ACADEMIC GRADUATION MONITORING REPORT

2025



European Association for Biometrics (EAB)

version: 2026-11-09

Email: secretariat@eab.org

RESEARCH MONITOR CONTENT

PREFACE 5

MONITOR PHD-THESES 6

FELIX ROSBERG - NON-REVERSIBLE AND ATTRIBUTE PRESERVING FACE DE-IDENTIFICATION 7

NOVA HADI LESTRIANDOKO - THE CONTRIBUTION OF FACIAL COMPONENTS TO FACE RECOGNITION 8

SIMONE MAURIZIO LA CAVA - 3D FACIAL RECONSTRUCTION AND DEEPFAKE DETECTION: ADVANCES IN SECURITY AND FORENSIC INVESTIGATION THROUGH COMPLEMENTARY DEEP LEARNING TECHNIQUES 9

HAOYU ZHANG - FACE MORPHING ATTACKS 10

PETER ROT - PRIVACY-PRESERVING FACE ANALYTICS USING DEEP LEARNING METHODS 11

TUĞÇE ARICAN - PATCHING UP FINGER VEIN RECOGNITION 12

PINAR SANTEMIZ - SIDE-VIEW FACE RECOGNITION 13

FELIX ROSBERG - NON-REVERSIBLE AND ATTRIBUTE PRESERVING FACE DE-IDENTIFICATION 14

MARCEL GRIMMER - DEEP GENERATIVE NETWORKS IN FACE RECOGNITION 15

COLTON CRUM - INTEGRATING HUMAN-PERCEPTUAL PRIORS INTO DEEP LEARNING 16

ANTON FIRC - ARTIFICIAL INTELLIGENCE IN COMPUTER SECURITY 17

SARA CONCAS - ADVANCED STRATEGIES FOR DEEPFAKE DETECTION, 3D FACIAL RECONSTRUCTION, AND IRIS RECOGNITION IN MODERN SECURITY 18

ZOHRA REZGUI - ENHANCED DEMOGRAPHIC PRIVACY IN FACE RECOGNITION: FROM IMAGES TO TEMPLATES 19

ILIAS BATSKOS - THE PROBLEM OF FACE IMAGE MORPHING IN IDENTIFICATION DOCUMENTS 20

MONITOR MASTER-THESES 21

MARICA PASQUALI - GENERATION OF DOUBLE-IDENTITY FINGERPRINTS USING A CONDITIONAL GENERATIVE ADVERSARIAL NETWORK (CGAN) 22

NISHTMAN ANDISHA - FAIRNESS EVALUATION OF FIQA 23

NATÁLIE IŘÍKOVÁ - RECOGNITION OF SKIN DISEASE TYPE IN FINGERPRINTS 24

PAVLA DRTILOVÁ - DETERMINATION OF HEAD TISSUE CHANGES 25

MACIEJ SALWOWSKI - DIGITAL AND PHYSICAL ATTACK DETECTION 26

THOMAS SCHUTH - BIOMETRIC TEMPLATE PROTECTION 27

MATEJ MIOČIĆ - GENERATING PHOTOREALISTIC FACIAL COMPOSITES WITH DIFFUSION MODELS 28

ELISA CARIA - EMOTION RECOGNITION THROUGH EEG BASED ON THE STUDY OF HEMISPHERIC LATERALIZATION 29

PEDRO DELGADO-DEROBLES - EXPLORING IDENTITY VERIFICATION THROUGH BEHAVIORAL PATTERNS IN VIDEOS 30

LEON TODOROV - DETECTION OF FACE FORGERIES WITH SELF-SUPERVISED LEARNING 31

DILARA CELEPI - BIAS OF BIOMETRIC QUALITY ASSESSMENT 32

NIKOLA MARIĆ - MORPHING ATTACK DETECTION USING MULTIMODAL LARGE LANGUAGE MODELS 33

VENDELA NJEGOVEC - FORENSIC AUTOMATIC SPEAKER RECOGNITION 34
MARICA PASQUALI - GENERATION OF DOUBLE-IDENTITY FINGERPRINTS 35
HANS HEJE - VISION LANGUAGE MODELS FOR PRESENTATION ATTACK DETECTION 36
JANA PUTOVÁ - FINGER VASCULAR STRUCTURE SENSING AND RECOGNITION DEVICE 37
K.C KADOLKAR - VISUALIZATION OF DEEPFAKE DETECTION USING FORENSIC METHODS 38
ROSA HORNERO - BIOMETRIC RECOGNITION OF HUMAN GAIT USING INERTIAL SENSORS IN SMARTPHONES 39
GUSTAV PEDERSEN - INTERPRETABILITY IN FACE IMAGE QUALITY ASSESSMENT 40
TAMÁS ENDREI - AERIAL-GROUND PERSON RE-IDENTIFICATION IN SURVEILLANCE SCENARIOS 41
IRIS BJÖRK - AGE MANIPULATION 42
JERNEJ SABADIN - GENERATION OF SYNTHETIC FACES WITH DIFFUSION MODELS 43
FERNANDO FERNANDEZ DEL CERRO - GENERATION OF SYNTHETIC ON-LINE SIGNATURES FOR BIOMETRIC RECOGNITION 44
RADIM HOMOLA - POSITIONING EQUIPMENT FOR PHOTOGRAMMETRY 45
MÁRK GYÖNGYÖSI - FACIAL IMAGE QUALITY ASSESSMENT 46
MONITOR BACHELOR-THESES 47
FILIP THUNBERG - IMPROVING OCULAR RECOGNITION WITH SYNTHETIC DATA 48
LUCA CAMILLINI - DEVELOPMENT OF A WRAPPER FOR THE MCC SDK AND INTEGRATION WITH AI MODELS 49
PHILIPP SCROCK - DETECTION OF FACIAL FILTERS 50
STEFANO LILLIU - EVALUATION OF THE ROBUSTNESS OF STEGANOGRAPHIC TECHNIQUES AGAINST MANIPULATIONS AND MORPHING ATTACKS 51
ADRIAN STERNER - USEFULNESS OF SYNTHETIC DATA IN BIOMETRIC RECOGNITION 52
ANDRES HUERGO-PEREA - BIOMETRIC RECOGNITION OF IN-AIR SIGNATURES USING MOBILE DEVICES 53
DANIELE FENU - ADVERSARIAL ATTACKS AGAINST FINGERPRINT-BASED BIOMETRIC DEVICES 54
DAVIDE GIANNETTI - DATA AUGMENTATION FOR TRAINING FACIAL MORPHING DETECTION SYSTEMS 55
MAXIMILIAN RUSSO - MULTI-INSTANZ-ANSATZ FÜR FINGERABDRUCKSMERKMALE 56
BARTLOMIEJ BAUT - SIGNATURES IN THE AIR AS A NEW METHOD FOR AUTHENTICATING INDIVIDUALS 57
PAULINA OTLIK - IMPLEMENTATION OF SELECTED ISO/IEC 29794-5 VERIFIERS AND PROPOSING ALTERNATIVES 58
ROK PISTOTNIK - ANALYSIS AND OPTIMIZATION OF MODELS FOR AUTOMATIC FACE RECOGNITION 59
MATTIA SENNI - ANALISI E SVILUPPO DI ALGORITMI PER LA VALUTAZIONE DELLA QUALITÀ DELLE IMMAGINI DEL VOLTO 60
BARTLOMIEJ PIOTROWSKI - KEYSTROKES DYNAMICS IDENTITY MODELS BASED ON FORCE BIOMETRICS USING HALL EFFECT 61
NICOLÒ PENSERINI - GENERAZIONE DI VIDEO SINTETICI PER IL RICONOSCIMENTO DI VOLTI 62
MATEVŽ VIDOVIČ - LIGHTWEIGHT MODELS FOR OCULAR SEGMENTATION 63
ESTER MASALA - DECEPTIVE BEAUTY: THE IMPACT OF BEAUTY FILTERS ON DEEPFAKE AND MORPHING DETECTION 64
MATYLDA MUSILOVÁ - EXPLORING THE METHODS OF DIGITAL FINGERPRINT SCANNING 65
PHILLIP SROCK - ANALYSIS AND DETECTION OF FACIAL FILTERS USING FACE BEAUTY 66

FRANCESCO MAROTTO - AUTOMATIC CORRECTION OF VERBAL DISFLUENCIES USING SYNTHETIC VOICE GENERATION TECHNIQUES 67

OSKAR KONJANČIČ - DISTANCE BETWEEN SCLERA IMAGES 68

MATTEO TRUDU - DEEPFAKE ATTACKS AGAINST AUTOMATIC SPEAKER RECOGNITION SYSTEMS 69

ELISA YAN - IDENTITY VERIFICATION THROUGH THE COMBINATION OF MULTIPLE FRAMES AND FACE QUALITY METRICS IN BORDER CONTROL SCENARIOS 70

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

FELIX ROSBERG - NON-REVERSIBLE AND ATTRIBUTE PRESERVING FACE DE-IDENTIFICATION

Full Title: Non-Reversible and Attribute Preserving Face De-Identification
Institution: Halmstad University, Sweden
Supervisor: Cristofer Englund, Eren Aksoy, Fernando Alonso-Fernandez
URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-55652
Contact email: feralo@hh.se

Abstract:
De-identification, also known as anonymization, is a broad term that refers to the process of redacting or obscuring personal data, or data that identifies an individual. In the context of video and image data de-identification, the most tangible personal information is the face. Faces are considered biometric data, thus change little compared to other aspects of an individual, such as clothing and hairstyle. Humans possess a strong innate ability to recognize faces. Computers are also adept at recognizing faces, and face recognition models are exceptionally powerful at identifying and comparing faces. Consequently, it is widely recognized as crucial to obscure the faces in video and images to ensure the integrity of de-identified data. Conventionally, this has been achieved through blurring or masking techniques. However, these methods are destructive of data characteristics and thus compromise critical attribute information such as eye gaze, pose, expression and the fact that it is a face. This is a particular problem because our society is data-driven in many ways. This information is useful for a plethora of functions such as traffic safety. One obvious such aspect is autonomous driving and driver monitoring, where necessary algorithms such as object detectors rely on deep learning to function. Due to the data hunger of deep learning, combined with society's demand for privacy and integrity through regulations such as the General Data Protection Regulation (GDPR), face de-identification, which preserves useful information, becomes significantly important. This Thesis investigates the potential and possible limitations of de-identifying faces, while preserving the aforementioned useful attribute information. The Thesis is especially focused on the sustainability perspective of de-identification, where the perseverance of both integrity and utility of data is important. The baseline method to achieve this is through methods introduced from the face swapping and face manipulation literature, where the current research focuses on changing the face (or identity) with generative models while keeping the original attribute information as intact as possible. All while being integrated and consistent in an image and/or video. Specifically, this Thesis will demonstrate how generative target-oriented and subject-agnostic face manipulation models, which aim to anonymize facial identities by transforming original faces to resemble specific targets, can be used for realistic de-identification that preserves attributes. While this Thesis will demonstrate and introduce novel de-identification capabilities, it also addresses and highlight potential vulnerabilities and security issues that arise from naively applying generative target-oriented de-identification models. First, since state-of-the-art face representation models are typically restricting the face representation embeddings to a hyper-sphere, maximizing the privacy may lead to trivial identity retrieval matching. Second, transferable adversarial attacks, where adversarial perturbations generated by surrogate identity encoders cause identity leakage in the victim de-identification system. Third, reconstruction attacks, where bad actor models are able to learn and extract enough information from subtle cues left by the de-identification model to consistently reconstruct the original identity. Through this, this Thesis points out several approaches that are: 1) Controllable, meaning that the proposed models do not naively change the identity. This means that the type and magnitude of identity change is adjustable, and thus tunable to ensure anonymization. 2) Subject agnostic, meaning that the models can handle any identity or face. 3) Fast, meaning that the models are able to run efficiently. Thus having the potential of running in real-time. 4) Non-reversible, this Thesis introduces a novel diffusion-based method to make generative target-oriented models robust against reconstruction attacks. The end product consists of a hybrid generative target-oriented and diffusion de-identification pipeline that achieves state-of-the-art performance on privacy protection as measured by identity retrieval, pose retention, expression retention, gaze retention, and visual fidelity while being robust against reconstruction attacks.

NOVA HADI LESTRIANDOKO - THE CONTRIBUTION OF FACIAL COMPONENTS TO FACE RECOGNITION

Full Title: The contribution of facial components to face recognition
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://research.utwente.nl/en/publications/the-contribution-of-facial-components-to-face-recognition/
Link description: The contribution of facial components to face recognition
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
Facial components, such as the eyes, nose, and eyebrows, play a critical role in biometric and forensic identification. While previous studies have explored the effects of partial occlusion and masking on face recognition, the systematic analysis of individual facial components' contributions to deep face recognition remains limited. This thesis introduces a method to analyze the importance of different face components to face recognition and a tool that enables the selective replacement of facial components to study their impact on recognition performance. Through a series of experiments, we demonstrate that certain components, particularly the eyebrows and nose, carry more discriminative information than others, with texture generally being more influential than shape, except for the eyebrows. The method also extends to historical facial analysis, such as identifying Roman emperors from sculptures by isolating features like hairstyles and facial hair. Moreover, we present an open-source tool developed in Python, capable of seamlessly replacing facial components, including their textures and shapes, suitable for both research and application contexts. This work bridges a gap in facial analysis by providing a systematic approach and practical tool for studying the role of facial components in face recognition.

SIMONE MAURIZIO LA CAVA - 3D FACIAL RECONSTRUCTION AND DEEPFAKE DETECTION: ADVANCES IN SECURITY AND FORENSIC INVESTIGATION THROUGH COMPLEMENTARY DEEP LEARNING TECHNIQUES

Full Title: 3D Facial Reconstruction and Deepfake Detection: Advances in Security and Forensic Investigation Through Complementary Deep Learning Techniques
Institution: University of Cagliari
Supervisor: Gian Luca Marcialis
Contact email: simonem.lac@unica.it

Abstract:
"Nowadays, facial biometrics holds a crucial role in security and forensics, bridging the realms of identification, authentication, and digital evidence analysis. Whether utilized for access control, surveillance, or forensic analysis, facial biometrics provide powerful and automatized tools, especially those based on deep learning, for authenticating identities and identifying individuals reliably and in a timely fashion. The integration of techniques for reconstructing 3D models from the available 2D facial data can further aid the reliability of facial recognition in challenging conditions, such as unfavorable illumination and non-frontal poses of the face, commonly faced by forensic practitioners and security operators. However, as for any other approach based on biometric characteristics, 3D facial reconstruction must observe strict requirements that still make its potential role in these application fields unclear. Moreover, the emergence of data manipulation technology poses further challenges to facial recognition in security and forensic investigations. This is particularly evident in the case of deepfakes, using artificial intelligence to generate highly realistic fake images or videos, often manipulating faces to alter behavior or identities. Similarly, another issue is morphing, which involves blending facial features from multiple individuals to create synthetic images potentially used for identity theft or fraudulent activities. Tools and algorithms that leverage digital artifacts and inconsistencies indicative of such manipulations are continuously being proposed to discern altered media from authentic content. However, these detection systems are still susceptible to novel manipulations and, therefore, unable to ensure the trustworthiness of digital content. This thesis investigates the deep connection facial biometrics share with security and forensics, particularly regarding face recognition and facial manipulation detection. Hence, we discuss the current obstacles to integrating traditional 2D analysis techniques and 3D face reconstruction into real-world security systems and forensic investigations. Then, we contribute to addressing some of these issues by proposing approaches exploiting the inherent complementarity of different facial characteristics and the synergy between the deep learning techniques based on them to improve the reliability of identity verification and manipulation detection. The presented contributions may represent steps towards making facial features a cornerstone in safeguarding public safety, enhancing forensic identifications, protecting against identity fraud, and ensuring the integrity of digital evidence."

HAOYU ZHANG - FACE MORPHING ATTACKS

Full Title: Face Morphing Attacks: Generation, Data Augmentation and Detection
Institution: Norwegian University of Science and Technology (NTNU)
Supervisor: Raghavendra Ramachandra, Kiran Raja and Christoph Busch
Contact email: christoph.busch@ntnu.no

Abstract:
This thesis focuses on face morphing attacks, a novel type of attack targeting deceiving the FRS by generating a single face image combined from face samples from multiple subjects. One of the most common scenarios is the Automatic Border Control (ABC) with Electronic Machine Readable Travel Document (eMRTD). In most countries, the face data in passports are collected from the submitted photo of the applicants, which leads to the risk of enrolling manipulated face images. Hence, it is crucial to develop robust morphing attack detection (MAD) algorithms to prevent intentional attacks. It is challenging because morphs can be generated by different algorithms and are considered unseen attacks. Another challenge is the shortage of sufficient training data. As face images are considered sensitive data, it is difficult to share high-quality and large-scale datasets for training well-generalised MAD algorithms. Finally, it is necessary to design novel MAD algorithms to provide accuracy and generalisability, and also study the explainability of the algorithms to make the algorithms trustworthy and user-friendly for real-world secure applications.

PETER ROT - PRIVACY-PRESERVING FACE ANALYTICS USING DEEP LEARNING METHODS

Full Title: Privacy-preserving face analytics using deep learning methods
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Vitomir Štruc, Peter Peer
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=166838&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
The rapid advancements in face analytics have enabled a wide range of applications, from identity verification to expression analysis and personalized services. In addition to identity information, these technologies can extract various soft-biometric attributes such as gender, ethnicity, age, and body mass index (BMI), providing valuable insights for different domains. However, the extraction of these attributes raises significant privacy and data protection concerns. To achieve a balance between the benefits and risks of face analytics, it is essential to develop privacy-enhancing techniques that safeguard individuals' privacy rights while responsibly utilizing facial data. De-identification methods, known for concealing identity-related features, are well-recognized examples of such approaches. However, a relatively lesser-studied group of privacy-enhancing methods has recently emerged, known as soft-biometric privacy-enhancing techniques (SB-PETs). In contrast to de-identification methods, SB-PETs aim to retain identity information while preventing the extraction of soft-biometric attributes. In recent years, several SB-PET methods have been proposed to eliminate information about soft-biometrics at different levels of the biometric pipeline, including the image- and representation-level. However, there are still many open and crucial research questions regarding these techniques. For instance, how can the evaluation of SB-PETs be conducted efficiently and comprehensively? How can their effects on images be detected? To what degree can information about individual soft-biometric characteristics be eliminated without critically affecting recognition performance? Can the privacy of multiple soft-biometrics be efficiently enhanced simultaneously? In this work, we address these questions and make the following scientific contributions: 1. We present a novel evaluation methodology, PrivacyProber, to assess existing image-level SB-PETs, revealing their vulnerability to reconstruction attacks. We investigate the robustness of soft-biometric privacy techniques against attribute recovery attempts, highlighting variations in their effectiveness. Using the newly proposed attribute-recovery robustness (ARR), we evaluate the robustness of SB-PETs by comparing attribute-classification accuracy between original and reconstructed images. 2. We propose a new detection approach, APEND (Evidence Aggregation for Privacy-Enhancement Detection), which effectively identifies privacy-enhanced images and outperforms existing detectors. The main advantage of APEND is that it operates under a black-box assumption that requires no knowledge or information about the specific SB-PET being employed. 3. We present PriDSS (Privacy through Fusion of Disentangled Spatial Segments), a novel image-level SB-PET, that effectively protects the gender attribute while maintaining the visual quality of facial images. PriDSS employs image fusion to combine identity-related facial parts (i.e., eyes, mouth, nose, etc.) with contextual information from the opposite gender that result in images that confuse machine classifiers and minimize modification traces. The generated images outperform the competing PrivacyNet model in term of photorealism. 4. We propose PFRNet (Privacy-enhancing Face-representation Learning Network), a representation-level method that effectively disentangles binary-defined facial attributes from face verification templates obtained using state-of-the-art face recognition models. PFRNet can be applied to various face verification templates and, in this regard, is not limited to a specific method for extrating these templates from faces. Feature disentanglement proves to be an effective approach for soft-biometric privacy enhancement. 5. We also introduce ASPECD (Adaptable Soft-biometric Privacy–Enhancement using Centroid Decoding), a representation-level SB-PET that enables controllable privacy-enhancement of multiple soft-biometric characteristics. ASPECD is built on multiple components, each dedicated to an individual soft-biometric modality. We extend PFRNet to be suitable for the privacy-enhancement of categorical soft-biometric characteristics. Finally, we evaluate ASPECD on gender and ethnicity, compare it with the state-of-the-art approach MultiIVE, and report promising results.

TUĞÇE ARICAN - PATCHING UP FINGER VEIN RECOGNITION

Full Title: Patching up finger vein recognition: An unsupervised approach using local information for robustness
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://research.utwente.nl/en/publications/patching-up-finger-vein-recognition-an-unsupervised-approach-usin/
Link description: Patching up finger vein recognition: An unsupervised approach using local information for robustness
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
In the era of heightened security and privacy concerns, finger vein recognition presents a significant advantage over traditional biometric methods like facial and fingerprint recognition. Unlike fingerprints and facial features, which can be easily captured or replicated, vein patterns are hidden beneath the skin, making them resistant to theft and forgery. This makes finger vein recognition a promising technology for high-security applications. However, several challenges hinder its widespread adoption. These include limited labelled data, difficulties in generalising learned representations, and the lack of comprehensive image quality assessment methods. Finger vein datasets are relatively small, making deep learning approaches reliant on transfer learning from natural image datasets. While this technique achieves state-of-the-art performance on individual datasets, it struggles with cross-dataset generalisation, limiting its effectiveness in real-world applications where multiple devices are involved. Additionally, current image quality assessments often focus on general image attributes like sharpness and contrast, overlooking their actual utility in recognition. To address these challenges, this thesis explores alternative approaches for improving the reliability and robustness of finger vein recognition. An unsupervised auto-encoder model is proposed to learn meaningful representations without requiring large datasets. However, it struggles with distinguishing vein structures due to the dominance of background patterns. To overcome this, a patch-based approach is introduced, dividing images into smaller sections to enhance training variability and reduce background interference. This approach outperforms traditional deep learning models and maintains consistent performance across unseen datasets. For cross-device recognition, a novel dataset comprising images from six different devices is introduced. The results show that device variations impact recognition performance, but the patch-based auto-encoder achieves superior generalisation compared to traditional and deep learning methods. This highlights the need for standardised acquisition protocols for improved interoperability. Finally, a patch-based quality assessment method is developed, focusing on vein visibility and diversity to ensure reliable recognition. Evaluations demonstrate its effectiveness in detecting poor-quality samples, enhancing system security. Overall, this research advances finger vein recognition technology, offering insights into its robustness, generalisation, and quality assessment, with potential for real-world applications.

PINAR SANTEMIZ - SIDE-VIEW FACE RECOGNITION

Full Title: Side-view face recognition
Institution: Side-view face recognition
Supervisor: Luuk Spreeuwers
URL: https://research.utwente.nl/en/publications/side-view-face-recognition-3/
Link description: Side-view face recognition
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
Face recognition is a widely used biometric method for its non-intrusive and passive nature. Side-view face recognition, in particular, offers unique advantages and expands the potential for real-world applications. While advancements in deep learning have greatly improved recognition perform ance for frontal faces, pose variation remains a significant challenge. Real-world face recognition applications, such as access control, sur veillance, security, and smart home systems, often involve non-frontal poses, making side-view face recognition a crucial biometric solution. Furthermore, long-term re-identification can significantly benefit from side-view face recognition as it enhances accuracy when frontal images are unavailable. However, side-view poses introduce unique challenges, including self-occlusion, asymmetry, and a scarcity of reliable facial landmarks, which complicates key tasks such as detection, alignment, and feature extraction. Unlike most systems that rely on frontal images or frontalization techniques, our study focuses on side-view-to-side-view face recognition, addressing a critical research gap in non-frontal recognition. We systematically investigate the challenges, limitations, and advancements in side-view face recognition to develop a system that performs reliably across diverse real-world conditions. Our key contributions are as follows: We provide atechnical report on early developments and an in-depth survey of state-of-the-art side-view face recognition, categorizing approaches into feature-based, image-based, and set-based methods. We critically analyze these methods and identify a significant gap in existing benchmarks. Most datasets exhibit a frontal bias and lack sufficient variation to reflect real world challenges, meaning high performance does not necessarily indicate robustness against extreme poses. While cross-dataset evaluations are crucial for proper assessment, they remain largely underexplored. Next, we contributed UT-DOOR, a video-based face dataset featuring recordings of 98 subjects captured by four doorpost-mounted cameras.The dataset primarily comprises side-view poses and presents unique challenges, including significant variations in face size and rotation. Additionally, varying subject-to-camera distances may result in partial face captures when the viewing angle fails to encompass the entire face. To address the challenges of face detection and registration, we examine landmark locations on side-view poses. We identify the eye center, mouth corner, and nose tip as the most reliable landmarks, as others are sensitive to pose, expression, and occlusion. We validate this by automating the detection and improving recognition with Local Binary Patterns (LBP). Then, we analyze the impact of face size, rotation, and position on deep learning similarity scores, emphasizing that accurate face detection remains particularly challenging in side-view poses. To address these challenges, we propose a registration method that enhances face detection and improves performance. Another key challenge is the scarcity of salient facial regions on side-view poses, which hinders reliable feature extraction. We compare various face description methods and highlight the key advantages of LBP, including robustness to minor pose variations through its local region-based ap proach and computational efficiency as an untrained algorithm. Moreover, we propose leveraging video information to eliminate misregistered images and enhance recognition performance. We then introduce a deep learning based system, which achieves improved performance over conventional methods. While deep learning enhances pose handling, our analysis of saliency maps across different poses underscores the challenges posed by feature sparsity. While many studies report high accuracy within specific datasets, our findings reveal that cross-dataset evaluations often produce suboptimal results, indicating that dataset-specific fine-tuning limits generalization. We benchmark deep learning against LBP and show that LBP, as an untrained method, exhibits strong resilience to cross-dataset variations, outperforming deep learning in our experiments. These results emphasize the need to improve the cross-dataset generalization of deep learning models for real-world applications. Also, expanding datasets for evaluating non-frontal poses, particularly side-view-to-side-view recognition, remains essential

FELIX ROSBERG - NON-REVERSIBLE AND ATTRIBUTE PRESERVING FACE DE-IDENTIFICATION

Full Title: Non-Reversible and Attribute Preserving Face De-Identification
Institution: Halmstad University, Sweden
Supervisor: Cristofer Englund, Eren Aksoy, Fernando Alonso-Fernandez
URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-55652
Contact email: feralo@hh.se

Abstract:
De-identification, also known as anonymization, is a broad term that refers to the process of redacting or obscuring personal data, or data that identifies an individual. In the context of video and image data de-identification, the most tangible personal information is the face. Faces are considered biometric data, thus change little compared to other aspects of an individual, such as clothing and hairstyle. Humans possess a strong innate ability to recognize faces. Computers are also adept at recognizing faces, and face recognition models are exceptionally powerful at identifying and comparing faces. Consequently, it is widely recognized as crucial to obscure the faces in video and images to ensure the integrity of de-identified data. Conventionally, this has been achieved through blurring or masking techniques. However, these methods are destructive of data characteristics and thus compromise critical attribute information such as eye gaze, pose, expression and the fact that it is a face. This is a particular problem because our society is data-driven in many ways. This information is useful for a plethora of functions such as traffic safety. One obvious such aspect is autonomous driving and driver monitoring, where necessary algorithms such as object detectors rely on deep learning to function. Due to the data hunger of deep learning, combined with society's demand for privacy and integrity through regulations such as the General Data Protection Regulation (GDPR), face de-identification, which preserves useful information, becomes significantly important. This Thesis investigates the potential and possible limitations of de-identifying faces, while preserving the aforementioned useful attribute information. The Thesis is especially focused on the sustainability perspective of de-identification, where the perseverance of both integrity and utility of data is important. The baseline method to achieve this is through methods introduced from the face swapping and face manipulation literature, where the current research focuses on changing the face (or identity) with generative models while keeping the original attribute information as intact as possible. All while being integrated and consistent in an image and/or video. Specifically, this Thesis will demonstrate how generative target-oriented and subject-agnostic face manipulation models, which aim to anonymize facial identities by transforming original faces to resemble specific targets, can be used for realistic de-identification that preserves attributes. While this Thesis will demonstrate and introduce novel de-identification capabilities, it also addresses and highlight potential vulnerabilities and security issues that arise from naively applying generative target-oriented de-identification models. First, since state-of-the-art face representation models are typically restricting the face representation embeddings to a hyper-sphere, maximizing the privacy may lead to trivial identity retrieval matching. Second, transferable adversarial attacks, where adversarial perturbations generated by surrogate identity encoders cause identity leakage in the victim de-identification system. Third, reconstruction attacks, where bad actor models are able to learn and extract enough information from subtle cues left by the de-identification model to consistently reconstruct the original identity. Through this, this Thesis points out several approaches that are: 1) Controllable, meaning that the proposed models do not naively change the identity. This means that the type and magnitude of identity change is adjustable, and thus tunable to ensure anonymization. 2) Subject agnostic, meaning that the models can handle any identity or face. 3) Fast, meaning that the models are able to run efficiently. Thus having the potential of running in real-time. 4) Non-reversible, this Thesis introduces a novel diffusion-based method to make generative target-oriented models robust against reconstruction attacks. The end product consists of a hybrid generative target-oriented and diffusion de-identification pipeline that achieves state-of-the-art performance on privacy protection as measured by identity retrieval, pose retention, expression retention, gaze retention, and visual fidelity while being robust against reconstruction attacks.

MARCEL GRIMMER - DEEP GENERATIVE NETWORKS IN FACE RECOGNITION

Full Title: Deep Generative Networks in Face Recognition - With Application to Face Image Quality Assessment
Institution: NTNU
Supervisor: Christoph Busch
Contact email: christoph.busch@ntnu.no

Abstract:
The widespread adoption of face recognition systems for authentication spans from convenience-based applications (e.g., smartphone unlocking) to security-critical applications (e.g., border control). This trend stems from the transition from traditional machine learning to deep learning-based recognition models, which have significantly improved recognition accuracy and robustness against various sources of variation. However, the effectiveness of deep neural networks largely depends on the availability of sufficient training and evaluation data. One possible solution to meet the high demand for data is to exploit recent advances in deep generative models, which can generate highly realistic facial images that are indistinguishable from images upon human inspection. Therefore, this thesis examines how large-scale data collection can be circumvented by using deep generative models for evaluating face recognition systems and deriving quality assessment measures.

COLTON CRUM - INTEGRATING HUMAN-PERCEPTUAL PRIORS INTO DEEP LEARNING

Full Title: Integrating Human-Perceptual Priors into Deep Learning
Institution: University of Notre Dame
Supervisor: Adam Czajka
URL: https://curate.nd.edu/articles/thesis/Integrating_Human-Perceptual_Priors_into_Deep_Learning/30759320?file=60268586
Contact email: aczajka@nd.edu

Abstract:
Within high-risk domains, such as medical diagnostics and biometric identification systems, generalization is essential to reaping the host of benefits artificial intelligence (AI) promises. AI must safely navigate unknown environments, make decisions with incomplete information, manage uncertainty, and convey its insights reliably to human operators. However, contemporary AI models fail to obtain sufficient generalization, curtailing its use within these important applications in society. Given that humans have a remarkable capacity for generalization, research has sought to incorporate human-perceptual priors into the training of AI systems. The integration of human salient information has not only raised AI's generalization capabilities, but also offers several ancillary benefits, such as improved explainability and faster algorithmic convergence, further strengthening its aptitude for real-world deployment. Unifying both human and machine intelligence forges a safer path forward as society traverses through an increasingly stochastic, chaotic, and uncertain world.

ANTON FIRC - ARTIFICIAL INTELLIGENCE IN COMPUTER SECURITY

Full Title: Artificial Intelligence in Computer Security
Institution: Brno University of Technology
Supervisor: Kamil Malinka
URL: https://www.vut.cz/en/students/final-thesis/detail/168471
Link description: BUT public repository for theses
Contact email: anton.firc@vut.cz

Abstract:
Since their origin, deepfake audio threatens computer security, increasing the effectiveness of social engineering attacks and enabling spoofing of speaker recognition systems. While the research focused primarily on detection methods, a structured cybersecurity perspective was missing, creating a research gap. This thesis introduces a structured cybersecurity assessment of risks posed by deepfakes. A key outcome is understanding an attacker model that further guides the development and evaluation of protection methods. We propose an evaluation framework for detection methods to address known challenges of deepfake detection, such as poor generalisation and limited comparability. Our analysis of the human perception of audio deepfakes inspired by real-world attacks revealed that humans fail to recognise deepfakes reliably in actual attacks. Based on our findings, we propose an extended protection model for deepfake threats. This model includes multiple measures active in different stages of the deepfake lifecycle, offering structured protection. Finally, we explore public awareness as a proactive defence strategy, delivering outreach and educational efforts to mitigate the risks of deepfake-driven social engineering attacks.

SARA CONCAS - ADVANCED STRATEGIES FOR DEEPFAKE DETECTION, 3D FACIAL RECONSTRUCTION, AND IRIS RECOGNITION IN MODERN SECURITY

Full Title: Beyond Reality: Advanced Strategies for Deepfake Detection, 3D Facial Reconstruction, and Iris Recognition in Modern Security
Institution: University of Cagliari
Supervisor: Gian Luca Marcialis, Giulia Orrù
Contact email: marcialis@unica.it

Abstract:
The rapid proliferation of deepfake technology has introduced a significant challenge in ensuring the integrity of multimedia content, with serious implications for privacy, security, and public trust. Deepfakes, created using advanced machine learning techniques, enable the realistic manipulation of video and image content, making it increasingly difficult to detect falsified media using conventional methods. While detection systems have quickly evolved to counter these threats, current solutions often struggle to generalize effectively when faced with novel, unseen manipulations. This thesis aims to develop more robust deepfake detection systems, focusing on improving their generalization capabilities. By integrating multiple detection techniques, such as visual artifact analysis, temporal consistency evaluation, and frame-based classifiers, this research explores the complementary strengths of di- verse models. The key contribution of this work is the adoption of a multi-modal approach that combines these classifiers through ensemble learning and score-level fusion techniques, addressing the limitations of individual models in handling a wide variety of deepfake manipulations. In parallel, the thesis also tackles challenges in related biometric security domains, including 3D face reconstruction and iris recognition. In 3D facial recogni- tion, advanced reconstruction techniques are explored to overcome the limitations of traditional 2D methods under uncontrolled conditions, enhancing the accuracy and robustness of recognition in surveillance applications. Additionally, this work investigates improvements in iris recognition technology, focusing on increasing the system'sresiliencetoenvironmentalvariationsanduser-specificfactors, contributing to more reliable and robust identification solutions. The proposed strategies not only improve the generalization of deepfake detection systems but also provide a robust framework for future developments in biometric security, from deepfake detection to 3D face reconstruction and iris recognition in real-world applications.

ZOHRA REZGUI - ENHANCED DEMOGRAPHIC PRIVACY IN FACE RECOGNITION: FROM IMAGES TO TEMPLATES

Full Title: Enhanced demographic privacy in face recognition: From images to templates
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://research.utwente.nl/en/publications/enhanced-demographic-privacy-in-face-recognition-from-images-to-t/
Link description: Enhanced demographic privacy in face recognition: From images to templates
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
This dissertation explores advanced methods to mitigate privacy risks associated with demographic profiling from both facial images and their numerical representations used for face recognition, known as templates. While templates are designed solely for identity verification and identification, they often reveal soft biometric attributes, such as gender and age, due to the overlap of identity and demographic features. This unintended leakage raises significant privacy concerns, particularly when demographic profiling is conducted without the user's consent. The research employs a dual approach. First, at the image level, adversarial attacks are applied as proof of concept to demonstrate their potential to fool demographic classifiers. This approach shows that it is possible to reduce the accuracy of demographic inference without degrading image quality or compromising face recognition performance. Second, at the template level, where identity and demographic features are deeply intertwined, adversarial techniques are extended to suppress demographic information from the face recognition templates while preserving recognition performance. Beyond noise-based adversarial methods, the dissertation introduces a model-based approach. By incorporating constraints during the training process, this approach generates demographic-invariant features and achieves stronger privacy protections with minimal trade-offs in verification performance. A final contribution is a method allowing dynamic control over the privacy-utility trade-off, which enables system operators to fine-tune the balance between privacy and performance without requiring extensive retraining. These contributions significantly enhance privacy-preserving technologies in biometric systems. They pave the way for face recognition applications that are not only effective but also ethically and legally compliant. By reducing demographic profiling risks and maintaining system performance, this work supports the development of adaptable and privacy-conscious biometric solutions.

ILIAS BATSKOS - THE PROBLEM OF FACE IMAGE MORPHING IN IDENTIFICATION DOCUMENTS

Full Title: The problem of face image morphing in identification documents: Analysis, prevention and detection
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://research.utwente.nl/en/publications/the-problem-of-face-image-morphing-in-identification-documents-an/
Link description: The problem of face image morphing in identification documents: Analysis, prevention and detection
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
This dissertation focuses on the problem of face image morphing in identification documents. Given the face images of two (or more) individuals, we can create a composite face image (a morph) using computer software that looks like both of them. One of the contributors (the accomplice) could use such a morph to apply for a new identification document, e.g. a passport. If that passport gets issued, the other contributor (the criminal) can then use it to conduct illegal activities and/or evade justice. This identity sharing scheme is known as a morphing attack and is a serious security vulnerability. In the first chapter, I introduce the subject of face morphing, talk about its historical use cases and analyse its causes and consequences. The second chapter is dedicated to improving morph generation algorithms, since being better prepared for what we might encounter in the real world is crucial. There, I present some improvements to a specific automated morph generation process, namely landmark-based morphing. The third chapter consists of a novel morphing prevention approach in ID document enrolment processes that, if implemented, would seriously limit the morphing attack threat. Next, I focus on morphing attack detection and present two methods based on image forensics that can be used to visualise morphing-related manipulation traces on digital images. Visualisation of morphing traces is very important as it can be used as evidence in a court of law. Finally, since the scale of the problem requires automated solutions, I use one of the aforementioned methods to create an automated morphing attack detection algorithm, so that any incriminating decision by the algorithm can be reviewed and explained by applying the corresponding image forensics method and visualising any possible traces.

MONITOR
MASTER-THESES

MARICA PASQUALI - GENERATION OF DOUBLE-IDENTITY FINGERPRINTS USING A CONDITIONAL GENERATIVE ADVERSARIAL NETWORK (CGAN)

Full Title: Generation of Double-Identity Fingerprints Using a Conditional Generative Adversarial Network (cGAN)
Institution: University of Bologna
Supervisor: Matteo Ferrara
Contact email: matteo.ferrara@unibo.it

Abstract:
Not available

NISHTMAN ANDISHA - FAIRNESS EVALUATION OF FIQA

Full Title: Skin Tone Fairness Evaluation of FIQA Algorithms based on 3D Morphable Face Models
Institution: Technical University of Denmark (DTU) and Hochschule Darmstadt (HDA)
Supervisor: Marcel Grimmer and Christoph Busch
Contact email: christoph.busch@h-da.de

Abstract:
Fairness in biometric systems requires accurate and unbiased skin tone classification. This study evaluates face image quality assessment algorithms to identify biases in skin tone estimation. Classification methods were employed based on predefined RGB color classes, utilizing the Google SkinTone guide with ten distinct skin tone categories. The datasets consisted of FFHQ and LFW images, supplemented by 10,000 synthetic images generated using StyleGAN and 50,000 hyperparameter controlled images. Additionally, a subset of 1,500 manually labeled images was incorporated to establish ground truth for evaluation. To improve accuracy, the TRUST model (Toward a Racially Unbiased Skin Tone Estimation) was utilized. This model reconstructs facial geometry using the FLAME 3D model and estimates albedo to separate intrinsic skin properties from lighting effects.

NATÁLIE IŘÍKOVÁ - RECOGNITION OF SKIN DISEASE TYPE IN FINGERPRINTS

Full Title: Rozpoznání typu onemocnění kůže v otiscích prstů
Institution: VŠB - Technical University of Ostrava
Supervisor: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
Contact email: martin@drahansky.cz

Abstract:
This thesis focuses on the analysis of fingerprints affected by dermatological conditions. The aim of the work was so design and verify an algorithm capable of automatically evaluating whether a fingerprint is suitable for further analysis and estimate the type of damage affecting it either localized or widespread. The algorithm was implemented in the Python programming language and employs standard image processing methods such as filtering, binarization, skeletonization and minutiae detection. A real-world dataset of fingerprint images from patients with various diagnoses was used for testing. The results show that the proposed approach can serve as a useful tool for preliminary fingerprint quality assessment in the context of skin disease, with the best performance achieved on fingerprints with localized damage.

PAVLA DRTILOVÁ - DETERMINATION OF HEAD TISSUE CHANGES

Full Title: Determination of Head Tissue Changes in 3D Models of Radiotherapy Patients
Institution: VŠB - Technical University of Ostrava
Supervisor: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
URL: https://dspace.vsb.cz/handle/10084/156959
Contact email: martin@drahansky.cz

Abstract:
This diploma thesis focuses on the detection of shape and volume changes in head tissues of patients undergoing radiotherapy. The teoretical part of the thesis provides an overview of head anatomy, pathological conditions treated with radiotherapy, radiotherapy and its side effects, description of linear acceleratos and use techniques, review of 3D camera types and analysis of software and algoritgms used for processing three-dimensional data. The practical part presents avaiable databases of 3D head models and proposes a methodology for processing 3D models. The models were modified in Blender 4.3 software, where tissue deformations simulating real changes occuring in oncological patiens were created. Based on the review of avaiable software tools and algorithms, suitable tools were selected for model analysis, along with the development of a custom algorithm in MATLAB r2023a. The designed algorithm enables the assessment of difference between the original and deformed models, generating outputs such as heatmaps, visualization of individual model layers, calculation of model volumes and their changes, and measurements of Hausdorff and Chamfer distances. The Fidentis Analyst II software was used for providing mainly visual data for model analysis.

MACIEJ SALWOWSKI - DIGITAL AND PHYSICAL ATTACK DETECTION

Full Title: Efficient Vision Language Models for Digital and Physical Attack Detection
Institution: Technical University of Denmark
Supervisor: Dr. Lazaro Janier Gonzalez-Soler
Contact email: lazaro-janier.gonzalez-soler@h-da.de

Abstract:
Recent research in biometric systems has made significant strides in addressing fraudulent practices. However, as detection methods improve, attack techniques become increasingly sophisticated. Attacks on face recognition systems can be broadly divided into physical and digital approaches. Traditionally, deep learning models have been the primary defense against such attacks. While these models perform exceptionally well in scenarios for which they have been trained for, they often struggle to adapt to different types of attacks or varying environmental conditions. These subsystems require substantial amounts of training data to achieve reliable performance, yet biometric data collection faces significant challenges including privacy concerns and the logistical difficulties of capturing diverse attack scenarios under controlled conditions. This work investigates the application of Vision Language Models (VLM) for detecting physical presentation attacks and digital morphing attacks in biometric systems. Focusing on open-source models under 8 billion parameters, the first systematic framework for quantitative evaluation of VLMs in security-critical scenarios through in-context learning techniques is established. The experiments demonstrate that VLMs achieve competitive performance in presentation attack detection task, outperforming some of the traditional CNNs without resource exhaustive training, and imply insightful trajectory for differential morphing attack detection challenge. The results validate VLMs as promising tools for improving generalization in attack detection.

THOMAS SCHUTH - BIOMETRIC TEMPLATE PROTECTION

Full Title: Improving the Current State-of-the-Art in Biometric Template Protection
Institution: Universität der Bundeswehr München
Supervisor: Osman Demir, Marta Gomez-Barrero
Contact email: marta.gomez-barrero@unibw.de

Abstract:
Biometric authentication systems have become integral to modern life, enabling convenient and secure access to devices, financial services, and restricted environments. These systems rely on distinctive physiological or behavioral characteristics — such as fingerprints, facial features, or iris patterns — which provide a more user-friendly and often more secure alternative to conventional passwords. However, the sensitivity of biometric data raises significant privacy and security concerns. Unlike passwords, biometric characteristics are permanent; if leaked, they cannot be reset or replaced, therefore biometric template protection is an active research topic.This field has emerged to address such vulnerabilities by developing methods to securely store and manage biometric data, preventing unauthorized access or misuse. Conventional cryptographic techniques like encryption are inadequate due to the biometric data's noise and variability, which preclude the exact matches required by traditional cryptographic operations. Consequently, specialized approaches are needed to ensure good security, privacy and performance results.Recent advancements in machine learning have introduced novel methods for biometric template protection. Neural Networks and related techniques have proven effective in feature extraction, transformation, and classification, improving the robustness and flexibility of protection mechanisms. This master's thesis leverages these advances to enhance state-of-the-art biometric template protection. This master thesis focuses on the iris as its modality, which is valued for its high distinctiveness and temporal stability, making it a strong candidate for reliable authentication. Three approaches were developed and rigorously evaluated for verification accuracy and presentation attack detection using publicly available datasets.The master thesis explains the fundamental theoretical foundations to ensure clear understanding of the experiments and situates the results within established field standards. Its primary aims are to advance biometric template protection techniques and to stimulate further research. Ultimately, this work seeks to improve the security and privacy of biometric systems, promoting their broader adoption and trustworthiness.

MATEJ MIOČIĆ - GENERATING PHOTOREALISTIC FACIAL COMPOSITES WITH DIFFUSION MODELS

Full Title: Generating Photorealistic Facial Composites with Diffusion Models
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Darian Tomašević
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=171779&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
Facial composites, also known as police sketches, are essential tools in law enforcement for reconstructing a suspect's appearance based on eye witness descriptions. Traditionally, forensic artists manually create these sketches by working closely with eyewitnesses, which is often slow and te dious. To simplify this process, modern law enforcement increasingly relies on advanced computer software. While deep learning has introduced several innovative approaches in recent years, the use of diffusion models for this task remains largely unexplored. We present Diff-FIT (Diffusion Facial Identification Technique), a novel framework for generating photorealistic facial composites using diffusion models. Diff-FIT enables fast generation of initial images from a textual description, followed by intuitive, sequen tial edits based on ongoing eyewitness input. Our approach generates facial composites with a preference comparable to existing methods, while enabling a greater range of facial variation and more diverse adjustments, without compromising identification performance or image quality. In a user study involving biometric experts and non-experts, facial composites generated by Diff-FIT were rated on par with those from state-of-the-art methods in both subjective evaluations and identification rates.

ELISA CARIA - EMOTION RECOGNITION THROUGH EEG BASED ON THE STUDY OF HEMISPHERIC LATERALIZATION

Full Title: Emotion Recognition Through EEG Based on the Study of Hemispheric Lateralization
Institution: University of Cagliari
Supervisor: Gian Luca Marcialis
Contact email: marcialis@unica.it

Abstract:
Automatic emotion recognition through EEG signals represents one of the most interesting and innovative challenges in the fields of neuroscience and artificial intelligence. In recent years, deep neural networks, known as Deep Learning models, have shown remarkable capabilities in the analysis of complex physiological signals, enabling the identification and classification of different emotional states with increasingly higher levels of accuracy. This work explores the main Deep Learning methodologies applied to electroencephalography, with particular attention to the most recent and high-performing models for emotion recognition. Through a critical review of existing architectures and experimentation on real data, the thesis investigates both the potential and the limitations of the techniques developed in the literature. In addition to aspects related to automatic classification, the work aims to verify the validity of the valence theory and the right-hemisphere dominance theory, with a particular focus on the contribution of different frequency bands and on highlighting the functional differences between the two cerebral hemispheres. The objective is to demonstrate how the integration of neuroscience and artificial intelligence can open up new application scenarios, from mental health monitoring to education, from road safety to immersive entertainment, promoting an increasingly deeper and more objective understanding of human emotional processes.

PEDRO DELGADO-DEROBLES - EXPLORING IDENTITY VERIFICATION THROUGH BEHAVIORAL PATTERNS IN VIDEOS

Full Title: Exploring Identity Verification through Behavioral Patterns in Videos
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Tolosana
URL: https://ieeexplore.ieee.org/document/11411089
Link description: Article published in IJCB 2025
Contact email: ruben.tolosana@uam.es

Abstract:
The rapid progress of generative models has enabled the creation of highly realistic talking-head avatars, capable of faithfully reproducing a person's visual appearance. While these avatars hold great potential for communication and entertainment, they also pose new security risks, as an impostor can take control of an avatar that looks identical to its legitimate owner. This scenario challenges traditional face recognition systems, which rely primarily on static appearance cues and are therefore ineffective against avatar-based impersonation. This Master's Thesis explores the use of dynamic behavioral traits, specifically facial motion patterns, as a novel biometric modality for verifying the identity of users behind photorealistic avatars. To this end, a lightweight and explainable verification system is proposed, based on Graph Convolutional Networks (GCNs) applied to facial landmark sequences, combined with an attention mechanism that captures temporal dynamics as intrinsic identity-specific patterns. Results demonstrate that facial motion provides a discriminative and robust signal for identity verification in avatar videos. Furthermore, the attention mechanism enhances interpretability by revealing which temporal segments contribute most to the verification decision, offering insights into the characteristic motion patterns learned for each individual. Overall, this work establishes a foundation for behavioral biometrics in synthetic media contexts, highlighting the potential of motion-based verification systems to counteract impersonation risks in emerging avatar technologies.

LEON TODOROV - DETECTION OF FACE FORGERIES WITH SELF-SUPERVISED LEARNING

Full Title: Detection of Face Forgeries with Self-Supervised Learning
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Marija Ivanovska Preskar
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=171822&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
In biometric identity verification, the growing fidelity of AI-synthesized faces is threatening the reliability of face recognition systems. Modern generative models can create extremely realistic facial forgeries that often evade detection by current methods. Among these, morphing attacks are especially dangerous: by digitally merging the faces of two or more individuals, they yield a single image that can fool face recognition systems into matching multiple identities, thereby facilitating identity fraud and other malicious exploits. Most Morphing Attack Detection (MAD) approaches use supervised learning on a fixed set of known morphing techniques. Such models often achieve high accuracy on morphs created by the same algorithms seen during training, but they tend to rely on method-specific artifacts and struggle to generalize to morphs from unseen techniques or under different data conditions. Unsupervised one-class methods avoid overfitting to specific attacks, but they often lack the sensitivity to detect the faint, distributed artifacts left by high-quality morphs. To overcome these challenges, a new face forgery detection framework with improved robustness and generalization is introduced. The approach uses self-supervised training on synthetic forgery artifacts, which helps the detector learn decision boundaries that are more generic and resilient. At the heart of the model, a gating mechanism fuses two complementary information streams: the high-level semantic features from a vision-language foundation model and the fine-grained spatial features from a high-resolution convolutional network. The semantic branch is built on a CLIP vision-language backbone and fine-tuned via Low-Rank Adaptation (LoRA) to adapt its image-text embeddings to the forgery detection task, enabling accurate discrimination between authentic and manipulated faces. In parallel, a high-resolution convolutional branch (based on HRNet) preserves detailed spatial information and aggregates multi-scale features, allowing it to capture even very subtle artifacts. An auxiliary segmentation module provides pixel-level guidance to this branch by distinguishing genuine facial regions from likely manipulated ones, which regularizes the training. By combining the CLIP branch's global semantic context with the convolutional branch's local artifact sensitivity, the model produces a well-balanced and highly discriminative representation for detecting face forgeries. The entire architecture is trained end-to-end with a composite loss that simultaneously enforces semantic alignment, segmentation consistency, and classification accuracy. Evaluated on diverse morphing benchmarks, the proposed method achieves state-of-the-art performance. It significantly outperforms both supervised and unsupervised baseline detectors, attaining an average Equal Error Rate (EER) of just 0.85%. Notably, the improvements are most pronounced on high-quality morphs generated by advanced GAN and diffusion models, highlighting the framework's resilience against next-generation forgery techniques.

DILARA CELEPI - BIAS OF BIOMETRIC QUALITY ASSESSMENT

Full Title: Potential Bias in Quality Components of Biometric Quality Assessment
Institution: Technical University of Denmark (DTU) and Hochschule Darmstadt (HDA)
Supervisor: Andre Dörsch and Christoph Busch
Contact email: christoph.busch@h-da.de

Abstract:
This thesis explores whether Face Image Quality Assessment (FIQA) contributes to demographic bias in biometric systems across skin tone, ethnicity, age, and gender. FIQA evaluates whether a given face image is suitable for face recognition, so any bias in this evaluation can lead to exclusion and unfair treatment. Ethnicity groups have traditionally been used to evaluate bias across demographic groups. However, this categorization is very broad and any specific disparity can be harder to identify. The Monk Skin Tone (MST) scale is used to measure how different quality components behave across varying skin tones. This thesis evaluates potential bias in quality components within the Open Source Face Image Quality (OFIQ) framework using both authentic and synthetic datasets. MST labels are automatically assigned to subjects by extracting pixels from the forehead and cheek regions. Fairness in the quality components was measured using four fairness measures: Gini Coefficient, Cubed Sample Quality Fairness Rate, Low-WeightedMean Score, and MeanDiscardGap Score. This thesis concludes that there are performance differences across quality components in OFIQ and that the proposed sclera based method improves fairness in the Luminance Mean quality component.

NIKOLA MARIĆ - MORPHING ATTACK DETECTION USING MULTIMODAL LARGE LANGUAGE MODELS

Full Title: Morphing attack detection using MLLMS
Institution: University of Ljubljana, Slovenia
Supervisor: Vitomir Štruc, Marija Ivanovska
URL: https://repozitorij.uni-lj.si/Dokument.php?id=215524&lang=slv
Link description: University repository
Contact email: vitomir.struc@fe.uni-lj.si

Abstract:
Face morphing attacks pose a significant threat to biometric security systems by enabling multiple individuals to authenticate with a single compromised credential i.e., a morphed face image. This thesis investigates the use of multimodal large language models (MLLMs) for morphing attack detection, demonstrating that foundation models trained on large-scale, heterogeneous data possess latent forensic capabilities that can be adapted for specialized security tasks. We evaluate four open-source models in a zero-shot setting, including Gemma3 27B, Qwen2.5-VL 32B, Llama-4 Scout 17B, and Mistral Small 3.1 24B, across diverse datasets covering landmark-based, GAN-based, and diffusion-based morphing attacks. Even without task-specific training, these models achieve measurable detection performance, confirming that multimodal language models inherently encode useful representations. To improve zero-shot detection reliability, we developed a structured forensic prompt, which guides the models through a systematic six-step procedure for detecting visual artifacts created during the blending of facial images. This structured prompting approach enhances both detection accuracy and interpretability of the outputs. The primary contribution of the thesis lies in parameter-efficient fine-tuning through Low-Rank Adaptation (LoRA). Using only 0.61% of trainable parameters, we fine-tuned Gemma-3 12B. This fine-tuned model substantially outperformed its zero-shot counterpart, reducing the average Equal Error Rate by more than half. It achieved near-perfect detection on landmark-based morphs, competitive results on challenging GAN-based and diffusion-based morphs. Overall, this research establishes multimodal large language models as a viable and promising direction for morphing attack detection, combining generalization and interpretability with competitive performance against state-of-the-art approaches.

VENDELA NJEGOVEC - FORENSIC AUTOMATIC SPEAKER RECOGNITION

Full Title: Forensic Automatic Speaker Recognition : Analyzing codecs for calibration and their impact on system performance
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://purl.utwente.nl/essays/105205
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
In this study the impact of audio codecs on the calibration performance of forensic automatic speaker recognition is analyzed, addressing challenges posed by mismatched conditions. Using the NFI-FRIDA (Netherlands Forensic Institute - Forensically Realistic Inter-Device Audio) database, a collection of speech recordings captured simultaneously with multiple recording devices relevant to forensic analysis, high quality audio samples are processed through various codecs to simulate real telephone speech and compared to actual telephone intercepts. The study uses an x-vector based automatic speaker recognition system, VOCALISE (Voice Comparison and Analysis of the Likelihood of Speech Evidence) for all experiments and system performance is measured in terms of calibration loss and cost of log likelihood ratio. The study reveals a significant performance loss due to codec mismatches and emphasizes the complexity of simulating telephone speech and replicating real world telephony conditions. Additionally, the study highlight the potential of cross-processing datasets with mismatched codecs to lower the calibration loss.

MARICA PASQUALI - GENERATION OF DOUBLE-IDENTITY FINGERPRINTS

Full Title: Generation of Double-Identity Fingerprints Using Conditional Generative Adversarial Networks
Institution: University of Bologna
Supervisor: Matteo Ferrara
Contact email: matteo.ferrara@unibo.it

Abstract:
It has been demonstrated that it is possible to generate double-identity fingerprints capable of deceiving current automatic recognition systems. However, fingerprints generated using existing approaches often exhibit artifacts that a trained human eye could detect. The aim of this thesis is the design and training of a generative artificial neural network capable of creating double-identity fingerprints with a high level of realism.

HANS HEJE - VISION LANGUAGE MODELS FOR PRESENTATION ATTACK DETECTION

Full Title: Vision Language Models for Presentation Attack Detection
Institution: Technical University of Denmark
Supervisor: Dr. Lazaro Janier Gonzalez-Soler
Contact email: lazaro-janier.gonzalez-soler@h-da.de

Abstract:
Presentation Attack Detection (PAD) remains a critical challenge in biometric security, particularly for face recognition systems vulnerable to presentation attacks. This thesis builds upon the current state of the art, which relies solely on the vision transformer while discarding the text transformer, by investigating the integration of soft biometrics—specifically facial attributes—into vision language models to improve PAD performance. A variety of models and experiments are conducted, including zero-shot PAD, zero-shot PAD using attributes, feature extraction, fine-tuning of vision transformers, fine-tuning of vision and text transformers with attributes, guided fine-tuning using attributes, and model fusion. Facial attributes are incorporated into the text encoder, while the foundation models' weights are based on FaRL—which is pretrained on significantly less data than the foundation models used in the state of the art—are employed to boost performance. LoRA layers are added during training to facilitate efficient fine-tuning. The results demonstrate that combining facial attributes with FaRL can potentially enhance the robustness and adaptability of PAD models, with the greatest improvements observed in zero-shot scenarios, having an increase in AUC of 3.3 percentage points and a decrease in HTER of 4.6 percentage points. These findings highlight the potential of integrating soft biometrics with domain-specific foundation models to strengthen biometric security.

JANA PUTOVÁ - FINGER VASCULAR STRUCTURE SENSING AND RECOGNITION DEVICE

Full Title: Zařízení pro snímání a rozpoznávání cévní struktury prstu
Institution: VŠB - Technical University of Ostrava
Supervisor: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
URL: https://dspace.vsb.cz/handle/10084/156958
Contact email: martin@drahansky.cz

Abstract:
This thesis is focused on the design and implementation of a device for capturing the vascular structure of the finger using near-infrared (NIR) imaging and the subsequent processing of image data for biometric identification purposes. A specialized imaging device was developed to acquire multi-view images of the finger, which were subsequently preprocessed using methods such as Gabor filtering, contrast limited adaptive histogram equalization (CLAHE), and morphological operations. Following preprocessing, the vascular structure was segmented using Otsu's thresholding method. The similarity between the segmented images was analysed using a correlation-based method, demonstrating that images with a small rotational difference exhibit a high degree of similarity, while images with greater rotation show a decrease in similarity. The results confirm the potential of multi-view imaging for enhancing biometric identification and simultaneously highlight the limitations of 3D reconstruction based solely on segmented data.

K.C KADOLKAR - VISUALIZATION OF DEEPFAKE DETECTION USING FORENSIC METHODS

Full Title: Visualization of Deepfake detection using forensic methods
Institution: University of Twente
Supervisor: Luuk Spreeuwers
URL: https://purl.utwente.nl/essays/105302
Link description: Visualization of Deepfake detection using forensic methods
Contact email: l.j.spreeuwers@utwente.nl

Abstract:
Abstract—The increased availability and ease of use of deep learning frameworks have led to a rise in the generation and distribution of deepfake images and videos 11. This has created a pressing need for algorithms capable of identifying and characterizing these manipulated media 12. While deep learning frameworks are a popular choice for such tasks, their black-box nature makes it challenging to understand or explain the features leading to a classification decision 13. This lack of explainability renders these methods unsuitable for scenarios where interpretability is essential 14. This study explores two approaches for deepfake detection: forensic methods and deep learning models. The forensic methods focus on visualizing specific artifacts in manipulated media, such as inconsistencies in blending, color, and texture in targeted facial regions like cheeks and eyebrows. These techniques enhance in- terpretability by highlighting anomalies and facilitating an under- standing of manipulations through visual evidence. Conversely, the deep learning approach employs a Convolutional Neural Network (CNN) trained with K-Fold Cross-Validation on the cheek, eyebrow, and full-frame regions, prioritizing classification accuracy over interpretability. A comparative analysis reveals the strengths and limitations of each method, emphasizing the trade-offs between accuracy and explainability. The findings contribute to the development of hybrid strategies that combine the strengths of forensic visu- alization with the predictive power of deep learning, advancing the field of deepfake detection. This increases the explanability of deep learning models by not only looking at the larger picture but also at specific parts which contain artifacts that can then be highlighted using forensic method.

ROSA HORNERO - BIOMETRIC RECOGNITION OF HUMAN GAIT USING INERTIAL SENSORS IN SMARTPHONES

Full Title: Biometric recognition of human gait using inertial sensors in smartphones
Institution: Universidad Autonoma de Madrid
Supervisor: Marta Robledo-Moreno
Contact email: marta.robledo@uam.es

Abstract:
In recent years, biometric recognition models have advanced thanks to the development of deep learning-based models. This has brought great benefits to various sectors, such as healthcare and security. These models identify individuals based on physical characteristics or behaviors that make them unique. Among biometric recognition techniques is the analysis of a person's gait pattern, known as gait recognition. This Master's Thesis explores the use of deep learning models for biometric gait recognition based on inertial sensors located in smartphones. To this end, experiments were conducted on three different tasks. First, a Transformer model was trained for user identification. Subsequently, work was carried out on classification models for two soft biometric characteristics: gender and age. When training the models, we used a widely used and validated database, such as the OUISIR database (characterised by highly controlled capture), as well as our own BehavePassDB database. This allowed us to evaluate the behaviour of the different models in a more realistic environment. The models achieved satisfactory results in the OU-ISIR database, confirming the validity of the approach and architectures used. However, when applying the system to the BehavePassDB database, captured in an uncontrolled environment, performance decreases significantly. This difference in performance reflects the dependence of these models on the quality and conditions of data acquisition. Therefore, to ensure reliable application in real-world contexts, it is important to have much more robust capture processing. In addition, the study provides a solid foundation for future work seeking to improve biometric gait recognition.

GUSTAV PEDERSEN - INTERPRETABILITY IN FACE IMAGE QUALITY ASSESSMENT

Full Title: Exploring Explainability and Interpretability in Face Image Quality Assessment Algorithms
Institution: Technical University of Denmark (DTU) and NTNU
Supervisor: Wassim Kabbani and Christoph Busch
Contact email: christoph.busch@ntnu.no

Abstract:
Face Image Quality Assessment (FIQA) algorithms provide a Unified Quality Score (UQS) or a Component Quality Measure (CQM). UQSs aim to describe the overall utility of a sample face image in a face recognition system, while CQMs aim to describe the quality with respect to a specific quality component. The best performing UQS FIQA algorithms are deep learning based models. Existing explainability methods attempt to explain how UQS FIQA algorithms make decisions. Some provide heatmaps visualising quality estimates of small parts of the image, down to pixel level. We present a new FineGrained Face Parsing (FGFP) algorithm, parsing the face image into medical literature based regions that are larger than the small parts used in other methods. Through a region removal experiment, we analyse how important for quality a UQS FIQA algorithm considers each region. We further present a Face Region Quality Estimation (FRQE) algorithm for explainability of UQS FIQA algorithm quality decisions, which estimates the quality of each region in a sample face image and visualises them in a heatmap. FRQE heatmaps are shown to have higher interpretability than heatmaps from an existing method. CQMs inherently provide explanation of why images are low quality, but a deep learning based UQS FIQA may not find quality components equally important for quality. We use random forest models to explain how important quality components are for UQS FIQA algorithm decisions. We further analyse the performance of UQS FIQA algorithms based on CQMs and random forests, and find they are outperformed by state of the art UQS FIQA algorithms.

TAMÁS ENDREI - AERIAL-GROUND PERSON RE-IDENTIFICATION IN SURVEILLANCE SCENARIOS

Full Title: Aerial-Ground Person Re-Identification in Surveillance Scenarios
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Tolosana
URL: https://ieeexplore.ieee.org/document/11410726
Link description: Article published in IJCB 2025
Contact email: ruben.tolosana@uam.es

Abstract:
Person re-identification (Person ReID) across aerial and ground viewpoints is an emerging and critical challenge in large-scale surveillance, public safety, and security applications. Traditional Person ReID research has primarily focused on ground-only scenarios, where camera viewpoints are relatively consistent. However, bridging the aerial-ground domain gap introduces significant challenges, including extreme viewpoint differences, scale variations, motion blur, and occlusions. This Master's Thesis addresses these challenges through the AG-VPReID 2025 Challenge, the first large-scale video-based competition specifically designed for high-altitude (80–120m) aerial-ground ReID. The challenge leverages the AG-VPReID dataset, which comprises 3,027 identities, over 13,500 tracklets, and roughly 3.7 million frames captured from UAVs, CCTV, and wearable cameras, representing diverse real-world surveillance conditions. The core contribution of this Master's Thesis is the proposal of X-TFCLIP, the winning solution of the challenge. X-TFCLIP combines attention-based temporal reasoning with CLIP-derived feature representations to achieve robust cross-view matching across aerial and ground cameras. The method integrates multi-modal cues and leverages temporal consistency to improve identification accuracy under challenging conditions. Experimental results demonstrate that X-TFCLIP attains 72.28% Rank-1 accuracy for aerial-to-ground ReID and 70.77% for ground-to-aerial ReID, outperforming existing baselines and state-of-the-art approaches. This Master's Thesis further provides a detailed analysis of the dataset, the baseline methodologies, and a series of ablation studies that quantify the contributions of different components of X-TFCLIP. The results highlight the importance of combining temporal modeling, foundational model-based feature extraction, and attention mechanisms to address the complexity of aerial-ground person ReID, offering valuable insights for future research in large-scale, multi-view surveillance systems.

IRIS BJÖRK - AGE MANIPULATION

Full Title: Age manipulation with Latent Diffusion Models
Institution: Hochschule Darmstadt and DTU
Supervisor: Christoph Busch and Marcel Grimmer
Contact email: christoph.busch@h-da.de

Abstract:
Face verification often fails due to a large age difference between a person and their photo. Advances in the field of simulating facial aging are also important when it comes to identifying missing individuals that for example have been missing for a large period. This study researches the possibility of using Latent Diffusion Models to perform age manipulation of facial images, i.e. age regression and age progression. The use of Latent Diffusion Models allows for customizing its conditioning procedure. The conditioning takes in labels that will give the model more information about the input image and using inference does have the option of manipulating the conditioning factor. The methods explored in the condition procedure are MagFace face embeddings to preserve the identity of an individual and a one hot encoder to represent the age of the individual. This research shows that a one hot encoder can be used with success to perform age manipulation on individuals. Taking a look at the evaluation procedure the model was able to generate images with moderate visual quality and it was able to preserve identity for a range of ages. Estimating the age of the generated images the data points from the age estimation of the generated images and the real image database follow the same trend, having difficulty estimating age for underrepresented ages. This study does show promising results in using Latent Diffusion Models in the field of age simulation.

JERNEJ SABADIN - GENERATION OF SYNTHETIC FACES WITH DIFFUSION MODELS

Full Title: Generation of synthetic faces with diffusion models
Institution: University of Ljubljana, Slovenia
Supervisor: Vitomir Štruc, Darian Tomašević
URL: https://repozitorij.uni-lj.si/Dokument.php?id=212295&lang=slv
Link description: University repository
Contact email: vitomir.struc@fe.uni-lj.si

Abstract:
Effective training of face recognition (FR) models requires large datasets that are precisely annotated with individual identities. Acquiring such datasets is highly time-consuming, and their use is often restricted due to privacy protection requirements. For this reason, in this master's thesis we introduce a new generative diffusion model, IDSync, which extends the Arc2Face method and enables the generation of high-quality facial images. By incorporating an additional classification-based objective function and a customized training procedure, IDSync preserves the original identity of individuals while producing visually convincing synthetic faces. The set of synthetic facial images generated by the model is evaluated using various metrics: cosine inter-class and intra-class similarity of extracted features, the distribution of face orientation angles, the Fréchet distance between features of synthetic and real examples, and other statistical measures. The main indicator of the quality of the artificially created dataset is how effectively a face recognition model can learn from it. This is measured by verification accuracy on standard benchmark datasets for FR model evaluation. The results show that data generated with the IDSync method are more suitable for training face recognition models than data produced with Arc2Face, as further confirmed by the mentioned metrics. Encouraged by these findings, we scale up training with IDSync to a larger volume of training data and present the obtained results. The thesis also includes a sensitivity analysis of hyperparameters for a deeper understanding of the impact of the additional objective function, as well as an ablation study. -- Translated from Slovene

FERNANDO FERNANDEZ DEL CERRO - GENERATION OF SYNTHETIC ON-LINE SIGNATURES FOR BIOMETRIC RECOGNITION

Full Title: Generation of Synthetic on-line Signatures for Biometric Recognition
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Vera-Rodriguez
Contact email: ruben.vera@uam.es

Abstract:
This Thesis presents a comprehensive experimental study on generative strategies for on-line handwritten signature synthesis and their application as data augmentation technique for online signature verification systems. We evaluate four complementary approaches: (i) generation of new synthetic identities by training TGANs on a complete real database, (ii) identity-specific few-shot and one-shot synthesis by fine-tuning or training TGANs from limited per-user samples, (iii) letter-level synthesis by training individual TGANs per alphabet letter and reconstructing full signatures from the generated letters, and (iv) targeted skilled forgery generation, assessing whether and how the same generative pipelines can be adapted to produce convincing synthetic skilled forgeries. Generated samples were assessed with predictive and discriminative scores as well as DET curves under standard verification protocols (1vs1, 1+3vs1, 4vs1). For verification we used the TA-RNN state-of-the-art verifier and the DeepSignDB mobile subsets for training and evaluation. We further compared our results against established synthesizers [1, 2] by repeating the enrichment-and-retrain procedure and plotting corresponding DET curves across noise-factor settings. Results quantify the trade-offs between scalability, identity-specific fidelity, and practical applicability: few-shot fine-tuning yields visually faithful per-user variants but is laborious to scale, one-shot expansion provides a practical route to dataset augmentation for verification models, and letter-level synthesis offers a modular alternative whose end-to-end quality compares favorably against prior work. Our experiments on forgery synthesis demonstrate the considerable difficulty of producing truly authentic skilled forgeries; nevertheless, we were successful in generating synthetic forgeries that, when used judiciously, provided measurable improvements to verifier training. These results both illustrate the practical challenges of perfect forgery realism and reinforce the practical value of forgery-free augmentation strategies used elsewhere in this Thesis. Overall, the experiments show that carefully constrained generative pipelines can produce synthetic signatures that materially benefit downstream verification systems.

RADIM HOMOLA - POSITIONING EQUIPMENT FOR PHOTOGRAMMETRY

Full Title: Polohovací zařízení pro fotogrammetrii
Institution: Faculty of Information Technology, Brno University of Technology
Supervisor: Ing. Vojtěch Mrázek, Ph.D.; Co-Supervisor: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
URL: https://www.vut.cz/studenti/zav-prace/detail/165200
Contact email: radimhomola579@gmail.com

Abstract:
This thesis focuses on the design and implementation of a positioning device designed to take images of objects from all sides. The resulting photos are used as input data for photogrammetric processing, the aim of which is to create an accurate 3D model of the object including texture. The proposed system uses four cameras and a rotation mechanism to ensure uniform rotation of the object. The device also allows storing the sensing parameters in the form of called "user profiles", which simplifies the repeated imaging of similar objects without the need for manual configuration. In this way, the user simply inserts the object, sets the configuration or loads the profile and the device then autonomously performs the entire image capturing process.

MÁRK GYÖNGYÖSI - FACIAL IMAGE QUALITY ASSESSMENT

Full Title: Implementation of InContext Learning for Facial Image Quality Assessment Evaluation and Compliance
Institution: Technical University of Denmark (DTU) and Hochschule Darmstadt (HDA)
Supervisor: Ana Estrada Real, Christian Rathgeb and Christoph Busch
Contact email: ana.estrada-real@h-da.de

Abstract:
Facial image quality assessment (FIQA) is essential for ensuring reliable performance in face recognition (FR) systems. Existing FIQA algorithms estimate quality through feature vectors but provide limited interpretability. This thesis investigates whether vision capable Large Language Models (LLMs) can complement existing FIQA workflows. A set of state of the art LLMs were evaluated on a dataset containing face images. Models were tested on four tasks: (1) binary classification of standard compliance, (2) identification of specific defects, (3) prediction of quality scores comparable to FIQA generated quality scores, and (4) generation of natural language explanations that justify the model's decision. Multiple prompt variants were tested to measure the effect of instruction detail on performance. The results show that larger models benefit from extended context, whereas smaller models frequently misinterpret instructions or deviate from the expected result. Across models, subject related defects (e.g., face obstructions, expression) are detected more consistently than capture related defects (e.g., illumination, resolution, background). Qualitative analysis further reveals that explanations remain fluent and confident even when incorrect.

MONITOR
BACHELOR-THESES

FILIP THUNBERG - IMPROVING OCULAR RECOGNITION WITH SYNTHETIC DATA

Full Title: Improving Ocular Recognition with Synthetic Data
Institution: Halmstad University, Sweden
Supervisor: Fernando Alonso-Fernandez, Kevin Hernandez-Diaz
URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-56447
Contact email: feralo@hh.se

Abstract:
Ocular recognition is a form of biometric identification that gained significance after the widespread use of face masks during the COVID-19 pandemic. Modern recognition systems are built upon deep learning methods, such as Convolutional Neural Networks, which require large datasets to be trained. However, acquiring extensive datasets of face and ocular images is hard to obtain due to privacy regulations, raising the question of whether synthetic data can be an alternative or complement. Tests were carried out on recognition models trained on real and synthetic data, with various Python programs. While metrics (e.g. Rank-1 rate) were promising, the overall performance, especially Equal Error Rate, did not meet required safety thresholds for a biometric recognition system.

LUCA CAMILLINI - DEVELOPMENT OF A WRAPPER FOR THE MCC SDK AND INTEGRATION WITH AI MODELS

Full Title: Development of a Wrapper for the MCC SDK and Integration with AI Models
Institution: University of Bologna
Supervisor: Matteo Ferrara
Contact email: matteo.ferrara@unibo.it

Abstract:
This thesis focuses on the development of two neural networks for assessing the similarity between pairs of fingerprint images. The proposed models integrate the Minutiae Cylinder Code (MCC), a state-of-the-art algorithm for minutiae extraction and comparison, with convolutional neural networks, in order to obtain accurate similarity estimations. The work describes the construction and management of the dataset, the design choices and optimizations of the neural network models, and the adopted strategies.

PHILIPP SCROCK - DETECTION OF FACIAL FILTERS

Full Title: Analysis and Detection of Facial Filters using Face Beauty
Institution: Hochschule Darmstadt (HDA)
Supervisor: Juan Tapia and Christoph Busch
Contact email: christoph.busch@h-da.de

Abstract:
Although facial attractiveness seems subjective, facial retouching is widely spread in social media, advertisements and even applied in professional photo studios to let the individuals appear younger, remove wrinkles and skin impurities and generally speaking: enhance the beauty. This is not a problem itself, but when retouched images are used as biometric samples and enrolled in a biometric system, it is one. Since previous work has proven facial retouching to be a challenge for face recognition systems, detection of facial retouching becomes increasingly necessary. This work analyzes changes in beauty assessment algorithms and quality assessment algorithms of retouched images, assesses different feature extraction methods for artificial intelligence based retouching detection and evaluates whether face beauty and face quality can be exploited to enhance the detection rate. An assumption can be made, that both provide useful features for the detection process. This study shows that even though face quality decreases while face beauty increases when a retouched sample is evaluated, face beauty and face quality do not measure the same features. Experiments conducted reveal that besides fusing multiple feature extraction methods, applying beauty scores improves the detection rate while face image quality has a very low impact when used to improve the detection rate. Detection results achieved on face filters not seen by the model during the training process are just above 1% average Equal-Error-Rate. Additionally it is shown that this rate can be further improved when using Machine Learning for the fusion process instead of a fusion function.

STEFANO LILLIU - EVALUATION OF THE ROBUSTNESS OF STEGANOGRAPHIC TECHNIQUES AGAINST MANIPULATIONS AND MORPHING ATTACKS

Full Title: Evaluation of the Robustness of Steganographic Techniques Against Manipulations and Morphing Attacks
Institution: University of Cagliari
Supervisor: Giulia Orrù, Marco Micheletto
Contact email: giulia.orru@unica.it

Abstract:
In identity recognition systems, used in critical contexts such as airport security checks, safeguarding the authenticity and integrity of images is an essential requirement to ensure high security standards. The evolution of digital manipulation techniques, particularly facial morphing, represents a growing threat to the reliability of such systems, as it allows faces in images to be altered in an extremely sophisticated way that is difficult to detect. This thesis aims to evaluate the robustness of a steganographic technique against different types of manipulations, both accidental and intentional, with a particular focus on threats arising from image morphing. The analysis was conducted by considering three fundamental aspects: the ability of steganography to guarantee image authenticity while preserving integrity, its resistance to unintentional manipulations, and the potential use of steganography as a tool to counter morphing attacks. The experimental results highlighted significant critical issues in the robustness of the steganographic technique analyzed. In particular, it was observed that most of the applied manipulations compromised the ability to recover the hidden information.

ADRIAN STERNER - USEFULNESS OF SYNTHETIC DATA IN BIOMETRIC RECOGNITION

Full Title: Usefulness of Synthetic Data in Biometric Recognition
Institution: Halmstad University, Sweden
Supervisor: Fernando Alonso-Fernandez, Kevin Hernandez-Diaz
URL: https://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-56564
Contact email: amomas@gmail.com

Abstract:
Ocular recognition plays a crucial role in scenarios where masks or partial faces limit the use of face recognition. However, privacy regulations and restrictions have hindered access to large-scale public databases necessary for training and evaluating recognition models. This thesis investigates whether synthetic face data can substitute real images while retaining the detail required for ocular recognition. Ocular crops were extracted from two real datasets, VGGFace2 and AgeDB, and from two synthetic datasets, GanDiffFace and DCFace. We evaluated five ResNet50 models trained under different conditions: VGGFace2 (face), VGGFace2 (ocular), GanDiffFace (ocular), Glint360K (face baseline), and ImageNet (baseline). Identification performance was measured using Rank-1 Accuracy, and verification was measured using Equal-Error Rate (EER). The model trained only on synthetic ocular data achieved 99% Rank-1 Accuracy and 4.9% EER on synthetic test data, but performance dropped to below 15% Rank-1 Accuracy and approximately 32% EER on real ocular images. In contrast, the model trained on real ocular images reached 68% Rank-1 Accuracy and 11.6% EER on real data, and 84% Rank-1 Accuracy and 9.6% EER on synthetic data. These results suggest that while the ocular region of current synthetic faces is suitable for benchmarking, they are not yet a suitable replacement for real data in training and evaluating models intended for real-world deployment.

ANDRES HUERGO-PEREA - BIOMETRIC RECOGNITION OF IN-AIR SIGNATURES USING MOBILE DEVICES

Full Title: Biometric recognition of in-air signatures using mobile devices
Institution: Universidad Autonoma de Madrid
Supervisor: Ruben Vera-Rodriguez
Contact email: ruben.vera@uam.es

Abstract:
Authentication systems in smartphones are becoming increasingly important to ensure the security of the information managed on these devices. However, the most widely used systems rely on single authentication, which leaves the device vulnerable to any potential failure they may experience. The motivation behind this work is to study the concept of continuous authentication as a complement to single authentication systems, as well as the possible biometric recognition systems based on an individual's behavior when handling mobile devices. This work aims to study the concept of in-air signatures as a behavioral biometric trait, to understand the method used for their capture and the signals that define them, and to analyze their feasibility within a biometric recognition system. On one hand, this work delves into the nature of the BehavePassUAM database, the techniques and conditions under which it was collected, and the various sensors involved in its acquisition. Imitations of the in-air signatures available in the database are also carried out to simulate realistic scenarios involving impostors. In addition, the possibility of generating three-dimensional representations of in-air signatures is explored as a complementary mechanism for biometric recognition based on handwritten signatures. On the other hand, the performance of algorithms such as Dynamic Time Warping and Sequential Forward Selection is investigated for the analysis of local features of in-air signatures. The results obtained, measured using the Equal Error Rate metric, reflect the potential of certain features to distinguish between individuals. In conclusion, despite the high variability of the data used, this work demonstrates that the development of a biometric recognition system based on in-air signatures captured with a smartphone is feasible, paving the way for future research that considers other types of algorithms or the integration of additional behavioral traits.

DANIELE FENU - ADVERSARIAL ATTACKS AGAINST FINGERPRINT-BASED BIOMETRIC DEVICES

Full Title: Adversarial Attacks Against Fingerprint-Based Biometric Devices
Institution: University of Cagliari
Supervisor: Marco Micheletto, Giulia Orrù
Contact email: marco.micheletto@unica.it

Abstract:
Fingerprint-based biometric systems are widely used for authentication due to their practicality and reliability. However, these systems are subject to security vulnerabilities, particularly so-called presentation attacks, in which artificial reproductions of fingerprints are used to deceive the sensor. To counter such threats, modern biometric systems integrate Presentation Attack Detection (PAD) modules to distinguish artificial fingerprints from genuine ones. Despite this protection, especially in recent years, a new vulnerability has emerged: adversarial attacks, which are able to compromise the effectiveness of biometric systems even in the presence of PAD modules, particularly when carried out directly at the sensor level. This thesis analyses adversarial attacks in the physical domain, with the aim of compromising the system's accuracy already during the fingerprint acquisition phase. After introducing the fundamental concepts of biometrics and the architecture of fingerprint biometric systems, including methods for generating artificial fingerprints, the work will focus on the design of digital perturbations, which will then be transferred to the physical domain. These perturbations are designed to compromise the image acquired by the sensor, in order to evade recognition mechanisms and assess the overall robustness of the system.

DAVIDE GIANNETTI - DATA AUGMENTATION FOR TRAINING FACIAL MORPHING DETECTION SYSTEMS

Full Title: Data Augmentation for Training Facial Morphing Detection Systems
Institution: University of Cagliari
Supervisor: Giulia Orrù, Marco Micheletto
Contact email: giulia.orru@unica.it

Abstract:
In recent years, the evolution and widespread adoption of biometric systems have made the face one of the most commonly used personal identifiers in authentication and identity verification processes, particularly in electronic documents such as passports and identity cards. However, this widespread use has exposed these systems to various classes of attacks, including morphing attacks, namely the circumvention of systems through a process in which two different faces are merged into a single image that is acceptable for both subjects involved. This type of attack represents a concrete threat to border security and to trust in automated biometric systems. To counter these threats, Morphing Attack Detection (MAD) systems have been developed [44], with the aim of recognizing and flagging morphed images so that they can be blocked in real time. However, the generalization capability of these systems is often limited: small changes in morph generation methods or in the data distribution can cause a drastic drop in performance. At the same time, recent developments in the field of generative models, particularly diffusion models, are opening up new possibilities not only for the synthesis of realistic faces, but also for the creation of morphs that are increasingly difficult to detect. On the one hand, these tools represent a threat, as they enable the creation of new generations of morphing attacks. On the other hand, they also represent a resource, since they can be exploited to improve the training of MAD systems through data augmentation techniques.

MAXIMILIAN RUSSO - MULTI-INSTANZ-ANSATZ FÜR FINGERABDRUCKSMERKMALE

Full Title: Multi-Instanz-Ansatz zur Dimensionalitätsreduktion DNN-extrahierter Fingerabdrucksmerkmale
Institution: Hochschule Darmstadt
Supervisor: Prof. Dr. Christian Rathgeb
Contact email: florian.bayer@h-da.de

Abstract:
Die fortschreitende Digitalisierung erfordert sichere und zugleich benutzerfreundliche Verfahren zur Authentifizierung von Personen. Klassische Methoden wie Passwörter oder PINs sind in der Praxis entweder unsicher, wenn sie zu einfach gewählt werden, oder schränken die Nutzerfreundlichkeit ein, wenn sie komplex gestaltet sind. Biometrische Systeme stellen daher eine vielversprechende Alternative dar, da sie auf unverwechselbaren, körpergebundenen Merkmalen basieren und sowohl ein hohes Maß an Sicherheit als auch einfache Bedienbarkeit ermöglichen. Fingerabdrücke zählen hierbei zu den am weitesten verbreiteten biometrischen Merkmalen. Gleichzeitig stellt die Speicherung und Verarbeitung biometrischer Daten jedoch hohe Anforderungen an Datenschutz und Datensicherheit, da diese Merkmale im Gegensatz zu Passwörtern nicht ohne Weiteres austauschbar sind. Die Datenschutz-Grundverordnung (DSGVO) verlangt deshalb ausdrücklich, dass biometrische Daten mit den bestmöglichen technischen Schutzmaßnahmen, insbesondere durch starke Verschlüsselungsverfahren, gesichert werden. Eine besonders geeignete Methode stellt in diesem Zusammenhang die homomorphe Verschlüsselung dar, die Vergleiche direkt auf verschlüsselten Daten ermöglicht. Ihr Nachteil liegt jedoch in einem bislang sehr hohen Rechenaufwand, wodurch praktische Anwendungen derzeit noch eingeschränkt sind. Die vorliegende Arbeit widmet sich daher der Frage, wie sich der Rechen- und Speicheraufwand bei der Verarbeitung von Fingerab- druckmerkmalen reduzieren lässt, ohne die Erkennungsleistung erheblich zu beeinträchtigen. Hierfür wurden Merkmalsvektoren, die zuvor mit tiefen neuronalen Netzen (DNN) extrahiert wurden, auf verschiedene Weise dimensional reduziert und anschließend im Hinblick auf ihre Klassifikationsleistung analysiert. Untersucht wurden sowohl Einzel-Instanz-Ansätze, bei denen nur ein Fingerabdruck betrachtet wird, als auch Multi-Instanz- Ansätze, die mehrere Fingerabdrücke kombinieren. Die Ergebnisse zeigen, dass eine Verringerung der Dimensionalität grundsätzlich möglich ist, ohne dass die Erkennungsleistung in erheblichem Maße leidet. Insbesondere der Einzel-Instanz-Ansatz mit Binärquantisierung und Interleaving erlaubt eine drastische Reduktion. Sowohl die Bitanzahl pro Eintrag als auch die Anzahl der Merkmale können reduziert werden, ohne gravierende Einbußen hinsichtlich der Klassifikationsgüte. Im Multi-Instanz-Ansatz erwies sich der AddTwo-Ansatz als besonders vielversprechend. Dabei werden die Merkmalsvektoren zweier aufeinanderfolgender Fingerabdrücke elementweise addiert, sodass die Information beider Finger bei unverändertem Speicher- und Rechenaufwand gegenüber der Verarbeitung eines einzelnen Fingers genutzt werden kann. Der AddTwo-Ansatz hat auch bei einer reduzierten Feature-Länge stabile Ergebnisse liefert. Insgesamt zeigte sich jedoch, dass Multi-Instanz-Ansätze keinen klaren Vorteil gegenüber Einzel-Instanz-Ansätzen bieten und in manchen Fällen sogar leicht schlechtere Ergebnisse erzeugen.

BARTLOMIEJ BAUT - SIGNATURES IN THE AIR AS A NEW METHOD FOR AUTHENTICATING INDIVIDUALS

Full Title: Signatures in the air as a new method for authenticating individuals and securing data in the digital world
Institution: Wroclaw University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: wojciech.wodo@pwr.edu.pl

Abstract:
Biometric techniques, despite their rich history, still leave plenty of room for research into adapting ever newer solutions to enhance human security around the world. For this reason, for the purpose of this thesis, a system based on behavioral biometrics of digital signatures made over-the-air to a camera was built and analyzed. From a technical point of view, the project was divided into modules for registering biometric data, extracting features from the signatures made, and classifying the information provided and processed accordingly. In addition to the description of the aforementioned tools, the paper presents the course and results of an on-site study conducted on a group of more than 30 people who agreed to test the system by submitting their signatures and participated in a survey evaluating the presented solution. Another important part of the text is the results of the study of the overall effectiveness of the developed tool in correctly authenticating people, which are presented with graphs containing the results of the FAR (False Acceptance Rate) and FRR (False Rejection Rate) coefficients depending on the decision thresholds used in the system. One of the last sections of this paper compares the results obtained from the developed classifier against off-the-shelf machine learning models tested on the same data samples. Finally, the advantages, disadvantages and limitations of the built system are presented, and possible perspectives for its future development are indicated.

PAULINA OTLIK - IMPLEMENTATION OF SELECTED ISO/IEC 29794-5 VERIFIERS AND PROPOSING ALTERNATIVES

Full Title: Implementation of selected ISO/IEC 29794-5 verifiers and proposing alternatives
Institution: Wroclaw University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: wojciech.wodo@pwr.edu.pl

Abstract:
Face recognition is currently the most popular form of biometric verification. As the effectiveness and security of this solution increase, so does its use in specialized fields. Considering that the verification process involves thousands of people, often under varying lighting conditions and with equipment of different parameters, biometric samples are of mixed quality. Therefore, there is a need to define the conditions under which a biometric sample is objectively good for a face recognition system. To address this, the international standard ISO/IEC 29794-5:2023 is being developed, with defined quality verifiers, along with a description of suggested implementation. The work on the standard is still in progress, but the majority of substantive work has already been completed, and it's on this work that the following solutions are based. This paper includes the implementation of two systems for assessing the face image quality based on selected standard's verifiers. The first system follows the implementation suggested directly from the standard, while the second utilizes the latest scientific and commercial solutions. Ultimately, these systems are compared using a database of photographs, differentiated by demographics and quality.

ROK PISTOTNIK - ANALYSIS AND OPTIMIZATION OF MODELS FOR AUTOMATIC FACE RECOGNITION

Full Title: Analysis and optimization of models for automatic face recognition based on feature visualization
Institution: University of Ljubljana, Slovenia
Supervisor: Vitomir Štruc
URL: https://repozitorij.uni-lj.si/Dokument.php?id=212296&lang=slv
Link description: The thesis is in Slovene
Contact email: vitomir.struc@fe.uni-lj.si

Abstract:
In this thesis, we present methods for reducing the influence of irrelevant facial characteristics in biometric face recognition, thereby increasing the reliability of verification under changes in illumination and face orientation. Each image is first represented in a multidimensional identity space, and then, through centroid analysis, we identify directions that describe variations in identity-related features. Using these directions, we quantify the expression of undesired facial characteristics with a global average and subsequently eliminate them with several derived methods. We evaluate the proposed approaches on modern face verification models such as ArcFace, CosFace, AdaFace, and SwinFace. For our experiments, we used two datasets, MultiPIE and CPLFW. The performance measure was the operating points on ROC curves. The results confirm that the methods improve verification accuracy, although none proves to be universally best across all architectures. The two most effective approaches for eliminating facial characteristic embeddings were: transforming the input embedding in such a way that the test and prototype embeddings encode the same facial characteristics (e.g., faces at identical viewing angles), and computing the average across all classes of facial characteristics. Possibilities for further development include describing directions of facial characteristic changes with functions, selecting specific directions of change depending on the model architectures, choosing a more suitable dataset, and incorporating multiple facial characteristics simultaneously when determining directions of change. (Translated from Slovene)

MATTIA SENNI - ANALISI E SVILUPPO DI ALGORITMI PER LA VALUTAZIONE DELLA QUALITÀ DELLE IMMAGINI DEL VOLTO

Full Title: Analisi e sviluppo di algoritmi per la valutazione della qualità delle immagini del volto
Institution: Università di Bologna
Supervisor: Annalisa Franco
Contact email: annalisa.franco@unibo.it

Abstract:
L'uso delle tecniche di visione artificiale per il riconoscimento delle persone tramite il volto è in costante aumento, grazie alla diffusione dei sistemi di riconoscimento biometrico automatico. In questi contesti, è fondamentale garantire un'acquisizione controllata e standardizzata delle immagini facciali, al fine di ridurre errori di riconoscimento e vulnerabilità a minacce come il face morphing. Una cattiva acquisizione può compromettere l'intero processo biometrico, esponendo il sistema a minacce quali la falsificazioni e riducendone l'affidabilità. Questo progetto contribuisce allo sviluppo ed alla valutazione di un software che ha l'obbiettivo di implementare un draft ISO, volto a valutare la qualità dell'acquisizione delle immagini facciali secondo diverse metriche.

BARTLOMIEJ PIOTROWSKI - KEYSTROKES DYNAMICS IDENTITY MODELS BASED ON FORCE BIOMETRICS USING HALL EFFECT

Full Title: Identity models based on keystroke force biometrics using keyboards with switches based on Hall Effect technology
Institution: Wroclaw University of Science and Technology
Supervisor: Wojciech Wodo
Contact email: wojciech.wodo@pwr.edu.pl

Abstract:
The main goal of this engineering thesis was to verify whether the use of keystroke force as an additional descriptor in biometric systems using keystroke dynamics biometry will contribute to a potential decrease in error rates. As part of the thesis, a biometric system was developed that, based on the previously mentioned keystroke force and two other popular features used in this biometry - dwell time and flight time, allowed for the identification of users based on their typing dynamics, thus enabling the analysis of the studied issue. The tests carried out showed that the keystroke force does not meet the expectations in terms of the effectiveness of minimizing error rates. This indicates the possibility of a suboptimal selection of mathematical methods used for signal processing. Despite this, the thesis provided valuable conclusions regarding the challenges related to the design of biometric systems, as well as the possibilities of potential development of the developed solution, including the use of other descriptors and statistical methods, or the use of neural networks. Another important aspect would be to collect a larger research sample, which would allow for a greater scope for analysis.

NICOLÒ PENSERINI - GENERAZIONE DI VIDEO SINTETICI PER IL RICONOSCIMENTO DI VOLTI

Full Title: Generazione di video sintetici per il riconoscimento di volti
Institution: Università di Bologna
Supervisor: Annalisa Franco
Contact email: annalisa.franco@unibo.it

Abstract:
Con l'avvento e il sempre più crescente impiego dei sistemi di intelligenza artificiale è stato possibile affrontare in modo nuovo molti problemi che da sempre hanno interessato vari ambiti dell'attività umana. Nell'ambito della visione artificiale, uno dei compiti per cui possono essere utilizzati modelli di intelligenza artificiale è il riconoscimento di volti all'interno di immagini o video. Per l'addestramento di questi modelli, tuttavia, sono necessarie grandissime quantità di dati e, sfruttando i tradizionali dataset reali si può incorrere in problematiche relative alla difficoltà di raccolta, alla scarsa variabilità o a restrizioni collegate alla privacy. In questo scenario stanno sempre di più emergendo dataset sintetici, i cui dati sono generati attraverso modelli di intelligenza artificiale generativa per replicare quelli del mondo reale. L'obiettivo di questa tesi è stato quindi generare, a partire dal dataset sintetico ONOT, contenente immagini raffiguranti persone di alta qualità e aderenti allo standard ISO/ICAO per l'uso in documenti leggibili elettronicamente, immagini modificate che ritraessero gli stessi soggetti con variazioni quali invecchiamento, aggiunta della barba, modifica dell'acconciatura, aggiunta di occhiali da vista o di un copricapo, modifiche alla pelle come tatuaggi o cicatrici. Le immagini originali e quelle modificate sono state poi usate per generare video sintetici e costruire così VAMONOT, un dataset sintetico di alta qualità che permetta l'addestramento di modelli incentrati sul riconoscimento di volti in sequenze video.

MATEVŽ VIDOVIČ - LIGHTWEIGHT MODELS FOR OCULAR SEGMENTATION

Full Title: Lightweight models for ocular segmentation using the IPAD method
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Matej Vitek
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=170320&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
It is known that deep neural networks are significantly overparameterized in most cases. Pruning reduces the computational complexity of the network and can even enhance its performance. To address this, we develop a framework for iterative pruning of convolutional neural networks, designed to support a variety of architectures in a user-friendly manner. We apply this framework to U-Net and SegNet models, which were trained for sclera and vein segmentation tasks on ocular images. The models were subsequently pruned using a diverse set of kernel importance measures, including the recently introduced Iterative Pruning with Activation Deviation (IPAD). We analyze the effects of pruning on model performance and compare the success of different kernel importance measures. The results we collected indicate a substantial performance advantage for pruned models over compact models trained from scratch, especially on the more challenging task of vein segmentation. We were able to confirm the superiority of the IPAD method in scenarios where ample training data is available and appropriate steps with respect to hyperparameter optimization can be taken given the computational budget.

ESTER MASALA - DECEPTIVE BEAUTY: THE IMPACT OF BEAUTY FILTERS ON DEEPFAKE AND MORPHING DETECTION

Full Title: Deceptive Beauty: The Impact of Beauty Filters on Deepfake and Morphing Detection
Institution: University of Cagliari
Supervisor: Gian Luca Marcialis
Contact email: marcialis@unica.it

Abstract:
In recent years, the use of digital beauty filters on social media has become increasingly widespread, raising new concerns about the reliability of facial images and videos. Although these transformations are often perceived as minor aesthetic modifications, they can alter facial characteristics that are relevant to automatic face analysis systems. This issue is particularly important in the field of digital manipulation detection, where the goal is to distinguish authentic content from altered content. In particular, techniques such as deepfakes and morphing attacks represent a threat to the security of biometric systems, as they can be used to deceive both human observers and automatic facial recognition systems. This thesis analyses the impact of beauty filters on the performance of automatic systems for detecting deepfakes and morphing attacks. To this end, an experimental evaluation is conducted on benchmark datasets, comparing the performance of several state-of-the-art detectors before and after the application of different smoothing and facial beautification techniques. The aim of this work is to understand whether, and to what extent, such filters can compromise the effectiveness of detection systems, thereby contributing to the assessment of the robustness of currently available tools and highlighting possible critical issues related to the use of modified facial images in biometric security contexts.

MATYLDA MUSILOVÁ - EXPLORING THE METHODS OF DIGITAL FINGERPRINT SCANNING

Full Title: Digitální záznam otisku prstů živých osob: komparace metod
Institution: Department of Anthropology, Faculty of Science, Masaryk University
Supervisor: Mgr. Mikoláš Jurda, Ph.D.; consultant: Prof. Ing. Dipl.-Ing. Martin Drahanský, Ph.D.
URL: https://is.muni.cz/th/bn6de/
Contact email: matyldamusilova@gmail.com

Abstract:
Digital fingerprint acquisition is a key component of modern biometric systems that are gradually replacing traditional ink-based techniques. The aim of this thesis was to compare the quality of fingerprints acquired using three digital fingerprint scan-ners (3D FLOW, LIVETOUCH Duo, CSF Flats) and the traditional ink-based method. Repeated captures of four fingers on both hands were collected from ten partici-pants using all methods. Fingerprint quality was evaluated using the NFIQ 2 algo-rithm, and physiological factors such as sex, skin temperature, and moisture were also considered. The highest quality scores were observed for images acquired us-ing the LIVETOUCH Duo device, while the traditional method yielded the lowest re-sults. The findings also suggest a potential influence of skin moisture on fingerprint image quality. Digital fingerprint scanners thus demonstrate the potential to replace conventional methods partially or fully, particularly in forensic contexts.

PHILLIP SROCK - ANALYSIS AND DETECTION OF FACIAL FILTERS USING FACE BEAUTY

Full Title: Analysis and Detection of Facial Filters using Face Beauty
Institution: Hochschule Darmstadt (h-da)
Supervisor: Christoph Busch and Juan Tapia
URL: https://dasec.h-da.de/2025/03/philipp-srock-successfully-defended-his-bachelor-thesis/
Contact email: christoph.busch@h.da.de

Abstract:
Although facial attractiveness seems subjective, facial retouching is widely spread in social media, advertisements and even applied in professional photo studios to let the individuals appear younger, remove wrinkles and skin impurities and generally speaking: enhance the beauty. This is not a problem itself, but when retouched images are used as biometric samples and enrolled in a biometric system, it is one. Since previous work has proven facial retouching to be a challenge for face recognition systems, detection of facial retouching becomes increasingly necessary. This work analyzes changes in beauty assessment algorithms and quality assessment algorithms of retouched images, assesses different feature extraction methods for artificial intelligence based retouching detection and evaluates whether face beauty and face quality can be exploited to enhance the detection rate. An assumption can be made that both provide useful features for the detection process. This study shows that even though face quality decreases while face beauty increases when a retouched sample is evaluated, face beauty and face quality do not measure the same features. Experiments conducted reveal that besides fusing multiple feature extraction methods, applying beauty scores improves the detection rate while face image quality has a very low impact when used to improve the detection rate. Detection results achieved on face filters not seen by the model during the training process are just above 1% average Equal-Error-Rate. Additionally, it is shown that this rate can be further improved when using Machine Learning for the fusion process instead of a fusion function.

FRANCESCO MAROTTO - AUTOMATIC CORRECTION OF VERBAL DISFLUENCIES USING SYNTHETIC VOICE GENERATION TECHNIQUES

Full Title: Automatic Correction of Verbal Disfluencies Using Synthetic Voice Generation Techniques
Institution: University of Cagliari
Supervisor: Marco Micheletto, Giulia Orrù
Contact email: marco.micheletto@unica.it

Abstract:
This thesis addresses the problem of personalized speech synthesis in the presence of speech affected by dysphonia, with the aim of developing and evaluating a pipeline capable of transcribing and regenerating the user's voice while preserving vocal identity. The research stems from the observation that voice disorders can significantly impair communication and social life, and that support systems based on Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) technologies could offer concrete benefits in terms of inclusion and communication quality. The work was structured into several phases, including data preparation using the FluencyBank dataset, the creation of a pipeline containing an ASR module and a TTS voice regeneration module, both integrated through a graphical user interface. The system was also evaluated using Word Error Rate (WER), acoustic quality analysis of the synthesized voice through Mel Cepstral Distortion (MCD), and subjective assessment through Mean Opinion Score (MOS). Experiments were also conducted on a voice external to the FluencyBank dataset, recorded under controlled conditions, in order to compare the results with those obtained using noisy data affected by dysphonia. In conclusion, the research confirms the feasibility of a personalized voice enhancement pipeline, while highlighting the limitations related to the quality of the available data and the reliability of speech synthesis. The preliminary results open up future development perspectives, particularly toward the use of cleaner datasets and more advanced models, with potential positive implications in clinical and social contexts.

OSKAR KONJANČIČ - DISTANCE BETWEEN SCLERA IMAGES

Full Title: Using a neural network to calculate the distance between sclera images
Institution: University of Ljubljana, Faculty of Computer and Information Science
Supervisor: Peter Peer, Matej Vitek
URL: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=168038&lang=eng
Link description: Thesis
Contact email: peter.peer@fri.uni-lj.si

Abstract:
This diploma thesis addresses the challenge of person recognition based on sclera images from the open dataset SBVPI. The work focuses on the use of deep learning to improve the recognition accuracy between two segmented vasculature sclera images. We developed and evaluated two different approaches: Siamese neural networks and binary classification. The results show that we have successfully improved the recognition accuracy. Furthermore, we found that the approach based on separating learning according to the direction of gaze is promising for further improvements in system performance.

MATTEO TRUDU - DEEPFAKE ATTACKS AGAINST AUTOMATIC SPEAKER RECOGNITION SYSTEMS

Full Title: Deepfake Attacks Against Automatic Speaker Recognition Systems
Institution: University of Cagliari
Supervisor: Marco Micheletto, Giulia Orrù
Contact email: marco.micheletto@unica.it

Abstract:
Audio deepfakes represent one of the most sophisticated and insidious manifestations of generative techniques based on artificial intelligence. Through the use of advanced Text-to-Speech (TTS) and Voice Conversion (VC) models, it is now possible to generate speech signals that are almost indistinguishable from real ones. Although these technologies have legitimate applications, they also pose new threats to the security of biometric systems, particularly Automatic Speaker Verification (ASV) systems. This thesis focuses on the analysis of the main voice attack techniques targeting ASV systems, with the aim of evaluating their effectiveness and practical implications. To this end, realistic attack scenarios were designed, based on the controlled generation of voice samples capable of reproducing credible operating conditions. The analysis ultimately made it possible to assess the robustness of the RawNet2 model in the task of detecting voice attacks. The results obtained provide critical insight into the current level of reliability of ASV systems, suggesting the need for more robust approaches and opening up new, still unexplored research scenarios.

ELISA YAN - IDENTITY VERIFICATION THROUGH THE COMBINATION OF MULTIPLE FRAMES AND FACE QUALITY METRICS IN BORDER CONTROL SCENARIOS

Full Title: Identity Verification through the Combination of Multiple Frames and Face Quality Metrics in Border Control Scenarios
Institution: University of Bologna
Supervisor: Matteo Ferrara
Contact email: matteo.ferrara@unibo.it

Abstract:
Face morphing is a technique that combines the biometric features of two or more individuals into a single image. This approach can pose a threat to biometric systems, particularly in automated border control gates, where the reliability of face recognition is crucial to ensuring border security. The objective of this thesis is to evaluate whether the use of multiple frames can improve the robustness of face recognition models and reduce the risk of false acceptances in the presence of morphing attacks. The AdaFace and MagFace recognition models were analyzed on a dataset acquired under simulated conditions, including variations in pose, occlusions, and illumination. Video sequences were represented by a single value through score aggregation strategies and quality metrics, such as mean, maximum, minimum, SER-FIQ, and OFIQ, to assess whether the integration of multiple frames enhances the robustness and reliability of the recognition process. Performance was measured in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR), using as a reference threshold the one defined by FRONTEX, the European Union agency responsible for border security.