteristics and evaluating their properties under different threat models. Finally, in Part III we also introduce novel PETs for protecting demographic information contained in biometric templates extracted from face images. Part IV explores the application of synthetic data for training face recognition technologies. Synthetic data are a thriving topic, providing advantages compared to real data in terms of privacy, data availability, and representation of diverse conditions of interest. Generative models are used in Part IV to create suitable databases for face recognition, and their effectiveness in training face recognition systems is evaluated in the subsequent sections of Part IV. Furthermore, an international challenge (the FRCSynChallenge) has been organized to assess the potential of synthetic data in training face recognition systems, addressing demographic biases, and enhancing face recognition performance under challenging conditions. FRCSyn has obtained significant interest and participation from both industry and academia, with numerous teams achieving remarkable results. Due to this success, a second edition of FRCSyn, featuring novel tasks, is currently in progress at the time of writing this PhD Thesis. To summarize, this Dissertation contributes to the understanding of privacy challenges in biometric technologies and provides novel insights and solutions across diverse applications. The main contributions of this PhD Thesis include: i) algorithmic advances in ECG applications for security and eHealth, ii) the analysis of existing PETs for biometric recognition systems, along with the proposal of novel PETs for safeguarding the soft-biometric attributes contained in biometric data, and iii) the proposal of novel ML methods to generate synthetic data, and their application to overcome current challenges in face recognition technologies. The objectives outlined at the beginning of the Dissertation have been fulfilled throughout the completion of the different research lines. Additionally, the research work completed throughout this PhD Thesis includes the generation of various literature reviews and new biometric resources.

MAHDI GHAFOURIAN - SECURITY AND PRIVACY IN DISTRIBUTED BIOMETRIC SYSTEMS INCLUDING BLOCKCHAIN AND FEDERATED LEARNING: NEW SCHEMES FOR PROTECTION AND DE-IDENTIFICATION

Full Title: Security and privacy in distributed biometric systems including blockchain and federated learning: new schemes for protection and de-identification
Institution: Universidad Autonoma de Madrid
Supervisor: Julian Fierrez and Ruben Vera-Rodriguez
URL: https://repositorio.uam.es/handle/10486/715029
Contact email: julian.fierrez@uam.es

Abstract:
This Thesis is focused on the security and privacy of state-of-the-art deep learning-based biometric systems in centralized and distributed paradigms. The main scientific goals of this PhD are 1) to analyze the main challenges and requirements of contemporary biometric recognition systems in terms of both security and privacy in single and multi-modal modalities; 2) to evaluate several state-of-the-art approaches, the information stored, the recognition performance, the potential advantages, and limitations; and 3) to review existing and propose novel metrics and algorithms to measure and improve the levels of security and privacy (noninvertibility, revocability and unlinkability) of biometric templates for both modalities. The Thesis addresses corresponding problems from a holistic perspective and proposes solutions based on state-ofthe- art in two main scientific disciplines: artificial intelligence using machine learning and deep learning methods, and cryptography. Due to the high level of popularity and deployment of face biometrics, the solutions given in this Thesis were practiced but not limited to this trait. In particular, we contributed to biometric protection by proposing a novel biometric template protection method. In addition, we addressed privacy preservation in biometrics using different strategies. To this end, we studied the impact of combining blockchain and biometrics in terms of its pros and cons on the security and privacy of biometrics. Moreover, we experimented with the privacy-by-design biometric models in distributed systems. Lastly, the utilization of adversarial examples as a method for preserving privacy in biometric systems has been implemented. This Dissertation consists of five parts. Part I first introduces the biometric systems and modalities that are being used in the current era, as well as a detailed description of related works for defining current security and privacy risks. This part finishes by providing metrics and databases that are used for this PhD study. The next three parts (Part II, III, IV) address three research paths that this PhD study has pursued to fulfill the aforementioned scientific goals. Part II is focused on biometric template protection (BTP) as the forefront concept for fighting vulnerabilities threatening the security of biometric systems. This part gives a thorough explanation of the proposed novel BTP method, OTB-Morph, for biometric verification. In the third part (Part III of this Dissertation), biometric security and privacy for distributed systems and collective learning have been addressed. This part presents an interdisciplinary comprehensive survey for combining biometrics and blockchain from both technical and legal perspectives. Furthermore, it takes the security challenges of the federated learning paradigm for face recognition into consideration. The last experimental part (Part IV of this Dissertation) is completely focused on privacy preservation in biometric systems. To this end, this part recounts the detail of using adversarial examples as a privacy preservation method to de-identify face biometrics from personal photos. Finally, drawn from experimental findings Part V concludes this Thesis and presents the main line of the future work for the security and privacy of contemporary biometric systems.

LUIS FELIPE GOMEZ - ENHANCING SECURITY AND APPLICABILITY IN MULTIMODAL FACIAL BIOMETRICS

Full Title: Enhancing security and applicability in multimodal facial biometrics
Institution: Universidad Autonoma de Madrid
Supervisor: Julian Fierrez and Aythami Morales
Link description: https://repositorio.uam.es/handle/10486/718080
Contact email: julian.fierrez@uam.es

Abstract:
The research interest in the applicability of facial biometrics has been progressively growing each year, primarily driven by rapid advancements in information technology, electronics, and telecommunications. Throughout this new deployment of telecommunications, the high availability and ease of communication through Wi-Fi, 4G, and 5G networks have spurred advancements in fields such as electronic national administration, banking, online education, healthcare, and commerce. The new technologies have enabled devices to acquire, process, and store a wide range of data massively during interactions between these devices and individuals, introducing numerous services into people's daily lives that were previously only accessible to a few, offering many possibilities and lines of research in applications such as security, healthcare, online services, and video surveillance. Among all these advancements, facial biometrics has experienced the most significant growth in recent years, thanks to its distinctive features, such as the ability to acquire information remotely without being intrusive to the user and the possibility of using inexpensive devices for capture, such as video cameras integrated into mobile phones, computers, and consumer digital cameras. This rapid growth and deployment of facial biometrics have generated the need to thoroughly investigate specific aspects of their applicability and security. The main objective of this Thesis is to analyze, develop, and implement new applications based on algorithms for modeling facial biometrics in multiple fields of study, such as health, security, and online learning. We propose revisions and evaluations of existing methods in the literature for each of these topics, as well as approaches using the potential of deep learning-based technologies and domain adaptation methodologies due to the lack of training data that may exist in certain fields. This Dissertation consists of five different parts. Part I focuses on stating the problem and the main contributions of the Thesis, as well as a comprehensive summary of the state of the art. The first experimental part of this Dissertation (Part II) is focused on Parkinson's disease detection. The research was initially carried out using classical machine learning techniques for facial expression analysis in video. Static and dynamic features were analyzed in a dataset based on facial geometry. Finally, three different facial analysis domains were used to evaluate users using deep learning models employing sequence analysis. The results show that facial expressions can be used to explore the detection of Hypomimia in Parkinson's patients through multiple techniques employed over the years in computer vision. The second experimental part (Part III) analyzes models based on pulse extraction for presentation attack detection. Multiple presentation attack instruments were implemented during development, varying from masks based on paper, latex, or silicone to video playback for identity spoofing. The results showed the high capacity of models based on physiological characteristics for detecting such presentation attack instruments. Part IV is the last experimental part of this Dissertation. In it, seven modules based on deep learning are analyzed to extract facial features to estimate high and low attention in time series. During the development of this part, two feature extraction methods were implemented: local features to analyze the entire time sequence and global features to extract relevant information from these time sequences. The results found that multimodal combinations among the extraction algorithms provided better results in estimating attention levels. Finally, in Part V, the conclusions drawn from the experimental part of the Thesis are presented and discussed, as well as the main lines of future work that have been identified. The research carried out in this Thesis has achieved several contributions advances in facial biometrics and offer new perspectives in aiding the treatment of Parkinson's disease, as well as improving security in facial recognition biometric systems and attention level estimation in online learning environments.

JAROMÍR ŠTĚPÁNEK - BIOMETRIC DATA, ITS COLLECTION AND USE BY THE MILITARY POLICE FOR IDENTIFICATION PURPOSES

Full Title: Biometrické údaje, jejich sběr a využití ve Vojenské policii pro identifikační účely
Institution: Police Academy of the Czech Republic in Prague
Supervisor: Assoc. Prof. JUDr. Mgr. Jan Bajura, Ph.D.
Contact email: stepanek@polac.cz

Abstract:
The experience of the current and ended military conflicts shows the importance of using the biometric data collection of soldiers for the purpose of their future identification, when the bodies of soldiers cannot be identified by face or other obvious landmarks for any reason. Apart from the forensic concept, securing biometric data entail mainly a legal dimension. The collection of biometric data and the subsequent identification of individuals is an essential basis in proceedings on the eligible interests of the individuals affected by the death of the testator and can be a part of the examination of the body in the clarification of the war crimes in the context of international criminal law. By evaluating of the anatomical-physiological-biometric knowledge, in connection with the knowledge of the police forensic methods in the field of identification, comparison of the national legal standards, including evaluation of the practice of individual units of the Military Police of the V4 states in the field of biometric data collection for also for the possible future identification purposes and conducted investigation among Czech professional soldiers seems to be appropriate to be considered regarding the legislative amendments to the Act on Military Police and other relevant laws within the meaning of the collecting and preservation biometric data from soldiers upon acceptance into their service and data updating, when sending soldiers on foreign missions. The proposed biometrics includes a three-part photograph including visible tattoos, dactylographic fingerprints and palm prints, DNA analysis, as well as procuring dental orthopantomography (OPG) X-ray images.

KEVIN HERNANDEZ-DIAZ - OCULAR RECOGNITION IN UNCONSTRAINED ENVIRONMENTS

Full Title: Ocular Recognition in Unconstrained Environments
Institution: Halmstad University
Supervisor: Fernando Alonso-Fernandez
URL: http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-53257
Contact email: feralo@hh.se

Abstract:
This thesis focuses on the problem of increasing flexibility in the acquisition and application of biometric recognition systems based on the ocular region. While the ocular area is one of the oldest and most widely studied biometric regions thanks to its rich and discriminative elements and characteristics, most modalities such as retina, iris, eye movements, or oculomotor plant have limitations regarding data acquisition. Some require a specific type of illumination like the iris, a limited distance range like eye movements, or specific sensors and user collaboration like the retina. In this context, this thesis focuses on the periocular region, which stands out as the ocular modality with the fewest acquisition constraints. The first part focuses on using middle-layers' deep representation of pre-trained CNNs as a one-shot learning method, along with simple distance-based metrics and similarity scores for periocular recognition. This approach tackles the issue of limited data availability and collection for biometric recognition systems by eliminating the need to train the models for the target data. Furthermore, it allows seamless transitions between identification and verification scenarios with a single model, and tackles the problem of the open-world setting and training bias of CNNs. We demonstrate that off-the-shelf features from middle-layers can outperform CNNs trained for the target domain that followed a more extensive training strategy when target data is limited. The second part of the thesis analyzes traditional methods for biometric systems in the context of periocular recognition. Nowadays, these methods are often overlooked in favor of deep learning solutions. However, we show that they can still outperform heavily trained CNNs in closed-world and open-world settings and can be used in conjunction with CNNs to further improve recognition performance. Moreover, we investigate the use of the complex structure tensor as a handcrafted texture extractor at the input of CNNs. We show that CNNs can benefit from this explicit textural information in terms of performance and convergence, offering the potential for network compression and explainability of the features used. We demonstrate that CNNs may not easily access the orientation information present in the images that are exploited in some more traditional approaches. The final part of the thesis addresses the analysis of periocular recognition under different light spectra and the cross-spectral scenario. More specifically, we analyze the performance of the proposed methods under different light spectra. We also investigate the cross-spectral scenario for one-shot learning with middle-layers' deep representations and explore the possibility of bridging the domain gap in the cross-spectral scenario by training generative networks. This allows using simpler models and algorithms trained on a single spectrum.

UNA KELLY - UNDERSTANDING FACE RECOGNITION SYSTEMS' VULNERABILITIES BY EXAMINING LATENT SPACES

Full Title: Understanding Face Recognition Systems' Vulnerabilities by examining Latent Spaces
Institution: University of Twente
Supervisor: Raymond Veldhuis and Luuk Sprteeuwers
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
Face recognition plays an important role in modern when we travel through airports that use automated border and police use it to find criminals in their databases. While its role in public surveillance is currently hotly debated,it is in some cases already being used. Understanding the algorithms used for face recognition and their potential weaknesses is therefore very relevant. A face recognition system verifies the identity of an individual by comparing two facial images and deciding whether or not identity information extracted from both images is similar. If it considers this to be sufficiently similar it accepts them as a match. Two images of different persons - person A and person B - can be mixed to create a morph. It has been shown in several publications that when a face recognition system compares the morph with an image of person A it is accepted as a match, but also when it compares the morph with an image of person B. This can lead to potential security issues. For example, if someone were to apply for an ID document using such a morphed passport photo this could enable more than one person to travel using the same ID document. In contrast to most detection approaches, which try to find traces of morphing in images, in this thesis we look at the effect of morphing by examining the feature spaces of face recognition systems. Instead of using traces caused by morphing to separate normal images from morphed images, which decreases vulnerability to known types of morphing attacks, we aim to develop approaches to fundamentally decrease the potential vulnerability of face recognition systems, i.e. also to unknown attacks. Our approach to the problem of detecting morphing attacks is to analyse face recognition systems in order to better understand why they are vulnerable to morphing attacks. This approach has helped us to identify two ways to support research on morphing attacks. First, we have understood that we need to look critically at reported performances of morphing attack detection methods, since they may be too optimistic, for example due to overfitting on a specific type of morph or a specific dataset. Developing new types of morphs can help estimate and ideally reduce overfitting, by leading to more varied morphing datasets for training and/or evaluation. This can help reduce the risk of overestimating performance of morphing attack detection methods and underestimating the vulnerability of face recognition systems. We introduced worst-case morphs, which allow one to understand the theoretical vulnerability of FR systems, and showed that it is possible to generate approximations of worst-case morphs. Exploiting information from embedding spaces of FR systems on the one hand allowed us to approximate such worst-case morphs in the image domain and on the other hand inspired an approach for face de-identification, where images are manipulated so that to the human eye they look almost unchanged, but can no longer be recognised by face recognition systems. By analysing normal and de-identified images in the latent space of a face recognition system, we discovered a way to circumvent de-identification and showed how de-identification can be improved to prevent this. Second, one reason face recognition systems are vulnerable to morphing attacks is because they were not trained with morphed images and were simply not developed to deal with images that contain identity information from more than one person. In fact, the better a face recognition system is at identity verification - distinguishing between mated and non-mated pairs of facial images - the more vulnerable it is to morphing attacks. While most morphing attack detection methods are based on texture analysis, there are very few detection methods that are explicitly based on identity information in facial images. We show that the robustness of face recognition can be improved, forcing it to rely on identity information by adding typical morphing artefacts to normal facial images in the training data. We compare the similarities and differences between face recognition systems and approaches for differential morphing attack detection, showing that they can reach similar performance on different types of morphs. We explain why there is a trade-off between performance on normal images and vulnerability to morphing attacks of face recognition systems, which we illustrate using simulations in the latent space, and suggest a new way to select decision thresholds that makes use of worst-case morphs to limit vulnerability to all

types of morphing attacks.

PESIGRIHASTAMADYA NORMAKRISTAGALUH - UNDERSTANDING THE IMAGING PROCESS AND ROLE OF ILLUMINATION IN FINGER VASCULAR PATTERN RECOGNITION

Full Title: Understanding the Imaging Process And Role Of Illumination In Finger Vascular Pattern Recognition
Institution: University of Twente
Supervisor: Raymond Veldhuis and Luuk Spreeuwers
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
Finger vascular pattern recognition, also known as finger vein recognition, is the utilization of finger blood vessels, including veins and arteries, for pattern recognition in biometric applications. In contrast to other biometric traits, such as fingerprints, faces, or iris, finger-vein characteristics cannot easily be replicated, leave no traces, and are convenient to use. Because of these advantages, finger vein recognition is increasingly being used in security applications. However, due to various aspects of the imaging process that can influence recognition performance, there is still research going on aiming at better image quality. Most research focuses on improved feature extraction to increase recognition performance. The near-infrared (NIR) spectrum has been used to illuminate the finger in several finger vein imaging devices. In practice, obtaining high-quality vascular patterns can be challenging since the images may be blurry, have varied intensity areas, and have varying contrast. The literature on finger-vein recognition does not go further in its explanation of the imaging process than the assumption that hemoglobin in the blood absorbs light while other tissues scatter it. One commonly accepted belief is that the high scattering of light in living tissues during imaging is the main reason for contrast deterioration in finger-vein images. Image formation and imaging processes of finger vein patterns are typically not explained in great depth. This thesis presents a model to obtain a better understanding of the imaging of finger vein patterns and the impact of illumination in the imaging process. It can be used to improve the acquisition device, resulting in improved image quality and recognition performance. With a literature study, Chapter 2 presents finger vein recognition challenges that are the basis of our research and provides a pre-processing technique for alignment. The implementation of a physical model with a prototype finger phantom is described in Chapter 3. Furthermore, the phantom is used to analyze more in-depth a model for a better understanding of the imaging of finger vein patterns, as elaborated in Chapter 4.To make finger vein patterns visible in the NIR spectrum, three types of illumination (top-transmission, 2-sided illumination, and reflection) are used for illuminating the finger. Although the illumination methods differ, the resulting finger-vein images show similar characteristics. We found that vascular patterns from different types of illumination are very similar, but the contrast saturation is different. The effect of illumination on the image quality of finger vein images for finger vein recognition has yet to be thoroughly investigated. Near-infrared (NIR) light-emitting diodes (NIR LEDs) with various broad opening angles, for example, have been widely employed in finger vein scanners instead of visible light. To the best of our knowledge, relatively few researchers have attempted to quantify the impact of illumination bundle width on the finger vascular pattern imaging process. Chapter 5 presents new results on the impact of illumination bundle width and illumination direction on the NIR image quality of the finger vein and the performance of finger vein recognition (FVR). In conclusion, the research in this thesis presented mainly two types of models: a physical model and a qualitative theoretical model. These models can be used to enhance image quality and improve the performance of finger vein recognition. All experiments that have been conducted support the proposed model.

PATRICK TINSLEY - TRUST, AI, AND SYNTHETIC BIOMETRICS

Full Title: Trust, AI, and Synthetic Biometrics
Institution: University of Notre Dame
Supervisor: Adam Czajka and Patrick Flynn
URL: https://curate.nd.edu/articles/dataset/Trust_AI_and_Synthetic_Biometrics/25604631?file=46169100
Contact email: aczajka@nd.edu

Abstract:
Artificial Intelligence-based image generation has recently seen remarkable advancements, largely driven by deep learning techniques, such as Generative Adversarial Networks (GANs). With the influx and development of generative models, so too have biometric re-identification models and presentation attack detection models seen a surge in discriminative performance. However, despite the impressive photo-realism of generated samples and the additive value to the data augmentation pipeline, the role and usage of machine learning models has received intense scrutiny and criticism, especially in the context of biometrics, often being labeled as untrustworthy. Problems that have garnered attention in modern machine learning include: humans' and machines' shared inability to verify the authenticity of (biometric) data, the inadvertent leaking of private biometric data through the image synthesis process, and racial bias in facial recognition algorithms. Given the arrival of these unwanted side effects, public trust has been shaken in the blind use and ubiquity of machine learning. However, in tandem with the advancement of generative AI, there are research efforts to re-establish trust in generative and discriminative machine learning models. Explainability methods based on aggregate model salience maps can elucidate the inner workings of a detection model, establishing trust in a post hoc manner. The CYBORG training strategy, originally proposed by Boyd, attempts to actively build trust into discriminative models by incorporating human salience into the training process. In doing so, CYBORG-trained machine learning models behave more similar to human annotators and generalize well to unseen types of synthetic data. Work in this dissertation also attempts to renew trust in generative models by training generative models on synthetic data in order to avoid identity leakage in models trained on authentic data. In this way, the privacy of individuals whose biometric data was seen during training is not compromised through the image synthesis procedure. Future development of privacy-aware image generation techniques will hopefully achieve the same degree of biometric utility in generative models with added guarantees of trustworthiness.

MONITOR
MASTER-THESES

JOHANNE DYBEVIK AND LISE MARIE BREKKE NILSEN - RANKING OF CYBERGROOMING CONVERSATIONS

Full Title: Ranking of Cybergrooming Conversations
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
As the threat of cybergrooming continues to escalate in today's society, the importance of finding ways to detect and prevent it is more pressing than ever. To address this issue, this master's thesis is focused on the development of a ranking system that can identify sexual conversations in real time on an online application. Earlier research has mainly focused on the detection part, but the ranking system has, to the best of our knowledge, not been investigated in previous research. We will therefore add a ranking system so application moderators can easier prioritize the most concerning conversations. The ranking system operates using a dynamic conversation-based approach, assigning each conversation with a risk score. A higher risk score indicates a conversation with a higher degree of sexual content, thus positioning the conversation higher up in the rank hierarchy. To optimize the efficiency and performance of the system, different language models and score-boost functions are evaluated and compared. The score from the language model is used to determine how much the risk of a conversation should go up or down. For this task, different score-boost functions are studied. To be able to fine-tune the language models and to test the results afterward, a dataset with real data from a gaming platform for children has been used. This has provided us with up-to-date data, containing both sexual and normal conversations. This master's thesis employs precision and speed-performance as metrics to evaluate the developed ranking system. The precision of 0.930 has been achieved by looking at the top 200 ranked conversations. Furthermore, based on our dataset, the system can score and rank up to seven times the average amount of data sent across the gaming platform in a single day. Our results demonstrate therefore that it is possible to quickly score and maintain a rank hierarchy for all the conversations within an application.

BENJAMIN GRJOTHEIM DYBVIK AND JOHANNE KAATORP - A DYNAMIC GRAPH, CONTEXT, AND CONTENT ANALYSIS APPROACH TO DETECT CYBERGROOMING

Full Title: A Dynamic Graph, Context, and Content Analysis Approach to Detect Cybergrooming
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
The internet, and especially social media, has become a fundamental part of our life, no matter the age. Many social media platforms are targeted towards children enabling them to contact new friends without the need for physical meetings. Despite the clear benefits of social media, it also raises concerns about threats facing children online. These platforms do not only give access to children, but also to people with bad intentions, such as predators. Predators can create fake online profiles, pose as a child, and contact vulnerable children with a minimal risk of disclosure. Online assaults can result in psychological, physical, emotional, behavioral, and psycho-social issues affecting the child for the rest of its life. To avoid such life altering consequences it is crucial to detect and prevent sexual abuse online. During this thesis we have investigated whether a combined graph, context and content analysis approach could be used to dynamically detect predators online. This was accomplished by studying the behavior of individual users in game chats. We implemented a supervised machine learning algorithm which classified the messages sent by the users based on several behavioral features. Further, a detection mechanism was created to detect predators as early as possible whilst achieving high recall and precision. Based on the results achieved we concluded that dynamic detection of predators in chats is possible. In addition, we concluded that early detection of predators was possible when monitoring the user’s behavior in ongoing chats. To continue the research into improving detection, the use of other classification algorithms, inclusion of other features and approaches to calculate them, and other detection mechanisms should be studied.

JANUSZ JAGIELLO - TRAINING TOOL FOR DETECTING FACE IMAGE MANIPULATION

Full Title: Development of a Training Tool for Detecting Face Image Manipulation Utilising Eye Tracking Data from Human Super-Recognisers
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Juan Tapias
Contact email: christoph.busch@h-da.de

Abstract:
This thesis investigates the innovative training concept utilising eye tracking data from human super-recognisers to enhance human performance in identifying manipulations in facial images, which is a crucial skill in highsecurity biometric verification settings like border control. The research, extending the foundational work of Nichols et al., is centred around developing intuitive visual feedback tools that specifically aim to boost human ability in recognising digital alterations in facial images. The methodology of the study involves a thorough analysis and interpretation of that eye tracking data to understand the focal points of superrecognises when examining facial images. The study features two newlydeveloped innovative methods for presenting eye tracking traces: spotlight and isotherm visualisations. Central to the research is an online experiment conducted with both professional and nonprofessional participants. This experiment was designed to test their improved ability to identify manipulated images using a tool providing detailed visual and textual feedback after each participant's decision. This innovative tool, acting as a training and enhancement mechanism, allowed participants to engage in an indepth analysis of the images. The interactions of the participants with the tool were carefully recorded, with findings indicating a notable improvement in detection capabilities across all user groups. These results demonstrate the tool's effectiveness in amplifying human skills in image analysis. The study concludes with a moderate success rate in manipulation detection, emphasising the substantial potential of merging human cognitive skills with technological advancements in biometric verification processes. Particularly noteworthy is the observed enhancement in accuracy during interactions with the tool. The experiment commenced with an average accuracy of 58%, which progressively rose to approximately 64% by its conclusion. Future research is suggested to focus on optimising feedback presentation techniques, introducing varied complexities in image manipulation, and investigating adaptive learning models. This thesis contributes crucial insights into the development of training methodologies for enhancing the accuracy and efficiency of human document examiners, who remain an integral component of various security frameworks.

MARIUS VALEN - CONTEXT VERSUS CONTENT

Full Title: Context versus Content - A context analysis of AIBA chat data using USE and SBERT
Institution: NTNU
Supervisor: Patrick Bours / Sushma Venkatesh
Contact email: patrick.bours@ntnu.no

Abstract:
In investigating criminal cases that deal with sexual abuse of children in the form of text, images and videos, it is always challenging to sort this data out of a larger amount of data. With the technological progress in society, the number of devices and the amount of data seized in criminal cases is increasing rapidly. Data storage and the amounts of data has increased exponentially in recent years and it does not seem to be stopping anytime soon. It is becoming more and more demanding to go through these amounts of data and to be able to effectively identify the data that illuminates the criminal relationship. This thesis will explore the sentimentation of messages as an aid to reveal the meaning of the content. We will further see how this scores in different sentence-models. This can lead us to the development of new lexicons for the sentiment of words that can be identified as sexual grooming and new methods to identifying sexual grooming faster and more reliable. This thesis will explore this by using a data set of message data from AiBA and analyze this through the use of Universal Sentence Encoder (USE) and Sentence-Bidirectional Encoder Representations from Transformers (SBERT) and then compare the results from the two models. We found that the sentences score quite differently even though they are contextually identical. This implies that further research to train the language models is needed.

PETER EJLEV - BIAS AND FAIRNESS WITHIN FACIAL IMAGE QUALITY ANALYSIS

Full Title: Bias and Fairness within Facial Image Quality Analysis
Institution: Technical University of Denmark (DTU) & Hochschule Darmstadt (h_da)
Supervisor: Christoph Busch, Torsten Schlett, André Dörsch and Aasa Feragen
URL: https://dasec.h-da.de/2024/08/peter-ejlev-successfully-defended-his-master-thesis-on-bias-and-fairness-within-facial-image-quality-analysis
Contact email: torsten.schlett@h-da.de

Abstract:
Facial recognition systems have become pivotal in various security and identification applications due to their reliability and non-intrusiveness. However, the performance of these systems heavily relies on the quality of the captured biometric sample. A critical concern is the potential for bias when dealing with different demographic groups such as ethnicity, gender, and age. This thesis aims to evaluate the performance of several Quality Components of the Open Source Face Image Quality (OFIQ) framework across demographic groups to identify any potential biases. OFIQ is a reference implementation for the international standard ISO/IEC DIS 29794-5, developed by the Federal Office for Information Security (BSI). This standard aims to provide a consistent method for assessing facial image quality, which is crucial for various applications. OFIQ evaluates facial images using 34 different quality assessment components. The output of OFIQ's quality measures is a quality score in the range of 0-100, with a higher score indicating better quality. The thesis examined the consistency and fairness of these quality components across demographic variables. For this purpose, the two datasets VGG-Face2 and Balanced Faces in the Wild (BFW) were selected for their comprehensive demographic representations. This work is limited to a subset of OFIQ quality components, namely: luminance mean, luminance variance, under-exposure prevention, over-exposure prevention, natural color, and unified quality score. Key findings revealed significant performance differences of aforementioned quality components across demographic groups. For ethnicity, the African American group exhibited very high discard rates in luminance mean and luminance variance, with discard gaps of up to 54 % and 17 %, respectively, indicating clear biases. The unified quality score, which is based on a model from MagFace, showed the worst performance for the East Asian group, with a mean discard gap of 10.03 % in the critical 0-50 scalar range. This suggests that potential biases in image quality assessment are not exclusively limited to OFIQ but also reflect biases inherent in the underlying MagFace model. In terms of gender, males were found to be assigned higher quality scores than females, especially considering luminance mean, with discard percentage gaps reaching up to 25 %. Looking at the unified quality score, males were scored marginally better than females with a max discard percentage difference of 11.6 %, indicating a moderate bias against females in these assessments. For age, the senior group (age above 61) performed the best with regards to the unified quality score, followed by the middle-aged group (aged between 26 and 60), and then the young group (aged 25 and under). A maximum difference in discard percentage from the young to the senior group was found to be 13.68 %, indicating a significant bias against the young group.

KATRINE BAY - FAIRNESS IN FACE RECOGNITION

Full Title: Enhancing Face Recognition Models with Synthetic Child Data: A Fairness Assessment
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Christian Rathgeb
Contact email: christoph.busch@h-da.de

Abstract:
Despite the widespread adoption of facial recognition technology in various applications, significant challenges persist in ensuring fair and unbiased performance across different age groups. These challenges are particularly pronounced in scenarios involving children, who are often underrepresented in training data sets, leading to biased algorithms that perform with higher accuracy on adults. This thesis investigates the enhancement of demographic fairness, particularly concerning children, in state-of-the-art face recognition models. It further seeks to align with a responsible development framework following the novel regulations for biometric identification systems in the EU AI Act and ISO/IEC standards. The research aims to address these issues by the bias mitigation technique of fine-tuning pre-trained face recognition models using synthetic images of children's faces. This approach seeks to mitigate bias while maintaining privacy. The thesis evaluates the fairness of these models using performance metrics, including the False Positive Identification Rate, False Negative Identification Rate, and the demographic fairness metric False Negative Differential. Performance is assessed across different age subgroups, categorising children into age ranges from 1 to 15 years and comparing these groups with adults. These insights contribute to enhancing fairness in face identification systems for children, suggesting that while fine-tuning on synthetic data improves the overall recognition performance for children, it does not enhance the demographic fairness of the face recognition system. To further the development of fair face recognition systems for identification, this thesis discusses alternative bias mitigation strategies, carefully balancing the trade-off between privacy and performance. These strategies are evaluated within the context of compliance with regulatory frameworks governing the field.

JOËL WATTER - FACE RECOGNITION BASED ON FACIAL ATTRIBUTES IN DEGRADED IMAGES

Full Title: Face Recognition Based on Facial Attributes in Degraded Images
Institution: Department of Informatics, University of Zurich
Supervisor: Manuel Günther
URL: https://seafile.ifi.uzh.ch/f/7c25c81f96cc4f34b0a9/
Link description: Master thesis Joël Watter
Contact email: guenther@ifi.uzh.ch

Abstract:
The classification and recognition of faces in image data is vital for countless digital applications. Ideal environments for image capture are rarely given and the resulting image data may be subject to degradations such as atmospheric turbulence. In recent years, deep convolutional neural networks (DCNN) have become the state-of-the-art for facial attribute classification. With no prior adaptation, such networks can suffer from low classification accuracy when confronted with perturbed images. This thesis explores and confirms the potential of training a DCNN on simulated atmospheric turbulence data to produce a classification model that is reasonably robust to different levels and types of image disturbances. With an in-depth analysis of the classification measurement results, the improved attribute prediction stability of an adapted model compared to existing approaches is assessed and validated. With the ever-increasing performance of DCNNs, most modern face recognition systems rely on deep feature embeddings rather than actual facial attribute classifications. Depending on the training of specific embedding models, such recognition systems can be prone to image perturbations. To investigate the usability for a face recognition task, support vector machines (SVM) are trained with the outputs of the adapted attribute classification models from this thesis. The performance comparison to a deep feature embedding model shows promising potential for images with higher levels of perturbation. A final analysis of different model and SVM recognition pipeline compositions demonstrates, that the solid recognition performance can be attributed to the underlying facial attribute classification model and does not heavily rely on an SVM trained with the outputs of the exact same model.

RAMLAH SARA REHMAN - TRAINING HUMANS FOR SYNTHETIC FACE IMAGE DETECTION

Full Title: Training Humans for Synthetic Face Image Detection
Institution: Technical University of Denmark
Supervisor: Mathias Ibsen, Christian Rathgeb, Christian D. Jensen, Christoph Busch
Contact email: mathias.ibsen@h-da.de

Abstract:
Advancements in generative models for image synthesis have revolutionised the field of computer vision and artificial intelligence. In recent years, generative models have become capable of producing hyper-realistic synthetic images. These synthetic images can be used for nefarious purposes and the prevalence of these images in digital media can have large scale negative implications for individuals and governments. The increased frequency of synthetic content appearing in digital media raises the concern of whether authentic content can be distinguished from the synthetic. This thesis addresses human detection capabilities in distinguishing authentic face images from the synthetic. To test these capabilities, two perceptual experiments are designed and carried out based on principles from experimental psychology and optimal experimental design. Participants are randomly assigned to either the experimental group or the control group. The experimental group receives training halfway through the experiment, while the control group instead receives a coffee break. In one trial of the experiment, participants are presented with a face image, and are then tasked with classifying it as either 'Real' or 'Synthetic'. Each experiment consists of 32 trials, where face images are presented to participants in a random order. Participants in the experimental group are provided with a training session. This training session is developed based on face perception theories and professional face identification training material. The training session consists of systematic analysis providing participants with a visual face identification strategy. It also includes providing participants with example images where visual artefacts, a consequence of the generation process, appear in synthetic images. Results from the perceptual experiments depict that the experimental group has an improved accuracy of 3.6% after training, compared to 0.2% in the control group. This proves that training resulted in slightly improved accuracy scores, but statistical analysis shows that there is no statistically significant improvement. A discussion of the results explores the limitations of human perception and detection capabilities, particularly in reference to synthetic faces. Future work highlights the continued importance of determining human capability to detect synthetic content in different contexts.

RASMUS CHRISTENSEN - MORPHING ATTACK DETECTION

Full Title: Morphing Attack Detection respecting Face Attractiveness
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Juan Tapia
Contact email: christoph.busch@h-da.de

Abstract:
In modern society, facial recognition has become more prevalent. Its uses include automatic border control and verification of documents without human oversight. For this reason facial recognition has become a more attractive target for cyberattacks. One such attack targeting face recognition, is known as morphing attacks. Morphing attacks consist of generating a morphed image, which is sufficiently close to multiple different people's facial biometric data. Thus allowing several people to use the same image for verification. To combat morphing attacks, there is a need for automatic detection of morphed images. In this project, we displayed a correlation between images being morphed, and the perceived beauty of those images. This is due to mathematical averagelooking faces being more attractive, and morphing techniques averaging out the facial features of the images being morphed. Using this tendency of morphing techniques, a new method for detecting morphed images was created, by combining a convolutional neural network trained on beauty scores of images, together with an existing differential morphing attack detection method. The performance analysis of this new method shows that facial beauty information has the potential to improve existing morphing attack detection methods. Currently, this method has some problems which need to be addressed before it can outperform existing methods. With clear shortcomings of the new method related to more challenging optimization, and difficulty handling morphing methods which does not attempt to reduce artifacts in the morphed images.

SEBASTIAN SCHACHNER - THE ANALYSIS OF MOTION BLUR IN BIOMETRIC FACE IMAGES

Full Title: Analyse von Bewegungsunschärfe in biometrischen Gesichtsbildern
Institution: Hochschule Darmstadt (h_da)
Supervisor: Christoph Busch and Torsten Schlett
URL: https://dasec.h-da.de/2024/09/sebastian-schachner-successfully-defended-his-master-thesis-on-the-analysis-of-motion-blur-in-biometric-face-images
Contact email: torsten.schlett@h-da.de

Abstract:
This work deals with the analysis of motion blur in biometric face images. In today's society, the verification of one's own person is increasingly automated. For this purpose, a reference image, such as the passport photo on an ID card, is compared with a photo taken on site. However, if the subject moves during the photo capture process, motion blurring occurs in the image created. Under certain circumstances, this can lead to an incorrect result of the verification procedure. This motion blur is to be analyzed and estimated. For this purpose, different machine learning and handcrafted approaches are compared with each other. The machine learning approaches are divided into three classification models and a regression model. Furthermore, handcrafted approaches, which are based on the Laplace and Sobel filter and the Fast Fourier Transformation are examined. In addition, an image sharpness approach based on the Open Source Face Image Quality project was used for comparison. It was also investigated whether there is a difference in detection performance between real and synthetic motion blur. For this purpose, the approaches were tested on data sets with synthetically created motion blur and real motion blur and the CNN models were trained. Furthermore, it was investigated whether it is possible to distinguish sharp images from images with motion blur and images with other types of blur. Finally, an attempt was made to determine the direction vector of the motion blur. Various experiments were carried out. The quality estimation approaches were evaluated using Error versus Discard Characteristic curves and the Mean Absolute Error. The model for estimating different types of blur was tested and evaluated on the basis of synthetically created blur, images with synthetic and real motion blur and sharp images. The proposed algorithm for calculating the angle of motion blur was empirically tested for accuracy and reliability. It was found that the estimation of motion blur is successful with both the trained and the handcrafted approaches. Likewise, synthetic as well as real motion blur could be used to train and estimate the other. It was also shown that it is possible to differentiate between types of blur. However, no algorithm for determining the direction vector could be found. This work can be used as a basis for further research. On the one hand, the results of this work can be used as a comparison for further research and, on the other hand, to improve the approaches described here.

LEVENTE NYUSTI - USING MACHINE LEARNING TO DETECT CYBER AND PHYSICAL ATTACKS IN MOBILE ROBOTS

Full Title: Using machine learning to detect cyber and physical attacks in mobile robots - Detecting manipulation attempts against man's best (artificial) friend
Institution: NTNU
Supervisor: Patrick Bours and Sabarathinam Chockalingam
Contact email: patrick.bours@ntnu.no

Abstract:
As more and more industries employ robots to perform critical tasks, the need to secure such robots are increasing as well. This is even more true for mobile robots, where cyber/physical attacks can lead to catastrophic events, potentially loss of life. Mobile robots are more vulnerable to being attacked, as these are not always deployed in well-controlled environments. In some cases, such mobile robots include limited to no security controls. Security controls could include an Intrusion Detection System, which is used to detect when an attack is carried out, and alert the robot operator, ensuring the deployment of appropriate countermeasures in a timely manner. Timely detection of attacks or attempted attacks might lead to deployment of appropriate countermeasures, which either prevent the attack completely, or limit the negative consequences of the attack. When considering intrusion detection in mobile robots, it is necessary to monitor both the physical and cyber domain for attacks, as by their nature, attacks conducted in the cyber realm can lead to serious damages in the physical realm. Utilizing such detection mechanisms can prove to be challenging, even in a relatively simple system. In this thesis conducted at NTNU Gjøvik in collaboration with the Institute for Energy Technology (IFE) in Halden, we proposed a solution for intrusion detection in mobile robots, using a Machine Learning-based approach. This work is conducted on a Boston Dynamics Spot robot, made available by IFE. The developed system can detect cyber and physical attacks, even when the robot is deployed in a previously unknown environment, which could otherwise lead to catastrophic events. Our proposed system shows promising results utilizing datasets that we collected from Spot. To assess the performance of this system, we implemented two physical and two cyber attacks against the robot, which were identified as a part of the threat landscape for mobile robots. The method described in this thesis is expected to be applicable to all mobile robots, to detect attacks in both the physical and the cyber domain, as the data used for intrusion detection should be available in other mobile robots as well.

SEBASTIAN AARØ - THE DIGITAL IMMUNE RESPONSE

Full Title: The Digital Immune Response - True Continuous Authentication using Artificial Immune Systems for Keystroke Dynamics
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
In our rapidly developing technological lives travelling through the interconnected cyber landscape, securing our digital assets becomes even more vital. Existing measures such as usernames and passwords create a protective border between assets and malicious actors. However, static measures do not protect the asset after a successful authentication process, enabling the possibility of session hijacking. This thesis examines the usability of previously researched continuous security mechanisms that authenticate a user through their typing patterns, where the process is controlled by artificial immune system algorithms. In contrast to previous methods, the user is authenticated for each individually typed key. For experimentation, 94 participants' keystroke latency features from the Clarkson II free text dataset were extracted and divided into training, validation, and test sets. The filtered training set was used to generate detectors from negative, positive, and clonal selection algorithms. During validation and testing, the Manhattan distance between each keystroke and the closest detector was used to calculate a score. For each session tested with users and impostors, a quantified trust concept and variable threshold controlled session termination. The change in trust was controlled by the dynamic trust model using the calculated score from each keystroke. The results of the models created were measured in how many keys on average a genuine user (ANGA) and impostor (ANIA) could perform and the ratio between them. The best model achieved an ANIA of 177 and an ANGA of 1969 with a ratio of 11.12. Although the results did not achieve state-of-the-art performance, rendering the method currently less suitable for continuous authentication, the approach showed potential. It surpassed the results of earlier research that used artificial immune systems for keystroke dynamics in continuous authentication. Should future research address the potential improvements outlined in the discussion, it might achieve results comparable to, or better than, state-of-the-art performance.

GABRIELLA KIERULFF - FAIRNESS IN FACE RECOGNITION

Full Title: Enhancing Face Recognition Models with Synthetic Child Data: A Fairness Assessment
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Christian Rathgeb
Contact email: christoph.busch@h-da.de

Abstract:
Despite the widespread adoption of facial recognition technology in various applications, significant challenges persist in ensuring fair and unbiased performance across different age groups. These challenges are particularly pronounced in scenarios involving children, who are often underrepresented in training data sets, leading to biased algorithms that perform with higher accuracy on adults. This thesis investigates the enhancement of demographic fairness, particularly concerning children, in state-of-the-art face recognition models. It further seeks to align with a responsible development framework following the novel regulations for biometric identification systems in the EU AI Act and ISO/IEC standards. The research aims to address these issues by the bias mitigation technique of fine-tuning pre-trained face recognition models using synthetic images of children's faces. This approach seeks to mitigate bias while maintaining privacy. The thesis evaluates the fairness of these models using performance metrics, including the False Positive Identification Rate, False Negative Identification Rate, and the demographic fairness metric False Negative Differential. Performance is assessed across different age subgroups, categorising children into age ranges from 1 to 15 years and comparing these groups with adults. These insights contribute to enhancing fairness in face identification systems for children, suggesting that while fine-tuning on synthetic data improves the overall recognition performance for children, it does not enhance the demographic fairness of the face recognition system. To further the development of fair face recognition systems for identification, this thesis discusses alternative bias mitigation strategies, carefully balancing the trade-off between privacy and performance. These strategies are evaluated within the context of compliance with regulatory frameworks governing the field.

THOMAS NYREM EILIFSEN - MIMICKING THE STUDENT

Full Title: Mimicking the Student - A Feature-Based Approach for Detecting AI-Generated Texts and Verifying Authorship in Educational Settings
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
This thesis investigates the influence of advanced artificial intelligence (AI) language models on academic integrity, focusing on contract cheating. As AI capabilities like those seen in models like ChatGPT, Claude, and Gemini evolve, distinguishing between student-written and AI-generated texts becomes increasingly challenging. This research aims to evaluate the efficacy of AI detection tools and the use of students' historical writing patterns to identify AI-generated text, with the goal of ensuring the integrity of academic work. The research employs a feature-based approach with multiple machine-learning models to identify differences between human and AI-generated texts, focusing on features like sentiment, readability, complexity, and errors. A feature-based approach was chosen as the preferred method due to a better interpretability and understanding of what led to the models' decisions. The study achieved high accuracy in distinguishing AI-generated texts from human-written texts, the CatBoost Classifier performed the best with an F1-score of 0.9797. A Feature importance analysis highlighted the usage of paragraphs, spelling, and grammatical errors, as important for the models' decisions. The second part focused on verifying authorship to detect deviations from students' known writing styles, The approach again used a feature-based methodology, with multiclass and binary classification models to differentiate between authors and identify individual texts that may not fit with a student's usual writing pattern. The results for the authorship verification were mixed, with the models' being able to correctly classify some authors fairly constantly, and others rarely. This indicates that some authors have a distinct style that is easier to distinguish from others. When distinguishing specific authors from AI-generated texts, the models did very well, showing that this is a feasible task with the right models and features. The findings confirm the potential for implementing these models within educational frameworks to detect AI-generated content and verify authorship. The study has several limitations that need to be addressed, future work and continuous development are needed to keep pace with advancing AI technologies and develop more reliable methods.

ADRIAN SKROBAS - ESTIMATION OF DEPTH FACIAL REPRESENTATION IN SEQUENTIAL PRESENTATION ATTACK DETECTION

Full Title: Discriminative estimation of depth facial representation in sequential presentation attack detection
Institution: Wroclaw University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: wojciech.wodo@pwr.edu.pl

Abstract:
This paper presents research on the issue of presentation attack detection. Within the current state of the art, directions related to computer vision techniques that facilitate the acquisition and processing of data on face representation and depth have been identified. The commercial aspects of the sought-after biometric solution were analyzed. A sequential approach to presentation attack detection based on the gesture of moving the face closer to the camera was proposed. For the purposes of this work, an extensive dataset was prepared, consisting of several thousand biometric interactions characterized by bona fide presentations and presentation attacks using prints, masks, and screens. The research part focused on experiments related to estimating distance based on the size of the human iris and the fluctuations in facial structure based on changes in the length of tessellation edges. The conducted studies demonstrated significant benefits from the proposed approach. Satisfactory effectiveness in estimating the distance from the camera, averaging over 85%, was achieved. Changes in facial structure were covered in multi-planar studies using various machine learning techniques. Variants of models with an interaction classification accuracy above 99% were indicated. Some algorithm variants achieved error rates of APCER and BPCER close to zero. This work constitutes a significant contribution to the search for effective techniques for detecting presentation attacks, which can find their application in fields such as banking, public security or personal data protection.

AGNAR PÉTURSSON - VISUALIZATION OF IMAGE SIMILARITIES IN FACE RECOGNITION SYSTEMS

Full Title: Visualization of Image Similarities in Face Recognition Systems
Institution: Department of Informatics, University of Zurich
Supervisor: Manuel Günther
URL: https://seafile.ifi.uzh.ch/f/badc3baecae5474eb5d6/
Link description: Master thesis Agnar Pétursson
Contact email: guenther@ifi.uzh.ch

Abstract:
This thesis explores the application of Class Activation Mapping (CAM) methods, particularly Element-wise Grad-CAM, to visualize decision-making areas in a pre-trained ArcFace model used for facial recognition. This study aims to enhance the interpretability and trustworthiness of deep learning models by highlighting how these models process faces under various conditions, such as different orientations and occlusions. Initial experiments identified key focus areas, primarily the eyes and nose. Subsequent analyses explored the impact of occlusions like sunglasses and scarves, revealing the model's adaptability by shifting focus to available facial features. Furthermore, a comparison of model behavior across frontal and non-frontal views further evaluated its robustness, revealing differences in feature prioritization. The research also highlighted subtle differences in model focus based on gender, suggesting variations in feature prioritization. The study highlights the effectiveness of using CAM techniques to enhance the transparency of facial recognition systems. This is especially important for applications that require high levels of reliability. The research contributes to the broader goal of developing more interpretable AI systems.

HJALTE BØGEHAVE - MORPHING ATTACK DETECTION AND PRESENTATION ATTACK DETECTION

Full Title: Tinyml-enabled Morphing Attack Detection and Presentation Attack Detection
Institution: NTNU and DTU
Supervisor: Christoph Busch and Wassim Kabbani
Contact email: christoph.busch@ntnu.no

Abstract:
Face recognition has emerged as a widely adopted biometric technology, finding applications in various domains such as security, surveillance, and access control systems. The advancements in artificial intelligence (AI) and machine learning (ML) have significantly enhanced the accuracy and reliability of face recognition systems. However, the increasing sophistication of these systems has also given rise to novel security threats, particularly in the form of presentation attacks and morphing attacks. this research aims to develop efficient and optimized PAD and MAD techniques specifically tailored for embedded devices. The primary objectives are to explore model compression and optimization techniques, such as pruning, quantization, and attention mechanisms, to reduce the computational complexity and memory requirements of the models while maintaining high detection accuracy. Additionally, the research seeks to investigate the impact of environmental factors, such as lighting conditions and camera quality, on the performance of PAD and MAD algorithms in real-world embedded scenarios.

MARIUS NESSET - INVESTIGATING CLUSTERING AND DATA AUGMENTATION TECHNIQUES, FOR VICTIM-AGNOSTIC INTER-KEYSTROKE TIMING ATTACKS

Full Title: Investigating clustering and data augmentation techniques, for victim-agnostic inter-keystroke timing attacks

Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
We perform a fully victim-agnostic inter-keystroke timing attack, capable of recovering written words from press timings alone, without any prior knowledge of the victim's typing behaviour as has previously often been required. We test several standard and custom normalization and clustering techniques for this task, managing to recover words of length 3 to 10 with a top-10 accuracy of 45% and a top-1 accuracy of 10.83%. Lastly, we also try to recover the hold timings as a fraction of the press timings to try to augment our data further.

ANDREJ KRONOVŠEK - DEEPFAKE DETECTION USING ONE-CLASS LEARNING

Full Title: Deepfake detection using one-class learning
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Borut Batagelj
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=164243&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
As part of our Master's thesis, we set out to build a model that could detect deepfakes. In general, models for identifying deepfakes are better when they are trained on as many different datasets of deepfakes as possible that are generated by as many methods for generating them as possible because this means that they generalise better. However, our approach to achieving better generalisation is one-class, meaning we only use a class of real images to represent the problem. From these images, we create synthetic fake images using the Self-Blending Images method. Neural networks are generally not considered to be easily interpretable, so we added segmentation to the learning process. Our model labels the part of the face in the image that it assumes has been forged, and based on the correctness of this mask, the model learns to identify deepfakes. We evaluate the masks generated by our model on six datasets. We evaluate the classification of the model on the datasets on which the authors of other models also assess, and on average we obtain the best results.

HANS GEISSNER - UNIFICATION AND IMPROVED EVALUATION OF MULTIBIOMETRIC FUZZY VAULTS

Full Title: Unification and Improved Evaluation of Multibiometric Fuzzy Vaults
Institution: Hochschule Darmstadt
Supervisor: Christian Rathgeb
Contact email: christian.rathgeb@h-da.de

Abstract:
The fuzzy vault scheme as an instance of a biometric cryptosystem is able to provide biometric authentication while also protecting privacy. In combination with multibiometrics the fuzzy vault scheme can potentially be used for applications that require a high security level. While many approaches for constructing multibiometric fuzzy vaults have been proposed there is a lack of a method that guarantees a balanced contribution of the individual characteristics to the fuzzy vault. Moreover, the potential security level of most approaches could only be extrapolated due to empirical testing being conducted with a limited amount of non-mated comparisons. This work aims to achieve three objectives. Firstly, craft a unified framework for multibiometric fuzzy vaults, that is able to construct balanced fuzzy vaults using any combination of characteristics. Secondly, investigate whether it is possible to empirically measure high security levels of multibiometric fuzzy vaults using a limited dataset. Thirdly, evaluate the proposed approach in terms of accuracy and security. The first objective was addressed by proposing a unified framework created through the utilization of a generalized approach for feature transformation, and employing deep feature extractors known for generating feature vectors of consistent representation. The second objective was addressed by proposing a method that improves the multibiometric evaluation for l characteristics exponentially increasing the number of non-mated comparisons with l through means of creating virtual subjects. Finally to fulfill the last objective an empirical evaluation using a multibiometric dataset composed of face, fingerprint and iris samples was conducted. To determine if the proposed framework and evaluation methods effectively achieved their intended objectives, further experiments were conducted investigating the effect of feature transformation and the impact of the improved evaluation on the measurable security level.

MATHIAS ØVEREN ENGER - RANKING THE STARS

Full Title: Ranking the Stars - Combining Graph Theory and Fully Logic to Detect Cybergroomers
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
As children increasingly immerse themselves in the digital world, they face new risks different from those in the physical world. Unlike in the physical world, where people can see and verify the identity of the person they are speaking to, the digital world often allows individuals to disguise their true identities. This anonymity enables child predators to pose as minors, gaining the trust of unsuspecting young users and ultimately exploiting them sexually. The rise in such malicious activities underscores the urgent need for effective detection and prevention mechanisms, with early detection being crucial to intervene before harm occurs. In this thesis, we have tackled the challenge of early cybergrooming detection by integrating graph theory with fuzzy logic to analyze user behavior in an action-based ranking system. We created a decision tree built on the principles of fuzzy logic, which serves as an analysis tool for every interaction a user is involved in. For every interaction, the user's risk score is updated, allowing for continuous assessment. This system allows us to dynamically rank users, with those exhibiting the most predatory behavior receiving the highest risk scores and being ranked near the top. The result of this study is that continuous analysis of user behavior is effective in detecting unwanted users such as sexters, spammers, and sexual predators. Our system can rank the majority of these users among the top ranks, effectively highlighting those who exhibit the highest risk based on their interaction patterns. This system also opens up numerous opportunities for future research. Integrating conversation analysis with behavior analysis may further enhance the system, which could enable a more comprehensive understanding of user interactions.

ANASTASIJA MANOJLOVSKA - INTERPRETING FACE RECOGNITION TEMPLATES USING SYMBOLIC REPRESENTATIONS

Full Title: Interpreting face recognition templates using symbolic representations
Institution: University of Ljubljana, Slovenia
Supervisor: Vitomir Štruc, Klemen Grm
URL: https://repozitorij.uni-lj.si/Dokument.php?id=190517&lang=slv
Link description: University repository
Contact email: vitomir.struc@fe.uni-lj.si

Abstract:
As the field of Artificial Intelligence (AI) is gaining popularity, there is an increasing demand for making the decisions of AI systems transparent and understandable. Explainable Artificial Intelligence (XAI) is an emerging field, which aims to address the "black box" challenge in deep learning architectures and make the processes that lead to the decisions more explainable/interpretable to humans. It is particularly important to make the AI systems more transparent due to various legal regulations, such as the General Data Protection Regulation (GDPR), which requires the AI systems to be not only accurate, but also explainable/interpetable. This is specifically relevant in scenarios where the AI system has to make decisions about a person's identity, since the wrong verdict might have huge consequences. In this thesis, we use symbolic representations to interpret the encoded facial attribute information in face templates, which are easier to understand by non-experts in this field. To achieve this goal, two strategies are developed. First, we employ the CLIP model to generate natural language descriptions of the extracted face templates. The face templates are initially generated with CLIP's Image Encoder. We further implement state-of-the-art face recognition and face analysis models AdaFace and SwinFace as the backbones to extract face templates, which we later interpret using CLIP's Text Encoder. The differences in these architectures allow us to analyze the impact they have on the encoded information content. The second strategy involves implementing the AdaFace and SwinFace models as the backbones to binary and multi-label classifiers to predict the presence of the facial attributes, such as "Male", "Young", "Attractive", "Brown_Hair", "Wearing_Hat", etc. in the extracted face templates. By using this approach we aim to represent the encoded information content using very basic symbolic representatons. Moreover, this strategy serves as a baseline for the CLIP-based models, to which we compare the performance. We further fine-tune and evaluate various model variants using the VGGFace2 dataset and the annotated attribute labels from the MAADFace dataset. The results indicate that fine-tuning the CLIP model on a domain-specific task improves its ability to better represent the information encoded in face templates and align encoded text descriptions with these templates, which allows for natural language interpretation. Furthermore, the results show that SwinFace outperforms AdaFace both in the CLIP-based and classification approaches, indicating that SwinFace is more effective at encoding the attribute information in the extracted face templates. Moreover, neither of the CLIP-based models outperform the baseline classifiers.

JONAS PEDERSEN - FACE IMAGE QUALITY

Full Title: Motion Blur Estimation for Face Image Quality Assessment
Institution: NTNU and DTU
Supervisor: Christoph Busch and Wassim Kabbani
Contact email: christoph.busch@ntnu.no

Abstract:
Face Recognition Systems are increasingly integral to personal and large-scale security applications, requiring robust mechanisms to ensure reliability. A critical aspect of Face Recognition Systems performance is the quality of captured face images, with motion blur being a reason for degraded recognition performance, stemming from capture subject movement or poor illumination. To address this, Face Image Quality Assessment quality assessment algorithms are employed to evaluate quality components to estimate the utility of face images for Face Recognition Systems. The ISO/IEC DIS 29794-5:2024 standard proposal describes several quality components and their corresponding quality assessment algorithms but also lacks defined quality assessment algorithms for some quality components, including motion blur. This thesis focuses on developing and evaluating Face Image Quality Assessment quality assessment algorithms for estimating the motion blur intensity in face images with both real and synthetic motion blur. This has been done utilizing both classic computer vision and machine learning approaches. The results achieved for motion blur intensity estimation using the classic computer vision method indicate that the implementation is inadequate, performing worse than a general sharpness measure. Conversely, the classic computer vision method for motion blur direction estimation shows promising results on the Essen Darmstadt Motion Blur (EDAMB) dataset, although it lacks ground truth labels. Over 500 machine learning models were fine-tuned for the machine learning method as part of hyperparameter tuning, combining several different base models and input transformations. Among these, a configuration using the DenseNet169 base model, with the alias densenet_jp_p1, demonstrates the best balance of complexity and predictive performance.

MUHAMMAD HASEEB KAMAL - DEFENDING FACE IMPERSONATION DETECTORS AGAINST ADVERSARIAL ATTACKS

Full Title: Defending Face Impersonation Detectors against Adversarial Attacks
Institution: Hochschule Darmstadt
Supervisor: Mathias Ibsen, Lazaro Janier Gonzalez-Sole, Christian D. Jensen, Christoph Busch
Contact email: mathias.ibsen@h-da.de

Abstract:
Face recognition systems are a popular choice for biometric authentication. However, they are known to be vulnerable to presentation and morphing attacks. To mitigate security risks of these attacks, face impersonation detectors for detecting presentation or morphing attacks are deployed in conjunction with face recognition systems. However, since these detectors are based on deep neural networks they are prone to another class of attacks known as adversarial attacks. The vulnerability of face impersonation detectors against adversarial attacks is not well-researched. This thesis aimed to assess this vulnerability through a variety of black-box adversarial attacks. The thesis also investigated the impact of the impersonation attacks on multiple face recognition systems before and after the adversarial attacks were applied to fool the impersonation detectors. A secondary aim was to evaluate defence mechanisms to mitigate the risk of adversarial attacks. It has been shown through experimental results that both presentation attack detectors and morphing attack detectors are vulnerable to query-based black-box attacks. In this regard, morphing attack detectors have been shown to be more vulnerable to adversarial attacks than the tested presentation attack detectors. The vulnerability of face recognition systems against attacks has also been shown. These vulnerabilities have been shown through analysis of various standardised metrics such as detection equal error rates and impostor attack presentation accept rates. Following this, it has been shown that both detector types can be defended against the attacks with varying success rates. To this end, defensive distillation was used on the presentation attack detectors while adversarial training was used on the morphing attack detectors. The former in this case led to a greater increase in model robustness.

FRANCK VIOREL SOUOP KOUAM - FACE RECOGNITION FOR CHILDREN

Full Title: Face Recognition for Children
Institution: Hochschule Darmstadt
Supervisor: Christian Rathgeb
Contact email: christian.rathgeb@h-da.de

Abstract:
In a digitized society, biometric systems are gaining increasing importance and are being applied in various fields of application. Facial recognition technology has established itself as one of the most prominent methods for personal identification due to its non-invasiveness and ease of application. Despite significant advances in this area, the reliable identification of children, especially in forensic scenarios, remains a challenging task. Existing facial recognition systems, which are mainly designed for adult recognition, reveal weaknesses in identifying children. This master's thesis therefore explores the potentials and challenges of retraining facial recognition models for the specific recognition of children through the use of synthetic datasets. The aim is to improve the performance of these systems and to examine their adaptability to the unique characteristics of children's faces. The results show a significant increase in recognition accuracy after fine-tuning existing models, thereby highlighting the potential of synthetic datasets in biometric research. This work thus contributes to increasing the efficiency and reliability of facial recognition in children and offers important impulses for the further development of this technology in security-critical and forensic contexts.

HONGZHI XIE - PORTING HLBS FROM THE SOAP PROTOCOL TO THE REST PARADIGM

Full Title: Porting High Level Biometric Services (HLBS) from the SOAP Protocol to the REST Paradigm
Institution: TU Darmstadt
Supervisor: Olaf Henniger, Arjan Kuijper
Contact email: olaf.henniger@igd.fraunhofer.de

Abstract:
The Bundesamt für Sicherheit in der Informationstechnik (BSI) Technical Guideline TR-03121-2-2 [10] specifies a web service called High Level Biometric Services (HLBS) that provides a high-level web service interface using the Simple Object Access Protocol (SOAP) protocol, which aims at reducing the programming effort required to integrate biometric workflows into applications. However, the Representational State Transfer (REST) paradigm offers a leaner, more flexible alternative to SOAP. Therefore, this work explores the porting of the HLBS from the SOAP protocol to the REST paradigm, which includes designing an improved RESTful web service interface, developing a proof-of-concept prototype, and evaluating the benefits and drawbacks of using the RESTful specification.

TEAKOSHEEN JOULAK - FACE IMAGE QUALITY ASSESSMENT

Full Title: LandmarkAgnostic Face Image Quality Assessment
Institution: NTNU and DTU
Supervisor: Christoph Busch and Wassim Kabbani
Contact email: christoph.busch@ntnu.no

Abstract:
This thesis conducts a literature review of landmarkdependent and landmarkagnostic face image quality assessment, including face detection, face alignment, face segmentation, landmark localization, and Facial Image Quality Assessment Measures. The primary focus of the research is a comparative analysis between the landmark agnostic approach, represented by the faceparsing method, and the landmark-dependent approach, represented by the Dlib method. The evaluation involves measuring various quality components, such as head length, head size, intereye distance, eye open, mouth closed, and crop of the face image. In addition, a novel heuristic function for computing head length is proposed and tested under various resolutions. The results of the comparative analysis, heuristic function testing, and their addressing of the research questions are presented through illustrative diagrams. The thesis concludes with suggestions for addressing limitations and outlines potential future work.

YUJING GU - FACE IMAGE QUALITY ASSESSMENT

Full Title: LandmarkAgnostic Face Image Quality Assessment
Institution: NTNU and DTU
Supervisor: Christoph Busch and Wassim Kabbani
Contact email: christoph.busch@ntnu.no

Abstract:
This thesis conducts a literature review of landmark dependent and landmark agnostic face image quality assessment, including face detection, face alignment, face segmentation, landmark localization, and Facial Image Quality Assessment Measures. The primary focus of the research is a comparative analysis between the landmark agnostic approach, represented by the faceparsing method, and the landmark dependent approach, represented by the Dlib method. The evaluation involves measuring various quality components, such as head length, head size, intereye distance, eye open, mouth closed, and crop of the face image. In addition, a novel heuristic function for computing head length is proposed and tested under various resolutions. The results of the comparative analysis, heuristic function testing, and their addressing of the research questions are presented through illustrative diagrams. The thesis concludes with suggestions for addressing limitations and outlines potential future work.

MICHÈLE FUNDNEIDER - DEMOGRAPHIC BIAS IN FACE RECOGNITION

Full Title: Demographic Bias in Face Recognition: Evaluating WERM Fairness Metric and Balancing Strategies
Institution: Department of Informatics, University of Zurich
Supervisor: Manuel Günther
URL: https://seafile.ifi.uzh.ch/f/19778e7143c249949315/
Link description: Master thesis Michèle Fundneider
Contact email: guenther@ifi.uzh.ch

Abstract:
Recent advancements in deep Face Recognition (FR) systems have demonstrated remarkable accuracy, yet these systems often suffer from demographic biases. A system exhibits demographic bias if there are noticeable performance disparities across various demographic groups, including ethnicity, age, or gender. Common training datasets, such as VGGFace2, are highly imbalanced concerning demographic groups, leading to biased systems. This thesis aims to analyze the stability of a state-of-the-art fairness metric called Worst-case Error Rate to the Geometric Mean (WERM) and to enhance demographic fairness by employing different balancing techniques and evaluating the model's fairness. The WERM metric calculates the maximum error rate divided by the geometric mean of error rates across all groups, using a small epsilon value to prevent division by zero. Thus, the metric can be sensitive to this epsilon. We first analyze the WERM on different validation set sizes and on different epsilon values. We then assess the fairness and accuracy of a pre-trained model. Finally, we propose different balancing techniques, such as undersampling by identities, undersampling by images, weighted loss by demographic class-balanced loss, group-specific focal loss, and adjustments of hyperparameters in the ArcFace loss. Our results show that the WERM metric is highly sensitive to the number of image pairs in the validation set and the small epsilon chosen to avoid division-by-zero errors. As the number of pairs increases and with a larger epsilon value, the WERM results stabilize. The results from our balancing techniques show that most methods do not effectively reduce the WERM. Undersampling by identities and the class-balanced loss demonstrate the most promising results. Overall, this thesis highlights the challenges in measuring and mitigating demographic biases in FR systems, providing a foundation for future research aimed at developing more equitable and robust FR models.

ANNA SCHIBELLE - FACE MANIPULATION DETECTION

Full Title: Towards Generalised Face Manipulation Detection for digital and physical Impersonation Attacks
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Christian Rathgeb
Contact email: christoph.busch@h-da.de

Abstract:
Biometric systems play an essential role in our daily lives, using biological and behavioural characteristics to identify individuals. FaceID and fingerprint scanners, integrated into most smartphones, are examples of such systems. This thesis focuses on the task of Face Recognition, which verifies an individual based on their facial image. However, these tools are vulnerable to various attacks, including morphing, face swapping, and makeup attacks. Two methods exist to detect these attacks: noreference and differential detection. While several noreference methods have been proposed to detect digital and physical manipulations, fewer differential detection methods are available. Unfortunately, many of these methods lack generalization capabilities and are biased towards the attacks they were trained to detect. In Ibsen et all 2023, the authors propose a differential detection framework that utilizes anomaly detection models to detect facial manipulations, showing promising results. This thesis builds upon their framework by evaluating its performance with different backbone sizes and types of anomaly detection models. Additionally, the thesis applies explainability to the framework to gain insight into the decision-making process of the applied manipulation detection method, aiding the detection process. Based on the results obtained, the size of the backbone significantly impacts the framework's detection capability. Additionally, a subset of anomaly detection methods has proven suitable for identifying face manipulations. As for the differential anomaly detection framework's explainability aspect, the outcomes suggest that there is potential for aiding the framework with explainability. However, more research is necessary before it can effectively assist in the detection process.

YASSER HMOUDA - FINGERMARK IMAGE QUALITY ASSESSMENT METHODOLOGY

Full Title: Fingermark Image Quality Assessment Methodology
Institution: Fraunhofer IGD
Supervisor: Arjan Kuijper, Olaf Henniger
Contact email: olaf.henniger@igd.fraunhofer.de

Abstract:
Latent fingerprints, also named fingermarks, are important tools to identify criminals, they are mainly used by law enforcement and forensic agencies. Processing latent fingerprints can be tedious and time-consuming. Identifying criminals requires comparing their fingerprints with the found latent fingerprints, but only the ones with an extremely high quality can result in a conclusive match. Therefore, our goal is to use modern machine and deep learning techniques to calculate quality scores for latent fingerprints using different approaches to serve different purposes. We trained different models and used different labels depending on the definition of quality. We calculated quality scores depending on how well the latent fingerprints compare to their references. We computed other quality scores, considering how badly they compare to non-mated fingerprints. Furthermore, we assessed the quality of a latent fingerprint depending on the minutiae characteristics of the print. We calculated these metrics using the classical machine learning approach to be able to simultaneously assess the predictive utility of used features. In addition, we propose models that classify the latent fingerprints into multiple classes indicating whether they have value for identification or have no value for the experts, this will help create databases in the future with high quality to use as baseline either in other research topics or for forensic experts.

ZBYNĚK LIČKA - REVERSIBILITY OF VOICE CHANGE METHODS

Full Title: Reversibility of Voice Change Methods
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/150236
Contact email: ilicka@fit.vut.cz

Abstract:
State-of-the-art voice-changing methods allow inexperienced users to create convincing voice recordings of famous individuals with just a few seconds of recorded speech. There are two major approaches to voice generation: voice conversion and text-to-speech. Voice conversion methods require the user to input source speech to be converted to the target voice. A trend with voice conversion methods, especially those requiring only mere seconds of reference speech, has been restricting the amount of information about the original speaker in the converted speech. This work focuses on studying the amount of information extractable about the original speaker from artificial speech and potentially reconstructing the original speech. The results of this work shed light on an unstudied property of voice-changing methods.

ROBERT NICHOLS - DIFFERENTIAL MORPHING ATTACK DETECTION

Full Title: A Composite Framework for Context-Based Data in Differential Morphing Attack Detection
Institution: Hochschule Darmstadt
Supervisor: Christoph Busch and Christian Rathgeb
Contact email: robert.nichols@h-da.de

Abstract:
Morphing attacks in the border control scenario remain a threat to public security. This makes them an area of continued significant scientific interest. This work addresses one of the main limiting factors in biometric machine- and deep-learning research, specifically morphing attack detection: the lack of available, high-quality, and accurately labeled data spanning up to 10 years of sample age intervals. To this end, a novel data collection approach is proposed that integrates multiple state-of-the-art computer vision and natural language processing models with technologies that constitute the World Wide Web, with the primary data source being live and archived news programs from German public television, and accurate labeling supplied by large-scale public knowledge graphs. State-of-the-art image morphing methods are applied to create a contemporary database for developing novel morphing attack detection systems. Additionally, using this new database, a preliminary novel approach to morphing attack detection is explored that follows recent findings from the object detection task, which incorporates additional information to boost detection performance. The results indicate a potentially fruitful interdisciplinary research area and promote a multi-modal view of traditionally unimodal vision tasks.

NAFEEZ HOSSAIN - KEY REGIONS, GRAPHS, AND IDENTITY

Full Title: Key Regions, Graphs, and Identity - Grouping Behavior Patterns to Unravel Shared Accounts
Institution: NTNU
Supervisor: Patrick Bours and Nima Farajian
Contact email: patrick.bours@ntnu.no

Abstract:
Account sharing has become a common occurrence in today's age of digital services, posing particular difficulties for user identification and services catered towards particular users. Conventional authentication classifiers frequently miss the subtle problems brought by account sharing since they are built mostly on general behavior biometrics. This negligence may lead to system vulnerabilities, especially in high-security settings like financial institutions and banks. If the classifiers are trained without taking account sharing into consideration, then they could model user behavior incorrectly, thus confusing shared account activities for the actions of specific users. This weakness in the authentication system may result in security breaches in sectors where the importance of integrity is paramount. Therefore, it is essential to include techniques to identify accounts for shared usage. This modification will provide a more reliable and secure framework for authentication, particularly in high-stakes situations when user identity precision is crucial. In addition to improving security, addressing account sharing will also bolsters the system's dependability and credibility. This thesis presents a novel approach for utilizing keystroke dynamics to identify account sharing. By converting keystroke log data into graph structures and adding keyboard regions as nodes and consecutive press times between nodes as edges, the study effectively addresses the issues with not having exact key press data. This graph-based approach allows for a more comprehensive analysis of keystroke dynamics compared to traditional tabular data formats for this specific case. The key contributions of this thesis include the exploration of different implementations of graph neural networks (GNNs), developing a method for graph translation of session log data, and applying feature engineering approaches to improve the recognition of distinct behavior patterns. The work illustrates the unified usage of machine learning and graph-based approaches, despite certain restrictions in the consideration of edge properties in GNN representations for keystroke dynamics. The creation of fixed-size vector embeddings of the graph data using an Autoencoder is a crucial component of this study as the model learns to preserve the original data and opens up a way to spot unique behavior patterns. Assessment measures, such as the Silhouette score, Calinski–Harabasz index, Within Cluster Sum of Squares, Davies-Bouldin Index and Dunn Index are used to quantitatively evaluate the process once it has been verified using a variety of classifiers and clustering algorithms. A scoring system is also developed that will help with detecting shared accounts based on the parameters set by our observation on behaviour of shared accounts. In situations when just keyboard region information is available, the results clearly show that behavior biometrics—specially keystroke dynamics, can be a powerful technique for identifying account sharing. Our study suggests improvements of established user identification systems based on keyboard dynamics and defines a unique basis for future research in this field.

MAGDA PYCHTJAROW - ENHANCING KEYSTROKE DYNAMICS MODELING

Full Title: Enhancing Keystroke Dynamics Modeling: Evaluating the Impact of Advanced Architectural Components and Key Code Transformation
Institution: Leiden University
Supervisor: Nele Mentens and Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
In light of the growing demand for robust and seamless authentication methods, biometric-based authentication has emerged as a promising direction for development. Combining this approach with advancements in deep learning techniques, keystroke dynamics-based authentication systems have shown significant potential. However, research into deep learning methods is often complex and frequently fails to provide clear insights into the influence of individual model components. This study aims to explore the impact of architectural decisions and key code feature processing, demonstrating how these factors affect performance.

FLORIAN BAYER - ADAPTIVE MULTI-MODAL BIOMETRIC TEMPLATE PROTECTION USING FHE

Full Title: Adaptive Multi-Modal Biometric Template Protection using Fully Homomorphic Encryption
Institution: Hochschule Darmstadt
Supervisor: Christian Rathgeb
Contact email: christian.rathgeb@h-da.de

Abstract:
Mobile devices have become ubiquitous in our daily lives. They are used for a variety of tasks, ranging from communication to entertainment. In addition, mobile devices are increasingly used for storing valuable personal information. Biometric authentication is a promising approach to increase the security of stored secrets while maintaining a high level of usability. However, biometric data is sensitive and must be protected. Homomorphic encryption is a promising approach to protect biometric data because it allows to perform computations on encrypted data without decrypting it. This thesis is concerned with the extension of a homomorphic encryption scheme for multi-biometrics to support adaptive verification. The implementation was evaluated in terms of biometric performance, computational performance as well as privacy. Our results show that the proposed extension combines the security advantages of storing extracted features concatenated with the flexibility to adapt the verification threshold at runtime in order to to spare the user unnecessary modality presentations for actions that only require a modest level of security. Our contribution therefore improves both usability and computational performance of biometric authentication in the mobile scenario.

SILJE BJØRNSTAD MARTINSEN - DETECT CYBER GROOMING IN CONVERSATIONS LOGS

Full Title: Detect cyber grooming in conversations logs
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
Detecting cyber grooming in messages is a critical challenge that requires precise and reliable methods to identify subtle and context-specific behaviours. This project develops a machine learning pipeline to detect grooming patterns in textual data by using five pre-trained models: K-Nearest Neighbors with TF-IDF, Neural Networks with TF-IDF, Multinomial Naive Bayes with TF-IDF, Multinomial Naive Bayes with binary word features, and Support Vector Machines with TF-IDF. The program processes messages using overlapping chunks to preserve contextual continuity, calculates predictive metrics such as confidence and binary crossentropy loss, and flags high-confidence predictions for further review. The project identifies the best-performing method by evaluating models on labeled datasets while emphasizing interpretability and scalability. The results highlight the effectiveness of probabilistic and similiar models in detecting conversational patterns. Future work includes refining the labeling process and explore the models in more detail to improve the performance metrics.

JAN-SIMON KÖHNKE - ADAPTION OF CYBERGROOMERS

Full Title: Adaption of cybergroomers - How predators digitally optimize their behavior
Institution: NTNU
Supervisor: Patrick Bours and Peter Valderhaug
Contact email: patrick.bours@ntnu.no

Abstract:
Cybergrooming is a major social problem that knows no national boundaries and is increasing with the growth of digital communication. This makes research into the detection of cybergrooming more important to identify perpetrators at an early stage and protect victims. Cybergroomers use chat conversations to build a relationship of trust with their victims with the goal of abusing them digitally or in person. This thesis attempts to contribute to our understanding of how these perpetrators use these manipulative techniques to achieve their goal. Two concepts of neuro-linguistic programming, mirroring and matching as well as pacing and leading, are considered and examined to see if and how cybergroomers practice these techniques in chat conversations with their victims. The methodological approach entails the analysis and preparation of chat data from Perverted Justice, with the application of natural language processing techniques. The findings indicate that a considerable number of cybergroomers exhibit behavioral patterns that align with the techniques of mirroring and matching, as well as pacing and leading. Furthermore, it was determined that the cybergroomers employed these techniques throughout the entirety of the analyzed chat logs. It was determined that the utilization of emoticons and emotional expressions serves as an indicator of mirroring behavior. In contrast, the analysis of pacing and leading revealed the use of combinations of N-grams with keywords, which provided insights into the manipulative strategies employed by cybergroomers. These findings have the potential to inform the development of more effective detection methods for cybergrooming.

SUSAN BABU PANDEY - AI TOOLS FOR TATTOO IMAGE SYNTHESIS

Full Title: AI Tools for Tattoo Image Synthesis
Institution: Technological University of Denmark
Supervisor: Prof. Dr. Christian Rathgeb and Dr. Lazaro Janier Gonzalez-Soler
Contact email: lazaro-janier.gonzalez-soler@h-da.de

Abstract:
Tattoos have long been used as complementary information to support the identification of subjects in forensic investigations. This is mainly due to their discriminative patterns and designs, which are valuable in identifying individuals. However, privacy concerns surrounding the collection of real tattoo databases have hampered the development of robust tattoo recognition systems in the past. With recent advances in generative neural networks, it is possible to generate synthetic tattoos, opening up new research directions. In the thesis, a framework called GenInk for the generation of synthetic tattoos based on an existing multimodal generative model is proposed. To the best of our knowledge, GenInk enables the generation of the first fully synthetic tattoo database that can be used for training tattoo recognition. Experimental evaluations on real tattoo databases show promising results, i.e., rank-1 identification rates above 95%, when using the proposed synthetic database for training in an identification task.

KRISTIAN HAVSTEIN - SANDBOXING PREDATORS USING OPEN-DOMAIN CONVERSATIONAL MODELS

Full Title: Sandboxing Predators Using Open-Domain Conversational Models
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
This thesis examines the feasibility of utilizing Large Language Models to prevent predatory behavior in online chat platforms. We fine-tune a state-of-the-art open-domain chatbot model using a predatory conversation dataset and modify the ParlAI framework to dynamically create memory augmentations from predatory conversation contexts. We randomly select a set of predatory conversations from the dataset and generate victim imitations. These are used in a questionnaire where we ask study participants to detect imitations in genuine and victim imitation conversations. We measure performance using the Imitation Rate and Imitation Ratio. Results indicate that our custom model achieves a mean Imitation Ratio of 79.6% in the first 16 conversation turns. Recent research developments and increased high-performance pretrained model availability suggest that future imitation performance will likely improve significantly. New international AI regulation efforts may, however, preclude our proposed solution to the online grooming problem.

LASSE MIKALSEN - DETECTING PARTIAL CONTRACT CHEATING

Full Title: Detecting partial contract cheating - A rolling attribution based approach for detecting partial contract cheating and verifying authorship in an educational context
Institution: NTNU
Supervisor: Patrick Bours
Contact email: patrick.bours@ntnu.no

Abstract:
This study combines stylometry and machine learning methods to determine whether parts of a text have been contract cheated. It explores the performance of different machine learning models, the impact of choosing the correct characteristics from the text, and a method that samples the text using a technique called rolling attribution. The research aims to provide a feasible method to increase the chances of a student getting caught when using contract cheating and, as such, preserve the integrity of academic work. This was achieved by developing three treatment designs, where the two first provided a baseline to which the third could be compared. The final experiments were run on 124 students individually to evaluate the rolling attribution method with and without partial contract cheating. The study shows that the machine learning models support vector machine and logistic regression, utilizing lexical and syntactic text characteristics, successfully identify text containing partial contract cheating 71% of the time. Additionally, it also measures the success rate when it cannot accuse a non-cheating student of cheating. This results in the method detecting a partial contract cheating text 10% of the time. These detection rates could increase the probability of a cheater being caught. By increasing the probability of detection, the perceived risk associated with partial contract cheating rises, potentially discouraging students from engaging in it. The study also discovers areas for improvement, both in the rolling attribution technique and in the relationship between the rolling attribution parameters and performance. It discovers that there is no relationship between the rolling attribution parameters and the performance, which was not expected. Additionally, it discovers that the rolling attribution technique, which, combined with the machine learning method, has a design flaw that causes misclassification. The study presents solutions and highlights the necessary development needed within the field to withstand more advanced contract cheating techniques, i.e., using artificial intelligence tools.

MARTA ROBLEDO-MORENO - FEDERATED LEARNING FOR MORPHING ATTACK DETECTION

Full Title: Federated Learning for Morphing Attack Detection
Institution: Universidad Autonoma de Madrid
Supervisor: Guido Borghi
Contact email: marta.robledo@uam.es

Abstract:
Face recognition systems are widely used for enhancing personal and public security, particularly at international border controls where they are employed for identity verification. These systems still face significant challenges from sophisticated digital attacks that exploit their vulnerabilities. One notable form of such attacks is Face Morphing, which uses digital manipulation methods to merge facial features of multiple individuals into a single composite image. This technique can lead to confusion regarding individual identities, which may allow unauthorized individuals to bypass security checks or pretend to be someone they are not. This Master's Thesis explores the use of Federated Learning (FL) to enhance Morphing Attack Detection (MAD) and protect the integrity of face recognition systems against deceptive practices. This research is motivated by the dual need to improve MAD's accuracy and to comply with the increasingly stringent privacy regulations governing biometric data. Traditional centralized learning approaches, while effective, centralize sensitive information, raising privacy and security concerns. Federated Learning, by contrast, offers a promising solution by decentralizing the learning process, allowing data to remain local while contributing to a global Machine Learning model. This study thoroughly investigates the feasibility and efficiency of employing FL for Morphing Attack Detection. The findings of this study demonstrate that FL can not only match but, in specific configurations, exceed the performance of centralized learning models in detecting morphing attacks. This superior performance of FL in certain scenarios underscores its potential to revolutionize MAD and, by extension, the security of facial recognition systems. Moreover, this research provides insights into the selection of appropriate face detectors and deep neural network architectures for maximizing MAD's detection accuracy. It highlights the scalability and effectiveness of FL in biometric security, suggesting a shift towards more secure, efficient, and privacy-preserving development methodologies. In conclusion, this Master's Thesis not only validates the feasibility of employing Federated Learning for Morphing Attack Detection but also sets the stage for further exploration into its application across other areas of biometric security. The promising results invite future research into advanced model architectures, data privacy techniques, and the broader implications of FL in securing digital identities against sophisticated threats.

ZONGJIAN LI - EFFECT OF IRREGULARITIES OF PROBE IMAGES ON FACE VERIFICATION PERFORMANCE

Full Title: Effect of irregularities of probe images on face verification performance
Institution: TU Darmstadt
Supervisor: Olaf Henniger, Arjan Kuijper
Contact email: olaf.henniger@igd.fraunhofer.de

Abstract:
This study investigates the effect of probe image irregularities on face verification performance. Although face verification has been widely adopted in various fields such as border control, mobile phone unlocking, and corporate attendance, the technology still has considerable room for improvement. The primary objective of this research is to analyze how different irregularities, including facial expressions, illumination and head angle yaw, impact the final performance of face verification. A mixed-methods approach was employed to achieve the research objectives. The experimental goal was accomplished by analyzing changes in comparison scores under different irregularities. The findings reveal that "Neutral" facial expressions yield the highest comparison scores, while "Scream" results in the lowest. A significant negative linear relationship was observed between the absolute value of head angle yaw and comparison scores. Additionally, certain OFIQ components showed correlations with comparison scores. Based on the model and comparison score assumptions, this study offers practical suggestions for managing irregularities in various face verification scenarios and provides valuable insights for future research on the impact of irregularities on face verification performance.

JESPER BLAK - MORPHING ATTACK DETECTION

Full Title: Morphing Attack Detection respecting Face Attractiveness
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Juan Tapia
Contact email: christoph.busch@h-da.de

Abstract:
In modern society, facial recognition has become more prevalent. Its uses include automatic border control and verification of documents without human oversight. For this reason facial recognition has become a more attractive target for cyberattacks. One such attack targeting face recognition, is known as morphing attacks. Morphing attacks consist of generating a morphed image, which is sufficiently close to multiple different people's facial biometric data. Thus allowing several people to use the same image for verification. To combat morphing attacks, there is a need for automatic detection of morphed images. In this project, we displayed a correlation between images being morphed, and the perceived beauty of those images. This is due to mathematical averagelooking faces being more attractive, and morphing techniques averaging out the facial features of the images being morphed. Using this tendency of morphing techniques, a new method for detecting morphed images was created, by combining a convolutional neural network trained on beauty scores of images, together with an existing differential morphing attack detection method. The performance analysis of this new method shows that facial beauty information has the potential to improve existing morphing attack detection methods. Currently, this method has some problems which need to be addressed before it can outperform existing methods. With clear shortcomings of the new method related to more challenging optimization, and difficulty handling morphing methods which does not attempt to reduce artifacts in the morphed images.

LINH NGUYEN - EXPRESSION NEUTRALITY ESTIMATION

Full Title: NeutrEx-Lite: Efficient Expression Neutrality Estimation For Utility Prediction
Institution: Hochschule Darmstadt
Supervisor: Christoph Busch and Marcel Grimmer
Contact email: christoph.busch@h-da.de

Abstract:
Face recognition systems have many useful applications in real life scenario, such as authentication for personal devices, border control at airports or attendance control for classrooms or institution. For these use cases, it is important for the system to achieve high recognition performance while still be able to process a large amount of transactions. To ensure that low quality images do not negatively contribute to the biometric performance, a method to quantify the quality of images taken from biometric samples is highly desirable. The current draft international standard of ISO/IEC 29794-5 introduces the concept of component quality, which quantitatively expresses the quality of a given biometric sample. In this work, we look into NeutrEx - a recently proposed quality measure which quantifies the expression neutrality of facial images in the context of ISO/IEC 29794-5. Additionally, we optimize the NeutrEx model to achieve better efficiency with regard to number of parameters, storage space, and inference time. Our proposed model NeutrEx-lite is intended to be a more streamlined version of NeutrEx, such that it becomes more suitable for real life applications, while still maintain respectable performance relative to the original one. In order to achieve this, we research well-known methods in the field of neural network optimization; such as pruning, quantization and knowledge distillation and apply them to NeutrEx.

EWALD MEIER - HUMAN DETECTION OF SYNTHETICALLY GENERATED FACE IMAGES

Full Title: Human Detection of Synthetically generated Face Images
Institution: Hochschule Darmstadt
Supervisor: Christian Rathgeb
Contact email: christian.rathgeb@h-da.de

Abstract:
The rapid development of generative AI, especially in the area of image generation, brings many benefits to the general public. But all these benefits come at a price. As the generated images become more realistic and thus harder to distinguish from the real ones, they also become more widely available through many free and easy-to-use online tools. This increases the danger these fake images pose to the general public. This creates the need for a countermeasure to mitigate these dangers. This thesis seeks to provide such a countermeasure in the form of a comprehensive guideline that can be easily applied by the general public. In addition, a diverse dataset of fake images needs to be created to provide a foundation for this study and to allow for further studies in this area. This led to the following two research questions, which will be answered in the course of this thesis. „What should a dataset of fake images look like in order to test the performance of humans in detecting them, considering different easy-to-use tools and diversity of the dataset?“ and „How does a guideline for humans look like to improve their performance in detecting fake images?“. In order to answer these questions, the landscape of currently available online tools that allow the creation of fake images is first assessed using a total of 7 defined criteria. Then, 4 of the best performing tools are selected to create the dataset. To ensure a diverse dataset, the images created are evenly distributed across 2 genders, 4 age groups, and 4 ethnicities. Real images are also introduced into the dataset for comparison to and thus allow the dataset to be used in research. Finally, all images are processed to have the same style to shift the focus to the content of the images alone. This dataset is then analyzed to find any anomalies that indicate a fake image. This is used to create the guidelines. The resulting dataset confirmed the potential dangers that these online tools pose to the general public, as these images are in large part indistinguishable from real images at first glance. The results suggest that some of the fake images are even preferred by people over real images, which is consistent with the current state of research. However, the guidelines created in this thesis provide a viable countermeasure to this danger, as they offer a classification accuracy of over 90% and are easy to apply, as they guide the user through the entire image analysis process without requiring any prior knowledge.

MONITOR
BACHELOR-THESES

ANA ARNEŽ - TOOLKIT FOR ANALYSIS AND ENHANCEMENT OF FINGERMARKS IN FORENSIC INVESTIGATIONS

Full Title: Toolkit for analysis and enhancement of fingermarks in forensic investigations
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Tim Oblak
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=155118&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
Fingerprints are a unique and long-lasting indicator of our identity. Partial fingermarks found at crime scenes have been used for over 100 years in criminal investigations for the purpose of personal identification. Despite the increasing automation of the forensic process, most of the work is still done manually by investigators. One of the major shortcomings in this process is the lack of dedicated software for guided fingermark analysis and enhancement, forcing investigators to use generic image processing software. In this thesis we will present a user interface for fingermark analysis and enhancement. The user interface allows the use of an open source framework for automated analysis, feature extraction and fingermark quality assessment. We will present its functionalities and demonstrate some of them with concrete examples. The tool will allow future forensic investigators to intuitively use more advanced computer vision methods for the purpose of processing fingerprint and fingermark images.

GIACOMO SEVERI - CREATION OF ISO/ICAO-COMPLIANT FACE IMAGES WITH GENARATIVE AI TOOLS.

Full Title: Creation of ISO/ICAO-compliant face images with Genarative AI tools.
Institution: University of Bologna
Supervisor: Annalisa Franco
Contact email: annalisa.franco@unibo.it

Abstract:
Artificial intelligence has revolutionized many fields, including image production. This thesis examines several generative artificial intelligence technologies, including Dall-E, Stable Diffusion, Midjourney, Adobe Firefly, and This Person Does Not Exist, analyzing their effectiveness in generating ICAO-compliant images. Through a requirements analysis and the use of Prompt Engineering techniques, the capabilities of each model are evaluated and a comparative study of the visual quality of the results obtained is carried out, highlighting the merits and shortcomings of each model. Next, the development of an automated tool for Stable Diffusion is proposed to simplify and customize the image generation process, allowing for variations in key parameters such as gender, age, ethnicity, and others, illustrating the system's goals and capabilities.

MAKSYMILIAN GORSKI - APPLICATION OF BIOMETRIC AUTHENTICATION METHODS IN CRYPTOGRAPHIC KEY EXCHANGE PROTOCOLS

Full Title: Application of biometric authentication methods in cryptographic key exchange protocols
Institution: Wroclaw University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: maksymilian_gorski@wp.pl

Abstract:
The ever-increasing demand for the amount of information exchanged over the Internet, requires the implementation of mechanisms to properly secure it. A key aspect of securing, as a result of encryption of the exchanged information, is also the provision of mechanisms to confirm the identity of the parties between whom the exchange takes place. The last decade has seen an increase in the popularity of the use of biometric authentication mechanisms for individuals, from where the proposals for protocols for the cryptographic exchange of a key to secure the aforementioned communication, while using biometric authentication of the users, were born. This paper undertakes a thorough analysis of proposals for two protocols: BAKE and BRAKE that meet the above-mentioned objectives, along with the presentation of an implementation that realizes the protocol of biometrically authenticated cryptographic key exchange. The scope of the realization of this paper also includes conducting an analysis of both the computational complexity and the size of the data exchanged between the parties involved in the proposed implementation of the protocol. Limitations and potential risks of the proposed implementations of the discussed protocols, which were not discussed by their developers, are also presented.

IZABELA MAJCHROWSKA - ANALYSIS OF SELECTED CANCELABLE BIOMETRICS SYSTEMS

Full Title: Analysis of template unlikability and impact on FAR and FRR coefficients for selected systems of cancelable biometrics
Institution: Wrocław University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: iza.majchrowska12@gmail.com

Abstract:
The use of biometrics for authentication purposes has become very popular in recent years. Due to the immutability of biometrics, an important aspect is to properly secure it against compromise. Cancellable biometrics is one of the solutions to enhance the security of biometric systems. Using appropriate algorithms, multiple, independent identities can be generated from a single biometric sample. The identities, in case of compromise, can be removed and replaced with new ones. In this study, the unlikability (independence) of the templates generated by the Bloom Filter and Biohashing algorithms is examined. The effect of using cancellable biometrics on the statistics of the biometric system - FAR and FRR coefficients - was also analyzed. To perform the analysis, a simulation of three systems - a basic system and two cancellable biometrics - was implemented.

LARA ANŽUR - FINGERPRINT RECOGNITION USING DEEP LEARNING

Full Title: Fingerprint recognition using deep learning
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Tim Oblak
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=160706&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
Fingerprints are an extremely reliable method of identifying individuals in forensic science, as they are unique and permanent. Classical fingerprint recognition methods that use machine learning often face challenges when processing low-quality samples, which requires forensic experts' assistance. The use of deep learning, which overcomes some of the limitations of classical methods, is becoming increasingly popular, but there are still too few developed solutions in this field. In this thesis, we developed a model based on Siamese neural networks (SNN) combined with the ResNet34 architecture, enabling us to efficiently compare fingerprints in latent space. We further enhanced the basic model by integrating spatial transformer networks (STN), which ensure rotational invariance, and incorporating domain knowledge about minutiae, adding additional relevant information to the process. We evaluated the methods on several publicly available datasets, where our model achieved a higher level of accuracy compared to some classical methods, confirming the potential of deep learning in the field of fingerprint identification.

DAVID BLAZHESKI - USE OF SUPER-RESOLUTION FOR IMPROVING THE QUALITY OF LOW-RESOLUTION IMAGES

Full Title: Use of super-resolution for improving the quality of low-resolution images
Institution: University of Ljubljana, Slovenia
Supervisor: Vitomir Štruc
URL: https://repozitorij.uni-lj.si/Dokument.php?id=190281&lang=slv
Link description: In Slovene
Contact email: vitomir.struc@fe.uni-lj.si

Abstract:
The thesis addresses the use of super-resolution to improve the quality of low-resolution images. Super-resolution is a process in which images of higher resolution are generated from low-resolution images. The work focused on the problem of low quality in natural classical images, which can affect various applications. The main objective of the thesis was to enhance the quality of such images using advanced super-resolution models such as Real-ESRGAN and ResShift. The methodology included a review of the theoretical foundations of super-resolution, the development and implementation of the Real-ESRGAN and ResShift models, and their testing on low-resolution images. Various metrics were used to measure the performance of super-resolution, such as PSNR, SSIM, BRISQUE, and NIQE, which allow for a quantitative evaluation of the resolution enhancement quality of the input images. The results showed that the applied models can significantly improve the quality of low-resolution images. More specifically, the ResShift model generally performed better on the PSNR and SSIM metrics compared to Real-ESRGAN, indicating higher reconstruction quality. -- Translated from Slovene

VOJTĚCH MUCHA - CONVERSION OF FINGERPRINTS SCANNED BY A MOBILE DEVICE INTO A STANDARDIZED FORMAT - IMAGE EDITING

Full Title: Převod otisků prstů nasnímaných mobilním zařízením do standardizovaného formátu - úpravy obrazu
Institution: Faculty of Electrical Engineering and Communication, Brno University of Technology
Supervisor: doc. Ing. Petr Číka, Ph.D.; Co-Supervisor: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
Link description: https://dspace.vut.cz/items/b0aca08f-8e17-411f-94f6-60d7ece25b9e
Contact email: martin@drahansky.cz

Abstract:
This bachelor thesis deals with the issue of fingerprint conversion taken by a mobile device into a standardized format. In the present day, mobile devices are used more and more often to acquire biometric data, fingerprints included. Processing and standardization of such data is an essential part of the subsequent biometric analysis. The aim of the work is to design and implement an algorithm which would convert a photo of a finger into a grey scale picture of its fingerprint with distinct papillary lines and subdued valleys. The algorithm is implemented in C++ using OpenCV library and a trained neural network for finger detection from hand image. The achieved results are evaluated according to the algorithms for assessing the quality of fingerprints NFIQ 2 and Innovatrics.

NOVÁK DAVID - RAISING USERS' SECURITY AWARENESS OF DEEPFAKES ATTACKS

Full Title: Raising Users' Security Awareness of Deepfakes Attacks
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/153545
Contact email: xnovak@stud.fit.vutbr.cz

Abstract:
This thesis provides a general overview of deepfakes, what they are, how they may be used or misused, and an introduction to cybersecurity education, especially concerning deepfakes attacks. The thesis aims to provide a way for users to enhance their awareness of security issues related to deepfake attacks. The work represents my design and implementation of a web-based application pursuing this aim, based on the summary of research concerning deepfakes. The solution offers users options to both learn about deepfakes and experience the creation of deepfakes in a simplified way. The testing of users before and after experiencing my platform indicated an increase in users' knowledge by up to 85.9\,\%. The data indicate both general user inexperience and a lack of understanding of deepfakes, which is problematic in today's trend to use deepfakes for cyber-attacks. However, based on the results, my application can fill this gap in crucial security knowledge.

EVA TRNOVSKÁ - MULTILINGUAL VOICE DEEPFAKE DATASET

Full Title: Multilingual Voice Deepfake Dataset
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/154478
Contact email: xtrnov01@stud.fit.vutbr.cz

Abstract:
This thesis examines the area of voice deepfakes: their creation and detection. It describes the state of current research and the methods of creating fake recordings. Furthermore, it provides a comprehensive analysis of available voice deepfake datasets, based on which a new multilingual dataset is designed and compiled. The dataset aims to enable further research on the generalization of deepfake detection across languages and the differences in the accuracy of male and female voice detection. The results of the experiments show that for the models tested, it is possible to replace detectors trained to detect in a single language with detectors trained on a multilingual set, with an accuracy loss of a few percent. The tested models were generally more accurate in detecting recordings with female voices, but this property was not demonstrated for all tested detectors.

PETR KAŠKA - RESILIENCE OF BIOMETRIC AUTHENTICATION OF VOICE ASSISTANTS AGAINST DEEPFAKES

Full Title: Resilience of Biometric Authentication of Voice Assistants Against Deepfakes
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/154457
Contact email: xkaska01@stud.fit.vutbr.cz

Abstract:
Voice assistants (Apple Siri, Amazon Alexa, Google-assistant, Samsung Bixby) supporting voice control offer more and more possibilities to make all our daily activities easier. People give them access to data and information to take full advantage of all these features. Along with the rapidly developing voice deepfake technology, there is a big threat in the area of misusing deepfakes to trick smart voice assistants. An attacker can record the victim's voice, synthesize the voice and create a recording of some command to trick the assistant in order to harm the victim. The aim of this work is to design an experiment that will simulate attacks, performed by synthetic voice, on voice assistants and then evaluate their defensiveness. The conducted experiment confirms the initial hypothesis of the vulnerability of voice assistants to deepfake attacks and the results are very alarming with an overall success rate of 90% indicating insufficient defense of voice assistants and require the implementation of additional countermeasures to prevent the risk of misuse as the number of voice assistants in active use is rapidly increasing.

KAMBULAT ALAKAEV - METHODS FOR REALTIME VOICE DEEPFAKES CREATION

Full Title: Methods for Realtime Voice Deepfakes Creation
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/154458
Contact email: xalaka01@stud.fit.vutbr.cz

Abstract:
This thesis explores the possibility of achieving real-time voice deepfake generation using open-source tools. Through experiments, it was discovered that the generation rate of voice deepfakes is affected by the computing power of the devices running the speech creation tools. A deep learning model was identified to be capable of generating speech in near real time. However, limitations in the tool containing this model prevented continuous input data for real-time generation. To address this, a program was developed to overcome these limitations. The quality of the generated deepfakes was evaluated using both voice deepfake detection models and human online surveys. The results revealed that while the model could deceive detection models, it was not successful in fooling humans. This research highlights the accessibility of open-source voice synthesis tools and the potential for their misuse by individuals for fraudulent purposes.

VALENTINA FOHR - BIOMETRIC FUSION IN THE FIELD OF MULTI-BIOMETRIC CRYPTOSYSTEMS

Full Title: Investigation and evaluation of various methods for biometric fusion in the field of Multi-Biometric Cryptosystems
Institution: Hochschule Darmstadt
Supervisor: Christian Rathgeb
Contact email: christian.rathgeb@h-da.de

Abstract:
Biometric Cryptosystems have become increasingly popular due to their ability to preserve privacy for biometric data, e.g., iris or fingerprints. However, the entropy of a single biometric characteristic is limited regarding recognition performance and security. Consequently, to improve the recognition performance and security of Biometric Cryptosystems, a fusion of multiple biometric characteristics is required. While various fusion methods exist, this work focuses on the concatenation, interleaving and randomly shuffled methods. This work aims to provide insights into which of these fusion methods is the most effective regarding recognition performance and security of Biometric Cryptosystems, specifically within the framework of the fuzzy commitment scheme. In order to accomplish this aim, the following steps are performed. First, monomodal biometric databases from distinct biometric characteristics are created. The creation of databases from different modalities with different extractors poses a challenge as such extracted modalities result in non-uniform representation vectors. To address this challenge, datasets generated by Convolutional Neural Networks are used. Next, fused biometric databases are created by fusing the embeddings of the monomodal biometric databases using the concatenation, interleaving and randomly shuffled fusion methods. Afterwards, the fused databases are evaluated with respect to their recognition performance and security utilizing bit-level and block-level error correction codes. The findings show that overall, the most effective fusion method regarding recognition performance is the random shuffling method, closely followed by the interleaved method. Whereas the concatenation method performs poorly in comparison to the other two methods. The findings also reveal that security depends on the block size and number of blocks in the bit-level error correction, and on the number of correctable blocks in the block-level error correction, but not specifically on the fusion method.

ALJAŽ JUSTIN - EAR RECOGNITION PIPELINE USING SIAMESE MODELS ON OPEN DATA SETS

Full Title: Ear recognition pipeline using Siamese models on open data sets
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Žiga Emeršič, Peter Peer
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=161574&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
The thesis addresses the problem of ear-based person recognition with the aim of improving accuracy and reliability in the process of ear detection and recognition, as well as developing a pipeline that enables real-time operation using deep neural networks. The solution consists of two parts: ear detection using the YOLOv8 model and recognition employing a Siamese model, combined into a unified system that operates with a single ear image on an open dataset. We evaluated two different variations of the Siamese model for recognition on open sets. The model based on the ResNet architecture proved to be superior to the model based on the EfficientNet architecture. With this work, we have demonstrated that Siamese neural networks are suitable for ear-based recognition and that there is significant room for improvement in this area.

TADEJ LOGAR - DEEPFAKE DETECTION USING VIDEO TRANSFORMERS

Full Title: Deepfake Detection using Video Transformers
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Borut Batagelj
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=155116&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
In this bachelor's thesis we examine the task of Deepfake detection. These fake videos are appearing online with increasing frequency. With the use of deep learning for their creation, they have become convincing enough to trick humans. The goal of creating these fake videos is often to spread misinformation or damage the reputations of celebrities. For this task of detecting fake videos, we present two related video-based approaches, with each using the transformer architecture. These approaches are known as the Video Vision Transformer (ViViT) and UniFormerV2. We trained models of these two approaches on two datasets of fake videos, FaceForensics++ and Celeb-DF-v2. We also tested the performance of these models on an additional test set of videos from the DFDC dataset. With the use of these models, we have achieved results comparable to state-of-the-art approaches in this field. As part of the thesis, we describe our methodology, the technologies used in the approaches, and certain implementation details. We also present detailed results of the models we trained, our experiments, and a comparison of our results with some of the different approaches to Deepfake detection.